Il browser Brave accusa Google di violare il GDPR e presenta un reclamo al Garante Privacy irlandese

Lo stabilirà il Garante Privacy irlandese se **Google** sta violando il **GDPR** come sostenuto dal browser **Brave**, che, invece, promette di essere a prova di privacy. Il responsabile policy del browser, **Johnny Ryan**, utilizzando **Chrome**, di proprietà di Big G, ha scoperto che *"Google utilizza pagine web nascoste assegnate agli utenti, senza il consenso di quest'ultimi, per fornire informazioni agli inserzionisti su ogni loro spostamento online, in totale violazione del GDPR'.* Così Ryan ha presentato un reclamo all'Autorità irlandese per la protezione dei dati personali.

La replica di Google

"Non offriamo annunci personalizzati o inviamo richieste di offerte agli inserzionisti senza il consenso dell'utente", ha replicato un portavoce di Google.

L'accusa nel dettaglio

Nel dettaglio, Johnny Ryan sostiene che il sistema di offerte in tempo reale (**RTB**) degli acquirenti autorizzati di Google – che viene utilizzato da milioni di siti Web per pubblicare annunci pubblicitari per i visitatori – "*trasmette dati personali"* sui visitatori a migliaia di aziende del settore pubblicitario per tutto il giorno, e ogni giorno.

"Tali dati possono essere utilizzati per tracciare gli utenti mentre navigano sul web, da un sito all'altro, in violazione del Regolamento europeo sulla protezione dei dati (GDPR)", ha

affermato Ryan. Negli Stati Uniti, questa pratica non è illegale.

Il meccanismo attraverso il quale Google trasmette illegalmente i dati agli inserzionisti, secondo il Chief policy officer di Brave, è noto come Push Page nascosta , che si carica senza essere visto dai visitatori del sito Web e avvia richieste di rete a vari servizi di annunci programmatici. Le pagine push vengono pubblicate da un dominio Google come file HTML denominati "cookie_push.html".

"Ogni pagina push è resa distintiva da un codice di quasi duemila caratteri, che Google aggiunge alla fine per identificare in modo univoco la persona su cui Google sta condividendo informazioni", ha spiegato Ryan nella sua denuncia. *"Questo, combinato con altri cookie forniti da Google",* ha aggiunto, *"consente alle aziende di identificare pseudonimamente la persona in circostanze in cui ciò non sarebbe altrimenti possibile".*

Le aziende invitate ad accedere a una pagina push, afferma Ryan, ricevono tutte lo stesso identificativo per la persona profilata, consentendo loro di fare un riferimento incrociato ai loro profili interni e di scambiarli con un'ampia visione dell'attività online di un utente.

Il portavoce di Google ha contestato la caratterizzazione di Push Pages da parte di Ryan. *"Un cookie_push non è un ID e non un identificatore"*, ha detto un portavoce in un'e-mail a *The Register* . *"È un parametro per misurare la latenza end-to-end".*

Staremo a vedere cosa deciderà il Garante Privacy irlandese.

https://www.key4biz.it/il-browser-brave-accusa-google-di-violare-il-gdpr-e-presenta-un-reclamo-al-garante-privacy-

irlandese/269953/

Senator pushes Amazon for details about Ring “partnerships” with police

Enlarge / A Ring video doorbell mounted on a home.

reader comments

30 with 21 posters participating

Share this story

Amazon’s Ring line of video doorbells and home surveillance equipment is particularly popular with one key group: police. More than 400 law enforcement agencies around the country have partnered with Ring to use its apps and help market its security cameras to residents in the name of safer neighborhoods. As a dozen recent media reports have shown, however, the details about these partnerships and the privacy concerns they raise tend to be shrouded in secrecy and hard to learn.

Sen. Ed Markey (D-Mass.) is now among those who would like Amazon to explain what, exactly, Ring is up to. “The nature of Ring’s products and its partnerships with police departments raise serious privacy and civil liberties concerns,” Markey said in a letter (PDF) addressed to Amazon CEO Jeff Bezos.

“Although Amazon markets Ring as America’s ‘new neighborhood watch,’ the technology captures and stores video from millions of households and sweeps up footage of countless bystanders who may be unaware that they are being filmed,” Markey said in a statement. “I am particularly alarmed to learn that Ring is pursuing facial-recognition technology with the potential to flag certain individuals as suspicious based on their biometric information.”

Until very recently, Ring would not disclose how many of these partnerships it currently has. Following media pressure, however, the company said in late August it had 405 active agreements.

A growing list of concerns

Throughout the summer, reports from outlets including The Washington Post, Gizmodo, CNET, and Vice Motherboard have dug into the details of these agreements, which are rarely made public. The reports have found that Ring writes the press releases, social media posts, and talking points police departments use to encourage widespread Ring adoption. The company also asks police not to call its surveillance products “security cameras” or use the word “surveillance.”

Concerns also abound about user privacy. Ring claims not to share lists of users or give maps pinpointing exact locations of cameras to police. In August, the company told Ars that participating agencies “must go through the Ring team when making a video request to customers,” adding, “Customers can choose to opt out or decline any request, and law enforcement agencies have no visibility into which customers have received a request and which have opted out or declined.”

But multiple reports have found evidence that Ring shared maps featuring active cameras with police in 2018, basically as a sales tactic to convince a police department to sign up for the partnership program by demonstrating how many cameras were

already operating in its jurisdiction. Reports also found evidence that Ring collected data about purchasers which it then shared with police in order to cross-reference eligibility for subsidy programs or camera giveaways that police conduct, in partnership with Ring.

The company also gets access to 911 call data in some jurisdictions, which it uses to "curate" crime news for its Neighbors app. The app, while open to anyone, is optimized for Ring users, who can easily share footage from their doorbells through it. Police can also use their companion portal to send out a localized blast to Neighbors users requesting footage as part of an investigation. Although Ring now says it does not share data about users who decline to share their footage, at one point it gave cops a breakdown about how their requests were performing.

Late last year, the ACLU also flagged a patent application from Ring that would allow devices to ship with facial-recognition software, such as Amazon's controversial Rekognition system. The patent would allow police or homeowners to flag certain faces as "suspicious." If a suspicious face showed up on camera, police could then be dispatched to its location. Rekognition, however, is far from reliable and, like many other facial recognition services, is particularly likely to indicate false positives for people of color.

Clear answers?

Sen. Markey gave Ring until September 26 to answer questions that reporters and the general public have increasingly been trying to gain clarity on. Those inquiries relate not only to information requests but also to data retention and sharing policies, as well as other privacy concerns.

"How long has Ring prompted its users to share video footage with law enforcement?" Markey asked Ring, pushing for a

“detailed timeline of when this sharing began and how, if at all, Ring has changed its policies” over time.

The letter asks Amazon to provide a list of all law enforcement agencies that have ever had or currently have access to Ring video, as well as a copy of a standard sharing agreement. It also asks if Ring requires police departments to delete users’ footage after a certain period, if Ring requires police departments to handle footage in such a way as to minimize the risk of data breaches or leaks, and if Ring has any kind of language in those agreements either permitting or barring police from sharing footage they obtain with third parties.

Sen. Markey also expressed strong concern about the potential for Ring products to contribute to racial profiling and civil liberties violations, especially if Rekognition integration does become a feature. He asked the company to provide a timeline for when or if it plans to add such features as well as a list of criminal justice and civil liberties consultants it has consulted in its work.

https://arstechnica.com/?p=1562925

Google, la FTC multa YouTube per 170 milioni per aver violato la privacy dei minori

Google ha concordato di pagare 170 milioni di dollari per risolvere le accuse della **Federal Trade Commission** e del procuratore generale di **New York** secondo cui **YouTube** avrebbe raccolto illegalmente informazioni personali da bambini senza

il consenso dei genitori.

Si tratta della più grande multa mai commiata ai sensi della legge sulla protezione della privacy online dei minori, approvata per la prima volta negli Stati Uniti nel 1998.

Le autorità americane hanno riscontrato che la piattaforma di streaming video controllata da Google ha consapevolmente e illegalmente raccolto dati di giovanissimi utilizzandoli poi a scopo di profitto, per raggiungere la giovanissima audience con pubblicità mirate. Con questo sistema la **FTC** ha dichiarato che YouTube "*ha guadagnato milioni di dollari*".

The Children's Online Privacy Protection Act

La legge USA sulla privacy online chiamata "**The Children's Online Privacy Protection Act" (COPPA)**, richiede che i siti Web e servizi online destinati ai minori forniscano notifiche delle loro pratiche informative e ottengano il consenso dei genitori prima di raccogliere informazioni personali da minori di 13 anni, incluso l'uso di cookie. Inoltre, terze parti, come le reti pubblicitarie, sono anche soggette alla privacy act, laddove conoscono effettivamente che stanno raccogliendo informazioni personali direttamente dagli utenti di siti Web per bambini e servizi online.

Come cambierà YouTube

Google ha annunciato che attuerà delle nuove modifiche su YouTube a partire dalla limitazione della raccolta e l'utilizzo dei dati sui video realizzati per i bambini. Inoltre interromperà la pubblicazione completa di annunci

personalizzati su questi contenuti e alcune funzionalità non saranno più disponibili, come commenti e notifiche.

I creatori saranno responsabili di contrassegnare i contenuti dei bambini e Google utilizzerà il **Machine Learning** per trovare video che mirano chiaramente a un pubblico giovane.

La società inoltre raccomanda l'uso del suo servizio *YouTube Kids* per garantire che i bambini guardino contenuti appropriati. Sta inoltre istituendo un fondo da 100 milioni di dollari per sostenere la creazione di "contenuti per bambini, famiglia e contenuti educativi" da erogare nei prossimi tre anni.

La multa a Facebook per 5 miliardi

Le autorità statunitensi hanno gli occhi puntati nei confronti delle big tech company americane ormai da tempo, dopo che a lungo l'Europa è stata all'avanguardia sulla protezione dei dati per gli utenti. La Ftc in luglio aveva deciso una multa di 5 miliardi di dollari contro Facebook, per lo scandalo **Cambridge Analytica.**

https://www.key4biz.it/google-la-ftc-multa-youtube-per-170-milioni-per-aver-violato-la-privacy-dei-minori/269689/

---

5 consigli per mettere in atto una solida strategia di data management

Nell'attuale economia delle informazioni, i dati sono diventati la più recente moneta digitale del mondo. Ogni

minuto, ci sono circa 450.000 tweet, 500.000 commenti pubblicati su **Facebook**, 999.000 swipe di **Tinder**, 3,6 milioni ricerche di Google, 4,1 milioni di video di YouTube visualizzati e 103 milioni e-mail di spam. A ciò si aggiungono una serie di dati dei clienti, dati dei dipendenti, dati medici, dati governativi, dati finanziari – e l'elenco è infinito.

Secondo **IDC**, entro il 2025 la sfera dati globale aumenterà fino a 163 zettabyte, 10 volte superiore alla quantità attuale.

Esaminando il modo in cui i social media gestiscono i dati degli utenti, la crescita di questi dati, la loro protezione e la privacy digitale sono argomenti al centro dell'attenzione.

I progressi nella business intelligence hanno dato alle organizzazioni la capacità di trarre insight da questi dati così ricchi da essere effettivamente di natura predittiva. Il risultato: le aziende restano un passo avanti rispetto alle aspettative e alle esigenze dei clienti, anziché limitarsi a reagire ad esse.

La raccolta, l'archiviazione e l'analisi di questi dati ispira innovazione e aiuta le aziende ad ottenere sul mercato vantaggi che non avrebbero mai pensato essere possibili. Allo stesso tempo, le organizzazioni devono essere preparate a compiere scelte strategiche per quanto riguarda la raccolta, l'archiviazione, l'analisi e la localizzazione dei dati e a come proteggerli da violazioni o cyber-attack.

Con l'aumento dei dati, aumenta la responsabilità. Ecco cinque passaggi che le aziende possono adottare per assicurarsi di disporre di una solida strategia di data management:

1. Mappare i propri dati

“Quali dati possiedo e quanto sono sensibili?” Questa è la prima domanda che un’azienda dovrebbe porsi. Per poter rispondere a questa domanda, l’organizzazione deve avere un approccio olistico alla gestione dei propri dati. Ciò significa avere una visibilità completa dei dati, quali informazioni sono memorizzate, come vengono utilizzate, chi le possiede, chi vi accede e come devono essere trattate dal punto di vista della compliance.

Questo approccio deve includere la capacità di classificare automaticamente grandi volumi di dati digitali, scansionarli ed etichettarli in modo preciso e intelligente per garantire che le informazioni siano gestite con efficacia e possano essere utilizzate on-demand.

2. **Nominare un responsabile dei dati**

Che si tratti di un responsabile della protezione dei dati (Data Protection Officer, DPO) o di un direttore dei sistemi informativi (Director of Information Systems, DSI), nominare una persona per gestire la protezione dei dati può essere molto utile per un’azienda. Il consiglio di amministrazione dovrebbe potersi affidare a questa persona per assicurarsi che prenda le decisioni giuste quando si tratta di gestire i dati. I compiti del DPO o del DSI dovrebbero comprendere, ad esempio, la registrazione del trattamento dei dati, l’elaborazione della strategia di protezione dei dati e la verifica della conformità. Oltre a garantire la protezione, DPO o DSI sarebbe responsabile dell’introduzione di tecnologie in grado di generare crescita, nonché di esaminare le possibili implicazioni di tutte le tecnologie che raccolgono, conservano o utilizzano dati personali

3. Ottenere l’ok dal Board

La trasformazione digitale è vitale per qualsiasi azienda che vuole non solo sopravvivere, ma anche avere successo. Pertanto, le decisioni relative alla tecnologia e ai dati non

dovrebbero più essere di esclusiva responsabilità del team IT, ma dovrebbero diventare discussioni a livello di Board. Quando si cerca di implementare una strategia di gestione dei dati, è indispensabile ottenere il consenso dal consiglio di amministrazione per garantire investimenti e impegno.

Il GDPR ha creato nuove comunicazioni e collaborazioni tra i dipartimenti IT e legali e, per continuare a utilizzare i dati in modo efficace e conforme, la collaborazione tra i vari dipartimenti e IT deve continuare.

4. Educare i dipendenti

Se i dati sono la valuta delle organizzazioni, la responsabilità è di ogni singolo individuo all'interno dell'azienda. Infondere una cultura del rispetto delle norme tra i dipendenti si dimostrerà il vero propulsore per un cambiamento a lungo termine. Le aziende devono implementare nuovi processi e politiche, tra cui formazione, premi e contratti aggiornati a supporto della gestione e della protezione dei dati, per evidenziare il ruolo che ogni dipendente svolge nella protezione dei dati della propria organizzazione.

Rendere tutti i dipendenti custodi affidabili dei dati creerà un impatto duraturo poiché la salute e la protezione dei dati diventerà un'abitudine quotidiana per tutti.

5. Misurare l'impatto in tempo reale della propria strategia di data management

Infine, le aziende devono quantificare i risultati della propria strategia di gestione dei dati. Rivalutando frequentemente i vantaggi e l'efficienza in termini di costi della propria strategia, le organizzazioni possono registrare tutte le azioni intraprese e tutti i miglioramenti apportati. I risultati possono poi essere valutati per decidere se continuare nella stessa direzione o cambiare rotta. Questo approccio non solo fa risparmiare tempo, ma rassicura anche i

team di gestione e gli stakeholder che la strategia di gestione dei dati è utile.

Le nuove modalità di raccolta e analisi dei dati, la diffusione dei social media, dell'intelligenza artificiale e dell'Internet of Things (IoT) rendono la gestione dei dati sempre più complessa. Non c'è una risposta uniforme a come ogni organizzazione dovrebbe gestire e proteggere i propri dati: per ogni singola azienda ci sono diverse opportunità e ostacoli. Tuttavia, è fondamentale dare la priorità al data management, alla protezione dei dati, all'ottimizzazione dello storage e alla governance, insieme alle decisioni su come i dati saranno utilizzati a fini commerciali. Questa mentalità deve provenire dall'alto ed essere integrata nella cultura di un'organizzazione.

https://www.key4biz.it/5-consigli-per-mettere-in-atto-una-solida-strategia-di-data-management/269476/

Piattaforma Rousseau, Luca Bolognini (IIP): 'Chi controlla la verificabilità dei codici e degli algoritmi?'

La nascita del **Governo M5S-PD** è legata all'esito del voto degli iscritti al M5S sulla **piattaforma Rousseau**. Si vota fino alle ore 18 di oggi. Molti mettono sotto la lente d'ingrandimento i possibili "attacchi informatici" manipolativi contro la piattaforma, ma secondo **Luca Bolognini**,

presidente dell'Istituto Italiano per la Privacy (IIP) e la valorizzazione dei dati, il vero problema è un altro.

Key4biz. ***Qual è?***

Luca Bolognini.Vede, io non demonizzo Rousseau: dico quello che direi di qualsiasi piattaforma di qualsiasi partito. Il punto è che oggi, in Italia, da Rousseau stanno dipendendo la formazione di un Governo e molte altre decisioni politiche cruciali. Naturalmente, la sicurezza dei sistemi informatici e dei dati personali è importantissima, a maggior ragione in caso di piattaforme politiche on line, sulle quali "girano" informazioni estremamente sensibili dei cittadini. È ovvio che sia un bene – oltre che un obbligo di legge – proteggerli da accessi abusivi e da aggressioni. Ma il problema più rilevante di tutti non è la prevenzione di patologie informatiche e attacchi malintenzionati – sacrosanta – quanto la trasparente verificabilità dei codici informatici, degli algoritmi, delle operazioni e dei trattamenti di dati che vengono eseguiti – fisiologicamente, legittimamente sul piano formale! – dal gestore della piattaforma. In buona sostanza, è essenziale che sia garantito il metodo democratico di cui all'articolo 49 della Costituzione Italiana, declinandolo anche in chiave tecnologica e non solo in termini di democraticità delle forme partecipative e associative "all'antica". Dopotutto, concordo con chi teorizza che i nuovi partiti siano i social network: anche i bit pesano nel gioco delle libertà

Key4biz. ***Cosa propone per risolvere questo problema?***

Luca Bolognini. Due interventi, se necessario anche di rango costituzionale. Uno per assicurare il metodo democratico, che citavo prima: deve essere garantita piena trasparenza dei codici informatici e dei log amministrativi e operativi delle piattaforme decisionali dei partiti politici. Negli ultimi

anni abbiamo introdotto norme stringenti in materia di trasparenza finanziaria dei partiti e dei movimenti politici, perché non fare lo stesso con gli algoritmi, i codici e i log delle loro piattaforme decisionali? Il secondo intervento potrebbe sembrare fantasioso, ma non lo è: introdurre in Costituzione il principio di "Stato di diritto umano", per evitare che in futuro decisioni o voti automatizzati e artificiali, non provenienti da espressioni di volontà dell'essere umano – ad esempio un singolo parlamentare o consigliere regionale – possano valere nella formazione delle regole e delle leggi.

Key4biz. ***La privacy degli utenti-elettori è tutelata sulla piattaforma di Casaleggio?***

Luca Bolognini. Oggi come oggi, la privacy è un terreno di battaglia cruenta, sia nel senso della tutela della riservatezza degli utenti-elettori, sia per il corretto trattamento dei loro dati, al di là del fatto che debbano essere o meno tenuti riservati: pensiamo a **Cambridge Analytica** e alle manipolazioni dell'opinione pubblica che ne sono derivate. Il Garante Privacy, nei suoi provvedimenti dedicati a Rousseau, ha precisato una serie di misure per consentire di proteggere meglio i dati degli utenti partecipanti alla piattaforma. Dalle dichiarazioni che ho letto, anche di **Davide Casaleggio,** le misure di sicurezza dovrebbero essere state implementate e presumo siano tenute costantemente aggiornate. La sicurezza, ripeto, è una battaglia continua, non arriva mai alla fine. Ma ritorno a quanto dicevo sopra: quis custodiet ipsos custodes? Chi controlla il data controller, il titolare del trattamento, il gestore della piattaforma e i suoi incaricati? Si potrebbe immaginare un ruolo di garanzia, proprio per questo, in capo al **Garante Privacy** e ad **Agcom**, congiuntamente, che vengano abilitati a svolgere verifiche di correttezza sul funzionamento dei codici informatici nelle operazioni di voto on line; questo consentirebbe ai partiti e ai movimenti politici di non pubblicare totalmente i codici,

rendendoli disponibili integralmente solo in un “ambiente protetto” dall’Autorità.

Key4biz. ***Quali le condizioni necessarie per introdurre in Italia l’evoting?***

Luca Bolognini. Credo fermamente nell’introduzione delle due innovazioni di cui ho parlato prima: trasparenza dei codici informatici delle piattaforme politiche, da un lato, e principio dello “Stato di diritto umano”, dall’altro. Ma sull’affidabilità dell’e-voting, mi permetta di essere ancora scettico, per ragioni di difficile tutela dell’anonimato e, insieme, di non manipolabilità interna/esterna dei sistemi. Per ora, mi limito a raccontare alle mie figlie la sera, prima di dormire, bellissime fiabe sul rospo che, baciato dalla principessa, si trasforma in un perfetto sistema di voto elettronico: magari, quando voteranno loro da grandi, i sogni saranno diventati realtà.

https://www.key4biz.it/governo-m5s-pd-voto-su-piattaforma-rousseau-bolognini-iip-chi-controlla-la-verificabilita-dei-codici-informatici-e-degli-algoritmi/269464/

Il caso svedese. Riconoscimento facciale e dati biometrici, cosa dice il GDPR?

L’autorità di controllo per la protezione dei dati personali svedese ha emesso un provvedimento con il quale ha sanzionato una scuola con il pagamento di circa 20.000,00 euro. Il

provvedimento è attualmente disponibile soltanto in lingua svedese; di seguito, pertanto, si propone una lettura della notizia con un sintetico commento privo di approfondimenti.

Cosa è accaduto?

Una scuola svedese ha utilizzato un sistema di **riconoscimento facciale** degli studenti che la frequentano al fine di verificare le loro presenze. In sede di istruttoria da parte dell'autorità di controllo svedese, la scuola si è difesa affermando che gli studenti hanno espresso il consenso. L'autorità di controllo ha chiuso l'istruttoria con un provvedimento sanzionatorio.

Quali sono gli aspetti rilevanti?

Il punto di partenza è l'utilizzo di un sistema di riconoscimento facciale. Con tale espressione solitamente si fa riferimento a uno o più algoritmi basati sulla **Intelligenza Artificiale** (IA) e il **Machine Learning** (ML), attraverso i quali è possibile identificare una persona mediante l'acquisizione dell'immagine del volto da una foto o da un video. L'algoritmo processa l'immagine utilizzando modelli matematici e restituisce, archiviandoli in un database, dati che sono riferiti alla persona.

Come è noto, il Regolamento (UE) 2016/79 (**GDPR**) al considerando (51) afferma, fra l'altro: "*Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica*".

Pertanto, l'utilizzo di immagini che ritraggono volti di persone mediante sistemi tecnici specifici che ne consente l'identificazione univoca fa classificare i dati trattati come "**biometrici**".

Dalla definizione dei dati biometrici fornita dall'art. 4(1)(14) del GDPR emerge che sono: "*i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*"; in sostanza, ciò che rileva è la modalità di trattamento dei dati dell'immagine del volto di una persona.

È possibile effettuare il trattamento dei dati biometrici e in particolare di quelli derivanti da un riconoscimento facciale?

In termini generali, il trattamento dei dati personali, anche biometrici, è consentito nel rispetto della disciplina del GDPR; a tale fine si rende necessaria un'interpretazione coordinata di una pluralità di norme: in particolare, per il trattamento di dati biometrici che si riferiscono all'immagine facciale di una persona per specifiche finalità delle quali è stato informato l'interessato va valutata preventivamente la sussistenza di una delle basi giuridiche previste dall'art. 6 del GDPR quale condizione di liceità del trattamento stesso.

L'art. 9(1) del GDPR pone un generale divieto di trattare dati biometrici; tuttavia il successivo paragrafo 2 indica 10 casi in cui il trattamento è lecito. Tra questi l'unico applicabile al caso di specie è il primo, ossia il consenso dell'interessato "**esplicito al trattamento di tali dati personali per una o più finalità specifiche**".

L'art. 9 del GDPR va coordinato con l'art. 6 che indica le condizioni di liceità del trattamento, tra cui c'è il consenso dell'interessato.

È opportuno sottolineare che il consenso deve essere "**esplicito**" (cioè chiaro ed espresso liberamente dall'interessato) e prestato "**per una o più finalità specifiche**" (il titolare del trattamento è, quindi, a informare l'interessato in ordine alle finalità per le quali i sui dati saranno trattati).

Appare necessario, inoltre, un ulteriore coordinamento con l'art. 7 che indica le condizioni del consenso: esso deve essere libero, ossia espresso senza alcun condizionamento da parte dell'interessato, il quale ha anche il diritto di revocarlo in qualsiasi momento.

L'onere di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali grava sul titolare del trattamento.

Vale la pena di evidenziare che in Italia, in seguito all' emanazione del D. Lgs. 101/2018 di adeguamento del c.d. "codice privacy" (D. Lgs. 196/2003) al GDPR, sono state aggiunte norme che riguardano i dati biometrici con espresso riferimento alla salute.

Nell'ipotesi di riconoscimento facciale il trattamento dei dati biometrici è possibile ove l'interessato esprima il proprio consenso libero ed esplicito per specifiche finalità.

Questi i presupposti e le condizioni ai sensi della normativa in materia di protezione dei dati personali.

A tutto ciò si aggiunga che anche gli algoritmi di riconoscimento facciale devono rispettare il principio previsto dall'art. 25 del GDPR "*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*" (**Data protection by design and by default**) e comunque quello universalmente noto come **Privacy by Design (PbD)**. Pertanto, sia nella fase di progettazione e di elaborazione dell'algoritmo (e quindi al momento di determinare i mezzi del trattamento) "*sia all'atto del trattamento stesso*" il titolare

del trattamento deve mettere in atto misure tecniche e organizzative adeguate per attuare efficacemente i principi sulla protezione dei dati personali e comunque integrare nel trattamento le necessarie garanzie per il rispetto del GDPR.

Perché la scuola svedese è stata sanzionata?

Le scuole, generalmente, effettuano diversi trattamenti di dati personali con specifiche finalità nel rispetto delle condizioni di liceità previste dall'art. 6 del GDPR adottando un'idonea base giuridica. Con riferimento agli studenti, una delle finalità può ben essere quella diretta alla verifica della frequenza scolastica.

Occorre verificare con quali modalità e con quali sistemi tecnici viene effettuato il trattamento dei dati personali.

Si è già detto che per il riconoscimento facciale è necessario il consenso dell'interessato; qualora gli studenti siano minorenni, questo deve essere prestato da parte di chi esercita la responsabilità genitoriale (il consenso dato dai minori infra-sedicenni, per il GDPR, e infra-quattordicenni, per la legislazione italiana, vale solo per i servizi della società dell'informazione).

Gli studenti devono poter frequentare la scuola, seguire le lezioni dei docenti ed essere sottoposti alle opportune verifiche verso il raggiungimento degli obiettivi. Lo studente, in questo contesto, non dovrebbe assolutamente essere condizionato dai docenti o dalla scuola sia riguardo alle proprie valutazioni sugli obiettivi formativi raggiunti sia in ordine al percorso formativo da compiere. Qualora, per assurdo, non fosse così, il consenso manifestato dallo studente potrebbe risultare viziato in quanto non espresso liberamente, ossia privo di qualunque condizionamento, e quindi non validamente prestato. Allo stesso modo, qualora lo

studente prestasse il proprio consenso – apparentemente esplicito e libero – ma condizionato da un timore reverenziale nei confronti dei docenti e della scuola, il consenso stesso risulterebbe viziato. Il consenso viziato, si presume (dato che il testo del provvedimento è unicamente in lingua svedese) essere, la motivazione che ha indotto l'autorità di controllo svedese a considerare deficitaria la primaria condizione di validità del trattamento dei dati personali degli studenti mediante un sistema di riconoscimento facciale.

Occorre, tuttavia, considerate aspetti ulteriori che potrebbero sensibilmente "limitare" la validità del consenso e i diritti dell'interessato.

Poiché lo studente è libero anche di non esprimere il consenso nei termini appena esposti, vanno valutate le modalità concrete del sistema di acquisizione delle immagini dei volti mediante un sistema di riconoscimento facciale.

In sostanza, se una telecamera con la quale si effettua l'acquisizione dell'immagine del volto fosse posizionata in un luogo comune della suola scuola (ingresso o aula o corridoi), luogo, cioè, nel quale il passaggio è obbligato per la fruizione dei servizi scolastici, ciò renderebbe di fatto inutile la negazione del consenso da parte dello studente. Come si potrebbe evitare che la camera riprenda il volto dello studente che non avesse espresso il consenso?

Tale aspetto assume un rilievo ulteriore se si prende in considerazione il diritto di revocare il consenso; infatti, come si eviterebbe la ripresa del volto dello studente che ha deciso di revocare il proprio consenso se la telecamera è posizionata in modo che riprenda indiscriminatamente chiunque?

Uno degli aspetti da considerare in questo complesso contesto, unitamente a quanto su indicato, è anche quello della sicurezza del trattamento ai sensi dell'art. 32 del GDPR. Infatti, il titolare o il responsabile del trattamento mette

"*in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*". In sostanza il titola-re o il responsabile del trattamento devono adottare le opportune misure idonee a ridurre il rischio "*di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*".

La sicurezza è uno degli aspetti rilevanti con riguardo al trattamento dei dati personali.

Le scuole italiane possono utilizzare sistemi di riconoscimento facciale?

Quanto all'Italia, si fa presente che il Garante Privacy già dal 2016 (prima dell'applicazione del GDPR dal 25 maggio 2018) aveva pubblicato un vademecum dal titolo "La scuola a prova di privacy".

Qualora non sia possibile fare riferimento ad altri casi, oltre a quello del consenso, previsti dall'art. 9(2) del GDPR, il trattamento dei dati biometrici non è consentito. Come si è detto, il trattamento è lecito solo in presenza di una condizione tra quelle indicate dall'art. 6(1) del GDPR, tra cui (quelle che appaiono compatibili con il caso di specie) si indicano:

6(1)(c)"*il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento*"; deve sussistere un obbligo di legge.

6(1)(e)"*il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*". Le scuole eseguono un compito di interesse pubblico; questa condizione va coordinata con quanto disposto dall'art. **9(2)(g)** e precisamente "*il trattamento è necessario*

per motivi di interesse pubblico rilevante". Il codice privacy italiano, così come modificato dal D. Lgs. 101/2018, menziona all'art. 2-sexies (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante) la seguente ipotesi che costituisce motivo di interesse pubblico rilevante: "*bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario*".

Non sembra facile, invece, collocare il trattamento dei dati personali per finalità di verifica delle frequenze scolastiche nell'ipotesi prevista dall'art. **6(1)(f)**secondo la quale "*il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore*". La condizione di liceità prevista dal citato art. 6(1)(f) – il legittimo interesse del titolare del trattamento meriterebbe particolare approfondimento sia in relazione al considerando (47) sia riguardo alla produzione del Comitato europeo per la protezione dei dati personali (EDPS, già Art. 29WP).

Il citato art. 6 va coordinato con l'art. 9 e tra i casi previsti, quelli che appaiono compatibili con le attività di una scuola appaiono essere i seguenti:

art. 9(2)(e)"*il trattamento riguarda dati personali resi manifestamente pubblici dall'interes-sato*", sempre che si sia in grado di dimostrare tutto ciò.

art. 9(2)(f)"*il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali*", ma in questo caso la finalità del trattamento non potrà essere quella della verifica della frequenza scolastica, ma probabilmente la tutela del patrimonio (es. installazione di sistemi di video-

sorveglianza).

art. 9(2)(g)“*il trattamento è necessario per motivi di interesse pubblico rilevante*” si ri-manda a quanto precedentemente evidenziato.

In conclusione

Ad oggi in Italia non risulta presente una normativa che consenta alle scuole di poter validamente e lecitamente porre in essere il riconoscimento facciale; occorrerebbe valutare attentamente e caso per caso il contesto e le tecniche utilizzate.

Di certo il provvedimento emesso dall’autorità di controllo svedese, oltre ad essere il primo sul punto, costituisce un’autorevole indicazione per perseguire un’opera di adeguata sensibilizzazione verso l’aumento di consapevolezza sui rischi connessi ai sistemi di riconoscimento facciale sia per i minorenni sia per i soggetti maggiori di età, specie nelle scuole.

https://www.key4biz.it/il-caso-svedese-riconoscimento-facciale-e-dati-biometrici-cosa-dice-il-gdpr/269241/

Ring reportedly shared video sharing data, detailed maps with police in 2018

Enlarge / A map showing the approximate location of the 405 police departments working with Ring as of August 30, 2019

reader comments

13 with 11 posters participating

Share this story

Ring, Amazon's home security camera and surveillance company, has since 2018 rapidly expanded its business by partnering with more than 400 police and sheriff departments nationwide. Amid a growing chorus of privacy complaints and media reports about these partnerships, Ring has repeatedly promised explicitly that police have no way of knowing details of who has the cameras installed and what residents are—or aren't—willing to share their footage. New reports, however, indicate that police departments may be receiving more data about Ring users in their jurisdictions than previously disclosed.

Gizmodo reports today that documents it obtained from a Florida police department included emails from Ring "about the number of times residents had refused police access to their cameras or ignored their requests altogether."

Owners of Ring devices can connect them to an app called Neighbors, which is also available for the general public to use. The app collects "crime reports" from participants, who can also choose to upload images and video either directly from their Ring devices or uploaded from other sources.

Police who partner with Ring have access to a sort of companion portal, which among other things, allows them to send out an email blast to all Neighbors members in a specific area asking them to share footage captured during a window of time as part of an investigation. "Law enforcement agencies who participate in the Neighbors app must go through the Ring team when making a video request to customers," a Ring

representative told Ars earlier this week. “Customers can choose to opt out or decline any request, and law enforcement agencies have no visibility into which customers have received a request and which have opted out or declined.”

Ring representatives have been pushing “engagement” hard on the police departments they work with, and the data obtained by Gizmodo makes it easy to see why. The police department in question issued 22 requests for footage between May and September 2018, Gizmodo found, leading to 319 distinct emails being sent to residents asking them to hand over footage. They received permission to access a total of 11 files, a 3.5% success rate.

Gizmodo notes that customers seemed intuitively to understand that the “do not share” option in the emails they received was not worth the effort: exactly zero recipients of the email clicked the button, instead simply ignoring or deleting the email 308 times.

In one email, a Ring manager admitted more granular data could be helpful. “Did one person share 11 videos or did 11 people share one video each,” the manager wrote. “We will have a better idea after we collect more data.”

Ring now keeps statistical data of this type to itself, the company told Gizmodo. “This is not representative of our current policies or the current video request process,” the company said. “Ring does not provide video request data to law enforcement agencies.”

Now you see it…

Ring doesn’t like for its law enforcement partners to share information about the portal back-end with the public. Cnet last week published a roundup of those features Ring might wish to keep quiet, including a “heat map” showing where police could find active Ring devices in their area. Ring told

Ars on Wednesday that it “recently updated the steps law enforcement partners take” to request video during an investigation, and, “as a result, there is no device density heat map” available any longer.

While heat maps may no longer be available, however, at one time Ring did indeed provided detailed maps to its partners. The Guardian obtained documents it published today showing the evolution of the agreement between Ring and Gwinnett County, Georgia, just outside of Atlanta.

Ring approached the Gwinnett police in August 2018, The Guardian found, and the agreement was approved by the police in May of this year. The records show that Ring heavily edited the press release Gwinnett authorities used to discuss the deal, as seems to be standard for these arrangements.

During those months, Ring also provided the Gwinnett police with a map showing the locations of “hundreds” of Ring devices within the county borders

The Electronic Frontier Foundation calls Ring “a perfect storm of privacy threats.”

“The rapid proliferation of this partnership between police departments and the Ring surveillance system—without any oversight, transparency, or restrictions—poses a grave threat to the privacy of all people in the community,” the EFF said. “The growing partnerships between Amazon and police departments corrodes trust in an important civic institution by turning public servants into salespeople for Amazon products.”

https://arstechnica.com/?p=1560667

Tessera sanitaria e videolottery per i minori, arriva l’ok dal Garante Privacy

L’Autorità **Garante per la Protezione dei Dati Personali** ha dato parere favorevole allo schema di decreto previsto dal Decreto legge Dignità, all’utilizzo della tessera sanitaria per vietare ai minori di giocare alle videolottery.

In particolare il dl varato lo scorso anno prevede che ‘‘*l’accesso agli apparecchi di intrattenimento è consentito esclusivamente mediante l’utilizzo della tessera sanitaria, al fine di impedire l’accesso ai giochi da parte dei minori*”.

Lo schema attuativo della norma è stato messo a punto dall’Agenzia delle dogane, che ha chiesto il parere del Garante per la privacy, in merito all’utilizzo della tessera sanitaria. Nel parere l’Autority scrive così: *”Per i profili di competenza non vi sono rilievi da formulare” e, di conseguenza, ”esprime parere favorevole”.*

Dal primo gennaio 2020, gli apparecchi privi di meccanismi idonei a impedire l’accesso ai giochi ai minori dovranno essere rimossi dall’esercizio e la violazione sarà punita con sanzioni pari a 10mila euro per ciascun apparecchio. Come noto, il testo prevede già lo stop alle pubblicità per il gioco d’azzardo. Nuovo è invece il logo di Stato “no slot” per i bar, gli esercizi pubblici e i circoli privati che eliminano o si impegnano a non installare apparecchi da gioco.

minori-arriva-lok-dal-garante-privacy/269017/

Siri, Apple chiede scusa agli utenti e licenzia 300 dipendenti

‘Mea culpa’ di **Apple** sul caso **Siri** e delle violazioni della privacy per gli utenti.

L’azienda di **Cupertino** si è scusata con gli utenti per aver ascoltato le loro conversazioni sul suo assistente digitale Siri dopo lo scandalo scoperto dal quotidiano inglese **Guardian**, il primo a denunciare la violazione della privacy da parte di Apple.

La società ha dichiarato di aver interrotto la pratica di rivedere le registrazioni audio Siri, ma riprenderà entro la fine dell’anno sotto severi controlli sulla privacy, in modo da poter continuare a migliorare il servizio ad attivazione vocale.

Licenziamenti

Il colosso americano ha quindi deciso di licenziare in massa i dipendenti in Europa, assunti per verificare la presenza di errori nelle registrazioni di Siri. Circa 300 persone sono state mandate a casa solo nella struttura di Cork. “*Come risultato della nostra revisione abbiamo realizzato di non essere stati interamente all’altezza dei nostri alti ideali e per questo ci scusiamo*“, dichiara Apple in una nota pubblicata oggi sul blog ufficiale dell’azienda, annunciando nuove

pratiche per tutelare la privacy.

Apple dunque prevede di ripristinare la pratica di classificazione dopo aver apportato alcune modifiche agli aggiornamenti del software in autunno.

Le modifiche includono la mancata conservazione delle registrazioni audio delle interazioni di Siri. Invece, Apple utilizzerà trascrizioni generate al computer per aiutare Siri a migliorare. Inoltre aggiunge l'azienda, solo i dipendenti Apple saranno autorizzati ad ascoltare campioni audio delle interazioni Siri e il lavoro non sarà esternalizzato.

I danni alla privacy degli utenti

L'uso di revisori in carne ed ossa da parte di **Apple**, **Google** e **Amazon** ha fatto storcere ai legislatori e alle autorità di regolamentazione negli Stati Uniti e in Europa. I difensori della privacy hanno espresso preoccupazione per il fatto che le pratiche delle aziende potrebbero violare i diritti degli utenti, in particolare nei casi in cui i dispositivi iniziano a registrare involontariamente o all'insaputa dell'utente.

Le scuse di Apple, quindi, al momento non bastano. Servono miglioramenti significativi, a partire innanzitutto, dal consenso degli utenti.

https://www.key4biz.it/siri-apple-chiede-scusa-agli-utenti-e-licenzia-300-dipendenti/268957/

Microsoft, dubbi dal Garante Privacy Olandese: ‘Windows 10 non rispetta il GDPR’

Microsoft sta raccogliendo da remoto i dati dagli utenti di **Windows 10**, in una potenziale violazione delle norme sulla privacy.

Lo ha affermato oggi l’agenzia olandese per la protezione dei dati (**DPA**) dichiarando di aver trovato le pratiche mentre stava testando le modifiche di protezione della privacy in Windows apportate l’anno scorso da **Microsoft** su richiesta dell’agenzia stessa.

Le nuove contestazioni sono figlie di un’indagine che era stata avviata nel 2017 e che ha indotto Microsoft a modificare il funzionamento della telemetria di Windows 10 a partire da aprile 2018.

“*Microsoft ha rispettato gli accordi conclusi*”, ha affermato il DPA in una nota. “*Tuttavia, il controllo ha anche messo in luce che Microsoft sta raccogliendo in remoto altri dati dagli utenti senza aver avuto il consenso dagli stessi. Di conseguenza, Microsoft è ancora potenzialmente in violazione delle norme sulla privacy.*“

Il regolatore olandese ha dichiarato di aver trasmesso i risultati alla sua controparte in Irlanda. Infatti il compito di indagare sulla questione spetta al Garante irlandese, visto che è proprio in Irlanda che Microsoft ha il suo quartier generale europeo.

Il DPC ha affermato che“*si impegnerà a breve con Microsoft per*

ottenere risposte sostanziali sulle preoccupazioni sollevate“.

L’azienda di **Redmont** dichiara di essere pronta a collaborare con le autorità per risolvere la questione il più in fretta possibile. Secondo le nuove regole del **GDPR**, una violazione può costare ad un’azienda fino al 4% del fatturato annuale in multe.

Microsoft ha già avuto un precedente in relazione alla telemetria di Windows 10: tra il 2016 e il 2017. Da quel momento l’azienda ha dichiarato di essersi impegnata a proteggere la privacy dei propri clienti e negli ultimi anni ha migliorato le funzionalità di sicurezza per utenti privati □□e piccole imprese di Windows 10.

https://www.key4biz.it/microsoft-dubbi-dal-garante-privacy-olandese-windows-10-non-rispetta-il-gdpr/268875/