



# FACCE, IMPRONTE E PRIVACY

Google, Facebook e il problema Gdpr. Dalle class action a una semplice email: le possibilità per tutelarsi

di Attilia Burke

**FINO A CHE PUNTO E COME** le grandi aziende che hanno a disposizione i dati biometrici dei propri utenti - dalle impronte digitali al riconoscimento facciale - possono usare queste informazioni?

In Usa questa domanda sta scatenando un vero e proprio putiferio e alcune leggi statali stanno mettendo in difficoltà colossi come Google e Facebook, che rischiano di dover pagare miliardi di dollari di risarcimenti. Ma l'Italia non è da meno: sono già in corso class action e tutelarsi - rispetto a quanto avviene negli Stati Uniti - è più facile, e non serve passare necessariamente per il tribunale. Ne ha parlato con Fortune Italia l'avvocato Melissa Marchese, dello studio Gianni, Origoni, Grippo & Partners, che da anni assiste società italiane e multinazionali nella gestione di aspetti di privacy e di informatica giuridica. Oltreoceano alcuni utenti americani hanno puntato il dito contro Google Foto, e in particolare

contro il tool che permette di creare in modo automatico gallerie di fotografie della stessa persona, grazie al riconoscimento facciale. Il colosso di Mountain View ha poi tirato un sospiro di sollievo quando un tribunale federale dell'Illinois ha stabilito che non doveva pagare i risarcimenti previsti nel caso in cui fosse stata ritenuta responsabile di aver infranto la legge - dai 1000 ai 5 mila dollari a utente 'leso'. In una sentenza di 28 pagine, il giudice distrettuale Edmond Chang, ha rilevato che benché Google avesse eseguito delle scansioni biometriche senza permesso, gli utenti non avevano subito danni e quindi non erano qualificati per il risarcimento. Diverso il discorso per Facebook che lo scorso anno ha perso un caso simile: oggetto della controversia, questa volta, lo strumento che permette di identificare le persone quando vengono caricate fotografie sul social - sempre attraverso l'analisi biometrica del viso.

Casi simili, sentenze opposte. Perché? La risposta giace in parte nei diversi modi con cui le aziende hanno utilizzato le scansioni. Google Foto è uno strumento che aiuta solo a organizzare le proprie, mentre i 'tag' di Facebook consentono a soggetti terzi di identificare le persone. Ma la normativa rimane fumosa e ora Fb si sta appellando, usando come riferimento il più recente caso Google.

Ben diversa la situazione in Italia dove, nel caso in cui un utente pensi che i propri dati vengano usati in modo improprio, onde evitare l'effetto 'Davide e Golia' in tribunale può rivolgersi, in primis, direttamente alla società: "è possibile chiedere direttamente all'azienda: che tipologie di informazioni hai su di me? E loro sono tenuti a darti tutti i dati e a spiegarti perché li trattano, a chi li comunicano, dove li conservano. E devono fornirteli anche in formato fisico, su un supporto durevole", spiega l'avvocato Marchese.

L'altra strada "è rivolgersi al Garante della privacy tramite email e quindi senza troppi costi e senza grande fatica - afferma l'esperta - Fare una segnalazione è semplice, è sufficiente scrivere: 'ho l'impressione che Google non rispetti le regole in materia di privacy nel trattamento dei miei dati biometrici'. E il Garante potrebbe mandare un'ispezione".

Sicuramente, può essere d'aiuto rivolgersi a un'associazione consumatori per intraprendere un'azione di gruppo. Altroconsumo, ad esempio, a ottobre ha ufficialmente avviato, presso il Tribunale di Milano, una class action contro

Facebook. Sono oltre 50mila gli utenti in Italia che, ad oggi, stanno chiedendo al big dei social i danni subiti in termini di mancato guadagno del consumatore, per lo sfruttamento economico dei propri dati e per l'indebito utilizzo di informazioni riservate e dei dati sensibili per finalità commerciali. Con la class action si richiede un risarcimento di 285 euro a iscritto per ogni anno di registrazione al social. Altroconsumo sta portando avanti l'iniziativa insieme ad altre organizzazioni di consumatori europee, per un totale, ad oggi, di oltre 170mila aderenti. In Italia, e in Europa, la class action in materia di privacy, "è una possibilità prevista nel Gdpr (General data protection regulation) - spiega Marchese - una via che prima dell'implementazione della legge europea sulla privacy lo scorso agosto, non era regolamentata".

Proprio a gennaio, la Francia ha inflitto la prima maxi-multa per violazione del Gdpr. Vittima Google che dovrà pagare 50 mln di euro. Tornando a Facebook, invece, il terreno per Mark Zuckerberg si è fatto ancor più scivoloso dopo la recente pubblicazione di un'inchiesta del New York Times, che coinvolge i tre quarti della Silicon Valley, e non solo. Pile di documenti e testimonianze dimostrano che Facebook ha condiviso i dati degli utenti - e non a gratis - con oltre 150 aziende, inclusi colossi quali Microsoft, Amazon e Yahoo. Addirittura, Spotify, Netflix e la Royal Bank of Canada, avrebbero avuto accesso alla messaggistica privata degli utenti. Il big dei social, per ora, sostiene di non aver infranto alcuna legge, e spiega come tali partner siano di fatto considerati delle vere e proprie 'estensioni' dell'azienda. I portavoce di Spotify e Netflix, invece, hanno rimarcato che non erano a conoscenza dei vasti poteri che Facebook aveva loro concesso. Mentre la Royal Bank ha negato il fatto che la banca fosse in possesso tali accessi. Uscire dal sentiero di mangrovie nel quale si sta avviluppando Facebook non sarà facile, e se negli Stati Uniti la mancanza di una regolamentazione sulla privacy potrebbe complicare ulteriormente la situazione, in Europa, in questo momento "siamo in una sorta di interregno perché il processo di adeguamento alle nuove norme sulla privacy non è concluso", spiega Marchese.

Cosa potrebbe succedere in Italia se qualcuno segnalasse problemi in termini di rispetto del trattamento dei dati biometrici, come avvenuto in Usa? "A mio parere il Garante della Privacy imporrebbe a Google e Fb il consenso: l'utente deve avere la possibilità di scegliere quali tipologie di dati vengono raccolte. Il dato biometrico non può essere mai imposto, non può esistere il trattamento di questa tipologia di dati senza consenso. In Italia, poi, verrà implementato un pilastro di garanzia ulteriore costituito dalle indicazioni fornite dall'Autorità Garante".

È dunque difficile stabilire se e quanto i colossi del web siano in linea con la normativa nostrana: "ci sono misure di sicurezza che già in passato erano state imposte dall'Autorità Garante che secondo me Google non applicherà mai, come ad esempio il divieto di creare banche dati centralizzate di tutte le informazioni biometriche. Io credo che tutti i dati biometrici siano collezionati in un unico data center. Va bene, saranno crittografati, però questo non è dato saperlo. Noi utenti vediamo solo l'informativa ed in genere quella di Google sui dati biometrici non è completa. Google, a mio parere, non ha mai chiesto un'autorizzazione all'Autorità Garante in tal senso, almeno che non l'abbia chiesta a livello europeo, ma non mi risulta". ■