Il riconoscimento facciale e la tutela della privacy come rapporto interpersonale

Date : 1 marzo 2018

Una delle novità con cui si è concluso il 2017 è stata, senz'altro, l'introduzione di nuove *features* sul social network Facebook. Il 19 dicembre, infatti, la piattaforma ha annunciato due importanti novità:

- un aggiornamento del sistema di suggerimento dei tag nelle fotografie;
- nuove tecnologie per il riconoscimento facciale rivolte, da un lato, ad agevolare utenti con difficoltà visive, dall'altro a depotenziare il numero dei furti di identità, di impersonificazione e di post fotografici a danno degli utenti ritratti che non hanno previamente acconsentito al caricamento delle immagini.

Si tratta, però, di due implementazioni che non sono state rese disponibili in Europa dove il riconoscimento facciale è assimilato alla biometria (i.e. dato biometrico) e, come tale, soggetto al divieto di trattamento di cui all'art. 9(1), GDPR. I dati biometrici, infatti, sono definiti come «*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*» (*ex* art. 4(14), GDPR).

Tuttavia, sarebbe interessante rileggere le nuove *features* di Facebook alla luce delle disposizioni del Regolamento privacy, che offre nuovi e ulteriori principi, quali la *data protection by-design*/*default* e l'*accountability*.

Innanzitutto, infatti, il Considerando 51 del GDPR ricorda che: «***Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica****, essendo inteso che l'utilizzo dei termini «origine razziale» nel presente regolamento non implica l'accettazione da parte dell'Unione di teorie che tentano di dimostrare l'esistenza di razze umane distinte.* ***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. *Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito nei casi specifici di cui al presente regolamento, tenendo conto del fatto che il diritto degli Stati membri può stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del presente regolamento ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Oltre ai requisiti specifici per tale trattamento, dovrebbero applicarsi i principi generali e altre norme del presente regolamento, in particolare per quanto riguarda le condizioni per il trattamento lecito. È opportuno prevedere espressamente deroghe al divieto generale di trattare tali categorie particolari di dati personali, tra l'altro se l'interessato esprime un* ***consenso esplicito*** *o in relazione a esigenze specifiche, in particolare se il trattamento è eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia* ***permettere l'esercizio delle libertà fondamentali***».

Diversi elementi fondamentali emergono da quanto riportato:

- la necessità di tutelare i dati personali sensibili, cioè maggiormente predisposti a violazioni di diritti e libertà fondamentali;
- la considerazione del trattamento di fotografie attraverso un dispositivo tecnico specifico come un dato sensibile, poiché in tal caso vi è identificazione univoca o autenticazione di una persona fisica;
- il consenso esplicito dell'interessato costituisce deroga al divieto generale di trattare dati sensibili salvo diversa disposizione nazionale che vieti ;
- se il trattamento svolto ha la finalità di permettere l'esercizio delle libertà fondamentali, esso è consentito qualora a compierlo siano associazioni o fondazioni.

Trasportando tali elementi nel panorama attuale degli illeciti online commessi in violazione delle libertà fondamentali di alcuni utenti, si possono formulare alcune interessanti riflessioni.

Ad esempio, se sul punto 1) non vi è alcuna aggiunta da fare, più interessante è la combinazione dei punti 2) e 3). Stante il requisito del consenso *ex* art. 9(2)(a), il riconoscimento facciale per la prevenzione del furto di identità, di fenomeni di cyberbullismo e di *revenge porn* potrebbe essere inteso come un trattamento la cui finalità è quella di permettere l'esercizio delle libertà fondamentali, tra cui proprio la protezione dei dati personali dell'interessato. Infatti, sempre più di frequente chi utilizza i social network posta foto/video non solo senza il consenso dell'interessato, ma anche con finalità che ne compromettono la dignità, anche a sua insaputa.

Inoltre, fenomeni quali il furto di identità e l'impersonificazione sono assai diffusi tra coloro che, per adescare i più giovani, utilizzano foto di profili altrui per costruire una *fake identity* che sia credibile per la vittima.

È interessante, dunque, come il requisito del consenso di cui al punto 3) acquisisca due diversi volti: da un lato esso è ovviamente premessa della tutela dei dati sensibili (i.e. fotografie trattate attraverso un dispositivo tecnico specifico) rispetto all'uso che ne potrebbe fare il social network. Dall'altro, però, il consenso prestato al social per indagare sulle immagini

dell’interessato presenti sui suoi server diviene anche una funzionalità (i.e. *feature*) grazie alla quale individuare tutte quelle situazioni in cui i dati dell’interessato sono stati utilizzati da altri utenti (e non dal social stesso) senza il suo consenso.

Internet, infatti, costringe a ripensare il concetto di “sfera personale”, poiché essa non riguarda più solo la privatezza effettuata per scelta (“*non rendo visibile a tutti questo contenuto che mi riguarda*”), ma richiede di fare attenzione anche ad altri due elementi: ciò che gli altri possono rendere pubblico su di noi e ciò che riguarda altre persone e che inconsapevolmente (o consapevolmente) pubblichiamo senza il loro consenso.

La privacy, oggi, non è più solo qualcosa di personale (“*le mie impostazioni privacy*”) ma è un rapporto interpersonale (“*cosa succede se questa informazione su di me viene resa pubblica da qualcun altro senza che io sia d’accordo? Cosa succede se rendo pubblica questa informazione su qualcun altro senza il suo consenso?*”). Non è più solo la scelta dell’interessato di condividere o meno qualcosa, ma è anche la decisione del soggetto terzo di rispettarne la privacy e di chiedere il suo consenso alla pubblicazione di informazioni o materiali che lo riguardano. uestoQu

Ciò premesso, è cosa certa che, in applicazione dell’art. 35, GDPR debba essere effettuata una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio. Tuttavia, dal momento che due dei principi cardine del Regolamento privacy sono la *data protection by design/default* e l’*accountability*, la valutazione di impatto dovrebbe andare a indagare soprattutto le misure più opportune per attenuare tale rischio, implementando i principi di minimizzazione e proporzionalità direttamente nel “*dispositivo tecnico specifico che consente l'identificazione univoca*”. Nel Parere 3/2012 sugli sviluppi nelle tecnologie biometriche, il Gruppo Art. 29 utilizza proprio il caso dei social network: “*Le fotografie su internet, nei media sociali, nelle applicazioni on-line per la gestione o la condivisione di fotografie non possono essere oggetto di ulteriori trattamenti al fine dell’estrazione di modelli biometrici o dell’iscrizione in un sistema biometrico per il riconoscimento automatico delle persone basato sulle immagini (riconoscimento del volto) in assenza di una specifica base giuridica (il consenso, per esempio) per questa nuova finalità. In presenza di una base giuridica per tale finalità accessoria, il trattamento dev’essere inoltre adeguato, pertinente e non eccedente rispetto a tale finalità. Qualora una persona interessata abbia fornito il proprio consenso al trattamento delle fotografie in cui essa compare per essere automaticamente associata a un album di fotografie online con un algoritmo per il riconoscimento del volto, questo trattamento dev’essere effettuato in un modo che tenga conto della protezione dei dati: una volta che nome, pseudonimo o altro testo specificato dall’interessato sono stati associati alle immagini, i dati biometrici non più necessari vanno cancellati. La creazione di una banca di dati biometrici permanente non è necessaria a priori per questa finalità*”. È dunque ammissibile che avvenga una “*iscrizione in un sistema biometrico per il riconoscimento automatico delle persone basato sulle immagini (riconoscimento del volto)*” se questa si basa sul consenso dell’interessato.

Nel caso di Facebook, ad esempio, è stato creato un tasto on/off per consentire/interrompere il riconoscimento facciale nelle immagini (compreso quello nelle immagini caricate dall’utente stesso). Potrebbe definirsi come una sorta di meccanismo di consenso, anche se embrionale,

che dovrebbe poi essere integrato con una corretta informativa circa le finalità di trattamento, le modalità, i termini di conservazione dei dati e il fondamentale diritto di revoca del consenso assieme a tutte le altre informazioni di cui all'art. 13, GDPR. Il modo in cui l'identificazione facciale è concepita riflette così i due volti della privacy: da un lato essa si basa sulla volontà del singolo di essere identificato a partire da caratteristiche univoche del viso che gli appartengono (consenso come strumento di tutela della privacy). Dall'altro, essa deve garantire che l'identificazione della persona abbia un'elevata probabilità di corrispondenza – per evitare che la funzionalità metta a disposizione di un utente immagini appartenenti ad altri utenti a lui somiglianti (privacy come rapporto interpersonale).

Il punto fondamentale rimane quello di rendere sicuro l'uso di dati biometrici per finalità di identificazione in grandi banche dati centralizzate, andando a fare leva sul principio di *accountability* e *data protection by default*, includendo nella valutazione di impatto tutti quegli elementi volti a dimostrare che il trattamento viene effettuato solo mediante l'utilizzo di dati necessari e indispensabili per la finalità di cui l'interessato è stato informato. I dati biometrici, però, contengono spesso più informazioni di quelle richieste per il raggiungimento delle finalità prestabilite. Le fotografie, ad esempio, possono rivelare informazioni sull'origine etnica, la religione, lo stato di salute. Ecco perché è importante costruire uno strumento di riconoscimento del volto che minimizzi i dati, trattando e conservando solo quei dettagli necessari a compiere l'identificazione fotografica. Così, ad esempio, qualora l'utente decida di disattivare la funzionalità (off), il titolare del trattamento (cioè il social network) dovrebbe eliminare in maniera efficace tutti i collegamenti all'identità creati durante l'attivazione della funzione. A ogni nuova attivazione (on), il sistema potrà procedere a una nuova analisi biometrica per rintracciare le fotografie in cui l'utente compare. Forse la ripetizione del procedimento ad ogni riattivazione del servizio può risultare macchinosa, ma perimetrare il riconoscimento facciale *by design* e incastonarlo nella base giuridica del consenso significa costruire una *feature* che incorpora e applica i principi della protezione dei dati, andando poi ad intervenire su situazioni in cui manca la base giuridica del consenso dell'interessato – come quelle costituite da furto di identità o da post fotografici indesiderati.

A cura di: **Camilla Bistolfi**