Riconoscimento facciale, adottate dal Consiglio d'Europa le Linee Guida sull'uso corretto delle tecnologie

Avv. Maria Cupolo | consulente esperto Privacy & Data Privacy Officer | docente di securindex formazione

In un momento in cui l'opinione pubblica pare accorgersi dei rischi delle tecnologie per il riconoscimento facciale per la privacy delle persone, il Comitato Consultivo della Convenzione 108 presso il Consiglio d'Europa ha adottato delle Linee Guida sull'utilizzo di queste tecnologie. Può riassumere i punti cardine?

Il 28 gennaio 2021, nella Giornata europea per la protezione dei dati, il Comitato Consultivo della **Convenzione 108**, istituito presso il Consiglio d'Europa, ha adottato le Linee Guida che si fondano sui principi della Convenzione 108 e forniscono una serie di misure di riferimento che governi, sviluppatori di **sistemi di riconoscimento facciale**, produttori, aziende e pubbliche amministrazioni dovrebbero adottare per garantire che l'impiego di queste tecnologie non pregiudichi la **dignità della persona, i diritti umani e le libertà fondamentali**.

L'uso della biometria accentua difatti il problema della proporzionalità dei dati trattati alla luce delle finalità del trattamento.

Nell'analisi della proporzionalità di un sistema biometrico, la prima considerazione da svolgere è se il sistema sia inevitabile per soddisfare la necessità accertata, ovvero se sia essenziale per soddisfare tale necessità o, piuttosto, sia il più conveniente o più efficace sotto il profilo dei costi.

Occorre una valutazione di impatto in presenza di un tipo di trattamento come la biometria del volto, che prevede l'uso di nuove tecnologie e che, considerati la natura, l'oggetto, il contesto e le finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Inoltre, è necessaria l'implementazione di misure di sicurezza adeguate, in ossequio al principio di "privacy by design".

Le Linee Guida esprimono particolare preoccupazione riguardo ai rischi derivanti dal riconoscimento facciale volto a rilevare i tratti della personalità, i sentimenti o le reazioni emotive dall'immagine del volto: le cosiddette tecnologie di "riconoscimento dell'affetto".

Le aziende e le pubbliche amministrazioni hanno l'obbligo di garantire il rispetto dei principi di protezione dati, compresa la necessità di effettuare una valutazione dei rischi, tenuto conto della tutela dei diritti e anche di tutti i profili etici che ne possano derivare.

Le persone devono, inoltre, poter esercitare i propri diritti, compreso quello di rettifica (ad esempio, in presenza di false corrispondenze) o quello di non essere sottoposto a decisioni puramente automatizzate senza che la propria opinione sia adeguatamente considerata.

L'uso di sistemi di riconoscimento facciale da parte delle forze dell'ordine dovrebbe essere consentito solo quando è strettamente necessario per prevenire un rischio imminente e grave alla sicurezza pubblica.
Le Linee Guida raccomandano inoltre agli sviluppatori di tecnologie di riconoscimento facciale di prestare specifica attenzione all'attendibilità degli algoritmi e all'accuratezza dei dati trattati, al fine di evitare disparità e possibili ricadute discriminatorie.
In particolare, a chi sviluppa è richiesto un approccio trasparente e di:

- Integrare la protezione dei dati nelle fasi di progettazione e di architettura di prodotti e servizi di riconoscimento facciale così come nei sistemi informatici interni, e inserire l'uso di strumenti dedicati, inclusa la cancellazione automatica di dati grezzi ovvero non elaborati dopo l'estrazione di modelli biometrici;
- Offrire un determinato livello di flessibilità nella progettazione di queste tecnologie al fine di adeguare le garanzie tecniche ai principi di limitazione delle finalità, di minimizzazione e di limitazione della conservazione dei dati;
- Implementare un processo di revisione interna progettato per identificare e mitigare i possibili effetti sui diritti e sulle libertà fondamentali prima che le tecnologie di riconoscimento facciale siano rese disponibili;
- Integrare l'approccio della protezione dei dati nel proprio modello organizzativo, ad esempio con personale dedicato ed adeguatamente formato, effettuando analisi di impatto e dei rischi possibili nelle fasi di sviluppo, modifica o integrazione di prodotti, soluzioni e servizi che riguardino il riconoscimento facciale.

Per arrivare a provvedimenti legislativi che definiscano i limiti dell'uso lecito e sanciscano gli usi illeciti quali altri passaggi saranno necessari?
Sarà necessario regolamentare il più possibile e saranno necessari comitati di esperti indipendenti, soprattutto quando ci possono essere aspetti anche etici da prendere in considerazione. Occorre riconoscere infatti i pericoli che possono derivare da tecniche particolarmente invasive e saranno fondamentali sia un dibattito pubblico che un approccio di tipo precauzionale
È dunque richiesto l'impegno da parte dei Legislatori al fine di implementare le garanzie e le tutele richiamate, così come è richiesto l'intervento delle Autorità di protezione dei dati che devono essere consultate riguardo a proposte legislative ed amministrative che comportino il trattamento dei dati personali mediante tecnologie di riconoscimento facciale.
Le Autorità debbono essere consultate prima di possibili sperimentazioni o utilizzi.

Riconoscimento facciale e tutela dei dati biometrici dalla parte della privacy, data breach e cybersecurity sul fronte del perimetro cibernetico nazionale: quali relazioni si possono cogliere tra due scenari all'apparenza distanti ma che, in questa fase, sembrano sovrapporsi?
Se pensiamo alla normativa vigente e alla strada aperta dalla direttiva NIS e dal Perimetro Cibernetico, non possiamo che rilevare come oggi l'obiettivo sia la sicurezza nazionale: garantire cioè i servizi e le attività critiche ed essenziali per il Sistema Paese attraverso un modello basato su misure di carattere tecnico ed organizzativo, dove la scelta di soluzioni e sistemi sempre più performanti e soprattutto sicuri deve essere una priorità.
L'interesse pertanto è certamente quello di costruire un modello che non deleghi alla tecnologia in maniera assoluta ma che ponga questa come una risorsa, andando a prendere in considerazione i temi legati alla sicurezza di reti, infrastrutture, sistemi informativi così come degli asset in ambito ICT, con uno sguardo attento anche alla tutela dei diritti, dignità e libertà degli individui con riferimento alla protezione dei dati personali e, dunque, dei dati biometrici coinvolti quando si parla di riconoscimento facciale.
È fondamentale adottare soluzioni che siano in grado di fornire adeguate misure contro i rischi possibili di perdita di disponibilità, integrità o riservatezza dei dati e delle informazioni, avuto riguardo alla tipologia ed alla quantità degli stessi, alla loro sensibilità ed allo scopo cui sono destinati.
Etica, fiducia, responsabilizzazione e trasparenza: questi aspetti concorrono tutti verso un modello di resilienza e tutela in termini non solo di sicurezza quanto agli asset, alle soluzioni sviluppate e adottate ma, anche, quanto alla tutela e protezione dei diritti e libertà degli individui.