DIRITTI COMPARATI
Comparare i diritti fondamentali in Europa

RICONOSCIMENTO FACCIALE E PROTEZIONE DATI: ATTENZIONE AL PUNTO DI NON RITORNO

Posted on 30 Gennaio 2020 by Federica Resta , Oreste Pollicino

Al dibattito sul riconoscimento facciale è sottesa, indubbiamente, una grande questione "di merito": stabilire in che termini siano legittimi la raccolta e l'utilizzazione, per le più varie finalità, di dati personali annoverati, dalla disciplina europea, tra quelli meritevoli di una tutela rafforzata. E questo in ragione della loro particolare attinenza alla persona e al suo vissuto e della loro idoneità, in caso di uso scorretto, a esporre il soggetto a discriminazioni o a forme, tra le più di diverse, di stigmatizzazione. Tale è il grado di protezione accordato a questa tipologia di dati, che il Regolamento generale sulla protezione dati ne sancisce in prima istanza il divieto di trattamento, derogabile solo in presenza di determinati, tassativi presupposti, espressivi di quella "funzione sociale" della protezione dati che il Regolamento stesso valorizza, nella consapevolezza di come nessun diritto possa essere "tiranno", come affermò, sia pur in contesto diverso, la Consulta sul caso Ilva (sent. n. 85 del 2013).

Ma in questo dibattito c'è in gioco qualcosa di più e di più importante: la definizione del katechon, il limite, cioè, che l'uomo deve saper (op)porre alla tecnica, il diritto al potere (privato, oltre che pubblico), la democrazia all'ideologia del controllo. Limite che tende fatalmente a spostarsi sempre

più avanti, sotto la duplice spinta di una lex mercatoria orfana dei suoi antichi confini (sociali e giuridici, prima che territoriali) e di una concezione tirannica della sicurezza, ben diversa da quella irenica delineata dalla Carta di Nizza, quale complementare e non antitetica alla libertà. Ed a questa progressiva erosione del limite (op)posto alla sinergia di tecnica e potere concorre, in misura determinante, la tendenza sempre più marcata alla delega, all'algoritmo, di attività, de-cisioni, persino valutazioni, per le quali la razionalità umana appare, paradossalmente, insufficiente, inadeguata, cedevole a chissà quali collusioni, "antiquata", per riprendere la provocazione di Guenther Anders (del 1956!).

Non stupirà, dunque, il progressivo incremento nel ricorso al riconoscimento facciale negli ambiti più diversi: se in Cina costituisce la regola del "vivere in pubblico" e se lo si è usato persino in alcune scuole, per analizzare le reazioni degli studenti alle lezioni, Singapore sta costruendo un sistema di riconoscimento facciale per i servizi governativi, mentre l'India utilizza scansioni dell'iride come parte del suo sistema di identità nazionale Aadhaar.
Ed in Europa, in cui il GDPR, prima menzionato non solo sancisce, come si diceva in apertura, un divieto al trattamento di dati biometrici, consentendo solo alcune eccezioni da interpretare in modo assai restrittivo?
Ebbene, nel vecchio continente, pur rappresentando una tecnica dall'uso ancora limitato, la tecnologia in questione va comunque sempre più diffondendosi. Significativo, in tal senso, che una scuola svedese lo abbia utilizzato per agevolare il controllo degli ingressi e delle uscite degli studenti (l'Autorità di protezione dati ha espressamente sanzionato tale trattamento di dati), che se ne faccia uso nella stazione londinese King's Cross e che, da noi, ne sia prossima la sperimentazione in alcuni aeroporti, mentre lo si auspichi da più parti per fini di gestione dell'ordine pubblico nel contesto, tutto particolare, degli stadi.
A livello più ampio, la Francia potrebbe essere il primo Paese dell'Unione europea ad implementare un sistema di riconoscimento facciale finalizzato alla creazione di una identità digitale diffusa a tutta la cittadinanza. Infatti con l'obiettivo dichiarato di rendere la nazione più

sicura ed efficiente, il governo transalpino ha nei mesi scorsi rilasciato un programma di identificazione, in versione test, chiamato Alicem. Dopo l'annuncio da parte del Presidente Macron del lancio di Alicem, la Commissione nazionale per l'informatica (Cnil) ha subito avvertito che un sistema del genere violerebbe la normativa europea in materia di consenso sul possesso e utilizzo dei dati personali e sensibili. Si configurerebbe, infatti, un progetto di identità digitale fondato su un dispositivo di riconoscimento facciale obbligatorio ai fini della fruizione del servizio stesso, rendendo dunque il consenso al trattamento dei dati invalido perché non libero, indebitamente condizionato dal fine di poter fruire del sistema d'identità digitale che non ammette alternative. E proprio il tema della effettiva libertà del consenso - oltre alla non completa sicurezza e resilienza informatica - è al centro del ricorso avanzato da La Quadrature du Net al Consiglio di Stato francese, per l'annullamento del decreto che prefigura tale sistema di identificazione, correlato all'applicazione Alicem.
La varietà degli usi ai quali il riconoscimento facciale può prestarsi dimostra come la valutazione della sua ammissibilità non possa prescindere dalla considerazione attenta dello specifico contesto, delle finalità e delle implicazioni che esso può determinare.
Se infatti, in alcuni ambiti (ad es. indagini di polizia o giudiziarie di una certa complessità) il ricorso, circoscritto e assistito da tutte le garanzie necessarie, a tale tecnologia può fornire un contributo difficilmente conseguibile altrimenti, in altri contesti - e soprattutto se concepito in chiave meramente agevolatoria di attività ben realizzabili in altro modo (ad es. per controllare l'uscita degli studenti)- esso può invece risolversi in un'ingiustificata (perché, appunto, sproporzionata) limitazione dei diritti individuali.
Di più. Il ricorso diffuso a queste tecniche in circostanze "ordinarie" e a meri fini agevolatori, rischia di indurre una sottovalutazione collettiva dell'invasività di simili misure: il pericolo non è tanto quello del "pendio scivoloso", quanto di un'acritica e poco consapevole accettazione sociale di una progressiva perdita di libertà (profilo, questo, su cui può leggersi un'acuta riflessione dell'European Data Protection Supervisor,Wojciech

Wiewiórowski, https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en, volta a sottolineare anche l'esigenza del vaglio della necessità della misura).

Tale rischio è particolarmente significativo ogniqualvolta il ricorso alla biometria, soprattutto, appunto, "facilitativa" sia legittimato sulla base del mero consenso, benché esplicito, del soggetto, in quanto una generale assuefazione a questo tipo di misure può indurre a sottovalutarne le implicazioni, dirette e non: dalla ubiquitaria geolocalizzazione consentita a chi detenga l'immagine del volto altrui, alla facile profilazione, sempre più incisiva e penetrante grazie alle applicazioni dell'intelligenza artificiale. Il tutto, in un contesto di generale asimmetria informativa tra soggetto passivo e attivo della raccolta dei dati, tale per cui il primo spesso non comprende effettivamente (per inerzia o difficoltà reale) le implicazioni del suo consenso, condannandosi inconsapevolmente a dissimulate "servitù volontarie". Anzi, quello dell'asimmetria cognitiva rispetto alle tecnologie rappresenta il terreno su cui le tradizionali diseguaglianze rischiano di ripresentarsi in forma tanto più incisiva quanto più sottile, lasciando alla tecnica il dominio della "nuda vita" di chi non possa comprenderne la potenza.

Ma quello della sottovalutazione dell'impatto di simili tecnologie è un rischio che, sia pur in misura minore, si corre anche rispetto al loro uso previsto dalla legge, generalmente per fini di prevenzione e accertamento dei reati. Le garanzie imposte, in questi casi, dalla disciplina europea e nazionale sono indubbiamente significative e contemplano anche elevate sanzioni penali nell'ipotesi di profilazione discriminatoria basata su dati, quali quelli biometrici, particolarmente sensibili.

Sarà dunque determinante, in questo senso, il rispetto, da parte delle norme che di volta in volta legittimino il ricorso a tali misure, dei principi di necessità e proporzionalità, su cui le Corti di Lussemburgo e Strasburgo, ma anche la nostra Corte costituzionale, hanno sinora fondato un rapporto armonico tra libertà e sicurezza. E' questo il più solido argine alla tendenza a rendere il panottismo il principale modello di controllo sociale e gestione della devianza o, persino, dell'ordine pubblico.

Per questo la soluzione, in discussione presso la Commissione europea, di una moratoria nel ricorso al riconoscimento facciale nei luoghi pubblici, per un periodo compreso tra tre e cinque anni pur con deroghe che è bene siano adeguatamente circoscritte- costituirebbe una decisione di rilevanza determinante, per una duplice ragione.

Da un lato, infatti, è particolarmente importante che tale scelta sia motivata in base all'esigenza di verificare il reale impatto di simili tecnologie e, solo all'esito, valutarne con maggiore consapevolezza la sostenibilità sociale, etica e, quindi, giuridica. Un'espressione, particolarmente rilevante, di quel principio di precauzione che non a caso, nel pensiero di un grande filosofo come Hans Jonas, è strettamente correlato al "coraggio della responsabilità".

Per altro verso, una simile scelta contribuirebbe a consolidare quel particolare profilo identitario che l'Europa sta progressivamente affermando sul terreno del rapporto tra diritto e tecnica, tentando di rimodularlo in chiave antropocentrica, perché il "destino dell'Occidente" non contraddica, con la cronaca, la propria storia (su questi temi, vds. A. Soro, Democrazia e potere dei dati, Baldini & Castoldi, 2019).

E l'Angelus Novus, insegna Walter Benjamin, non distoglie lo sguardo da ciò da cui, fatalmente, si allontana.