Dati rilevati dagli Enti certificatori o autocertificati
Tiratura: n.d.
Diffusione 09/2020: 200.000
Lettori: n.d.
Quotidiano - Ed. nazionale

Domani

Dir. Resp.: Stefano Feltri

19-NOV-2020
da pag. 12
foglio 1 / 3
www.datastampa.it

GRANDE FRATELLO

Le nostre facce sono già schedate Ma la sorveglianza è senza legge

PHILIP DI SALVO
ricercatore

Uscendo dalla stazione di Como San Giovanni si attraversa un parco pubblico poco frequentato. Dallo scorso anno quell'area ospita un sistema di videosorveglianza in grado di riconoscere i volti di chi la attraversa, a fini investigativi e di sicurezza. Il fatto che la città, una delle più sicure in Italia, abbia dovuto interrompere l'uso del riconoscimento facciale per assenza di paletti di legge chiari è un elemento chiave per capire come questa tecnologia, che apre diversi scenari sinistri di sorveglianza indiscriminata, stia progressivamente diventando una realtà normalizzata delle nostre vite quotidiane. Il riconoscimento facciale è una tecnologia assai controversa e contestata da attivisti e accademia per la sua invasività, per questioni di sicurezza in relazione ai dati biometrici che raccoglie e per l'assenza di linee guida di legge chiare che possano regolamentarne o limitarne l'utilizzo. In un intervento su Nature, Kate Crawford, cofondatrice del centro studi AI Now di New York, ha scritto: «Noi accademici abbiamo fatto notare i rischi sociali e tecnici del riconoscimento per anni. Ci servono salvaguardie legali più forti che possano mettere al sicuro i diritti civili, la accountability e la correttezza. Altrimenti, questa tecnologia ci renderà tutti meno liberi».

Il riconoscimento facciale è già una realtà presente nonché uno dei terreni di battaglia tecnologici più accesi. Il concetto dietro questa tecnologia è all'apparenza semplice: abbinare alla videosorveglianza le potenzialità degli algoritmi di *machine learning*, connettendo quanto viene ripreso dagli occhi elettronici a volti umani già precedentemente raccolti in vari database, per combinare i due e, letteralmente, assegnare un'identità a chi viene ripreso. Le applicazioni sono di varia natura: sbloccare gli smartphone velocemente, salire a bordo di un aereo senza interagire con esseri umani, pagare prodotti e servizi con un selfie. Al contempo, sta diventando una delle tecnologie più utilizzate da governi, agenzie di intelligence e forze dell'ordine per monitorare gli spazi pubblici e attuare varie forme di sorveglianza. Non si parla di semplice videosorveglianza, a cui si è avvezzi da decenni. Il riconoscimento è molto più invasivo, raccoglie e analizza dati biometrici molto più sensibili, mettendo in essere un potenziale stato di costante sorveglianza e di identificazione automatizzata dei cittadini. Esiste, inoltre, ben poca trasparenza su come vengano riempiti i database su cui lavorano i sistemi di *facial recognition*: quali criteri potrebbero portarci a finire su una lista nera? Dobbiamo dare per scontata la possibilità di essere considerati tutti potenziali criminali?

Algoritmi razzisti

La letteratura scientifica da tempo si concentra su aspetti profondamente controversi del riconoscimento: la reale efficacia per finalità anti crimine o anti terrorismo e la natura inerentemente propensa a riprodurre in fase di progettazione i *bias* — inclinazioni — cognitivi umani di varia natura, a cominciare da quelli razziali. Negli Stati Uniti, il National Institute of Standards and Technology ha testato 189 algoritmi utilizzati da questa tecnologia e messi in commercio da 99 produttori: i risultati hanno mostrato come la maggioranza di questi sistemi tenda a identificare erroneamente afroamericani e altre minoranze con un rapporto dalle 10 alle 100 volte più frequente che per i bianchi. Non succede solo in laboratorio: Kashmir Hill sul New York Times a giugno ha raccontato la storia di Robert Julian-Borchak Williams, un 42enne afroamericano dell'area di Detroit, arrestato per furto perché erroneamente "riconosciuto" da un sistema di riconoscimento facciale. Uno studio curato dalla ricercatrice del Media Lab del Mit, Joy Buolamwini, nel 2018 considerava i sistemi di *facial recognition* di Microsoft, Ibm, e la cinese Megvii, riscontrando anche *bias* importanti in relazione all'identità di genere: i software identificavano correttamente il genere dei maschi bianchi nella maggior parte dei casi, ma erano molto più imprecisi quando si trattava di identificare persone di colore, in particolare donne. Lo scorso giugno, mentre infuriavano le proteste anti razziste, Amazon aveva annunciato di voler cessare la vendita del suo software Rekognition alle forze di polizia per un anno, in risposta alle accuse. Una mossa a cui erano seguite altre simili da parte di Ibm e Microsoft. Secondo la ong statunitense Fight for the Future queste sarebbero però solo mosse di pubbliche relazioni: è noto, ad esempio, come Amazon abbia venduto la sua tecnologia anche alla Immigration and Customs Enforcement (Ice) — una delle agenzie più controverse dal punto di vista dei diritti umani e delle loro violazioni lungo i confini Usa — e a un numero imprecisato di forze di polizia.

Le regole

In Europa, l'uso del riconoscimento facciale ricade sotto i principi contenuti nel regolamento sulla protezione dei dati (Gdpr) e nella Law Enforcement Directive. Dice Ioannis Kouvakas di Privacy International: «È difficile pensare che il riconoscimento possa rispettarli. Questa tecnologia non può, in nessun caso, rispettare i principi di necessità e proporzionalità: è estremamente invasiva. Potrebbe cambiare la democrazia per come la conosciamo». In molti paesi, Italia compresa, mancano, però, framework legali chiari e l'applicazione del riconoscimento negli spazi pubblici avviene spesso in un limbo di regolamentazione, il che tende a generare abusi. Negli Usa, diverse città hanno preso decisioni unilaterali e autonome, mettendo completamente al bando il riconoscimento: è successo a Boston, San Francisco e Portland. A inizio 2020, una bozza di *white paper* della Commissione Ue sull'intelligenza artificiale sembrava suggerire la possibilità di valutare una moratoria di cinque anni sull'utilizzo del riconoscimento facciale sul territorio europeo. La prospettiva è stata però accantonata nella versione finale del paper: niente moratoria. Sul fronte dell'attivismo, qualcosa si muove anche in Europa: la campagna ReclaimYourFace.eu, lanciata da una coalizione di ong la scorsa settimana, chiede ora una messa al bando della sorveglianza biometrica.

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura: n.d.
Diffusione 09/2020: 200.000
Lettori: n.d.
Quotidiano - Ed. nazionale

Domani

Dir. Resp.: Stefano Feltri

19-NOV-2020
da pag. 12
foglio 2 / 3
www.datastampa.it

Sorveglianza nostrana

Chi scrive, comasco, ha collaborato con Laura Carrer e Riccardo Coluccini a un'inchiesta pubblicata da Wired a giugno e interamente basata su una richiesta Foia, dedicata al sistema installato a Como. L'inchiesta ha attivato il garante della privacy che ha costretto il comune a spegnere le funzionalità di facial recognition, ricordando l'assenza di una legge nazionale specifica che ne regolamentasse l'uso. Nonostante l'ingiunzione, il comune ha comunque installato e testato ad agosto altre telecamere — che non può usare — e che hanno persino fallito i test voluti dalla stessa amministrazione. Soldi pubblici spesi inutilmente per una tecnologia inutilizzabile, acquistata con leggerezza, su spinta dei produttori privati e senza considerare nessun aspetto critico. «Purtroppo spesso prevale sia negli operatori privati che tra le pubbliche autorità un'insana fascinazione per un soluzionismo tecnologico apparentemente economico, smart e sexy che porta a piazzare telecamere dappertutto con la convinzione di ridurre criminalità, ma generando unicamente ulteriore disagio ed emarginazione», dice l'avvocato e fellow del Nexa Center for Internet & Society Carlo Blengino. A mancare è «una consapevolezza nei decisori delle conseguenze di trattamenti massivi di tal tipo. Che poi le attuali regole discendenti dal diritto fondamentale alla privacy siano adeguate a regolare pienamente il riconoscimento è più complesso». In seguito all'inchiesta, il caso di Como è approdato in parlamento.

Anche la polizia di stato si è dotata, senza alcun dibattito pubblico, già nel 2017 del *facial recognition* su vari livelli, compreso il sistema Sari Real-Time, attorno al quale esiste pochissima trasparenza. È sempre più chiaro, quindi, come una tecnologia tanto controversa e potenzialmente lesiva dei diritti di tutti venga presa in considerazione, implementata e testata senza le forme di controlli e contrappesi democratici che invece sarebbero dovuti e urgenti. Nessuna tecnologia è un destino e nessuno scenario di uso è ineluttabile. Occorre vigilare affinché la legittima richiesta di sicurezza non sfoci in violazioni o sospensioni dei diritti.

L'autore

Philip Di Salvo è ricercatore post-doc presso l'Istituto di media e giornalismo dell'Università della Svizzera italiana di Lugano, dove fa ricerca e insegna nell'ambito del giornalismo investigativo e dei rapporti tra informazione e hacking. Il suo ultimo libro in italiano è *Leaks. Whistleblowing e hacking nell'età senza segreti* (Luiss University Press)

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura: n.d.
Diffusione 09/2020: 200.000
Lettori: n.d.
Quotidiano - Ed. nazionale

Domani

Dir. Resp.: Stefano Feltri

19-NOV-2020
da pag. 12
foglio 3 / 3
www.datastampa.it

Il comune di Como ha installato un sistema *di sorveglianza facciale senza tener conto delle criticità. Manca un dibattito sul tema*
ILLUSTRAZIONE DI DARIO CAMPAGNA