Grande fratello e Ia si alleano Per sorvegliarti

ALESSANDRO DE PASCALE

Oltre 35mila. È il numero di telecamere a circuito chiuso statali installate negli spazi pubblici in Ungheria. In altre nazioni europee sono molte di più: circa 5,2 milioni quelle nel Regno Unito, dove ogni cittadino può venire ripreso fino a 70 volte al giorno. Soltanto a Londra gli occhi elettronici sarebbero almeno 627mila, all'incirca uno ogni 14 abitanti. A Roma, per avere un metro di paragone, c'è una telecamera ogni 250 residenti, contando le mille nuove per il Giubileo 2025 del progetto Smart Police Support. Quelle a circuito chiuso pubbliche ungheresi usano dal 2019 il sistema centralizzato di riconoscimento facciale Dragonfly, che raccoglie dati biometrici e consente alla polizia di identificare le persone dai loro volti. «Se a una sala di controllo sono collegate 50 telecamere, il sorvegliante potrà al massimo vederne 4 o 5, non tutte contemporaneamente. L'intelligenza artificiale supera questo limite operativo non perdendo nemmeno un frame», ricorda **Francesco Arruzzoli**, responsabile del Centro Studi Cyber Defense di Cerbeyra, realtà italiana da oltre vent'anni attiva nel campo dell'Information e Communications Technology. Il 18 marzo il partito del premier ungherese **Viktor Orbán** ha fatto approvare una legge a tutela dei minori che vieta i pride della comunità Lgbt (il prossimo è in programma a giugno), prevede sanzioni fino a 500 euro per coloro che vi prendono parte e propone di utilizzare il riconoscimento facciale per identificare i partecipanti.

I sistemi di riconoscimento facciale con l'intelligenza artificiale si diffondono tra le forze dell'ordine in Europa. E la nuova normativa lascia spazio agli abusi

Lo scorso 2 febbraio nell'Unione europea è entrato in vigore il tanto atteso regolamento comunitario sull'intelligenza artificiale, nonché il primo di questo tipo al mondo. «L'Ai Act è basato sui rischi e non sui diritti delle persone», chiarisce subito **Antonella Napolitano** dell'Hermes Center for Transparency, Digital & Human Rights, un'organizzazione dedita alla difesa dei diritti umani nello spazio digitale. Frutto di due anni di trattative segrete tra Stati, le maglie del provvedimento sarebbero state allentate su richiesta della Francia, la quale sarebbe poi stata fiancheggiata da Italia, Finlandia, Ungheria, Romania, Svezia, Repubblica Ceca, Lituania e Bulgaria. «Sarà così possibile usare il riconoscimento facciale in tempo reale per 16 reati e non solo per i crimini maggiori come terrorismo o criminalità organizzata», ricorda Napolitano. Uno Stato potrà inoltre ricorrervi per non meglio specificati motivi di sicurezza nazionale. L'Italia aveva già provato ad adottare applicazioni di questo tipo: il Sari Real-Time acquistato dal ministero dell'Interno, collegato a una banca dati in grado di contenere fino a 10mila volti ma mai en-

Foto: J. Cros – NurPhoto / Getty Images

CONTROLLATI
Un sistema di riconoscimento facciale basato sull'intelligenza artificiale

trato in funzione per lo stop imposto nel 2021 dal Garante della privacy, per il quale si configurava come «una forma di sorveglianza indiscriminata/di massa». Oltre a essere «privo di una base giuridica», ora creata dall'Ai Act.

Riguardo ai database, l'unico noto italiano è il Casellario Centrale d'Identità del Servizio Polizia Scientifica (Afis). «Un sistema dalla forte disparità e dalla scarsissima trasparenza», denuncia Napolitano. «Sulla base degli unici dati forniti dal ministero dell'Interno nel 2020 sappiamo che allora conteneva 3 milioni e 289mila volti di cittadini italiani indagati o condannati per crimini vari e oltre 15 milioni di stranieri finiti al suo interno anche solo per aver avuto un'interazione con lo Stato (rinnovo del permesso di soggiorno, richiesta della carta di identità, ottenimento della cittadinanza e così via)», evidenzia Napolitano dell'Hermes Center. All'Afis si aggiungono poi altri database interoperabili a livello europeo. «Un'altra criticità è che se l'Ai Act stabilisce che serve un'autorità indipendente per la verifica di come queste applicazioni vengono utilizzate, il governo italiano ha scelto l'Agenzia per l'Italia Digitale (Agid) e l'Agenzia per la Cybersicurezza Nazionale, due autorità che non sono indipendenti in quanto nominate dall'esecutivo».

Tra i divieti del nuovo regolamento comunitario c'è quello per lo *scraping*, l'uso di sistemi che per creare o ampliare le banche dati cercano immagini facciali da Internet o nei filmati delle telecamere a circuito chiuso. «Un caso emblematico – ricorda Arruzzoli di Cerbeyra – è quello della statunitense Clearview Ai, che ha un database di circa 20 miliardi di immagini cercate su Internet utilizzate per poter identificare le persone quando passano sotto le telecamere dei servizi di sorveglianza. In uno spot Clearview sosteneva di essere in grado di mappare qualsiasi persona con otto foto». Sanzionata dalle autorità garanti per la protezione dei dati personali di Francia, Regno Unito e Italia, «tuttora la usano i servizi di intelligence ucraini per individuare eventuali spie russe sul territorio».

L'Ai Act ha inoltre posto il veto «sulla cosiddetta intelligenza artificiale generativa – continua l'esperto di Cerbeyra – che non solo riesce a riconoscere la persona ma a carpirne i sentimenti, analizzare il comportamento». Tecniche usate anche per la cosiddetta polizia predittiva, espressamente vietata dal regolamento comunitario. «Tempo fa – ricorda Arruzzoli – un dirigente pubblico mi disse che adoperava un sistema di un'azienda statunitense che gli permetteva di fare il riassunto delle riunioni. Il problema è che dava indicazioni anche su quando parlava una persona, fornendo dati quali il livello di interazione dei partecipanti o il loro stato d'animo mentre venivano esposti gli argomenti, tutte analisi che venivano fatte sul volto delle persone, sulla parola, sulla voce, che andavano proprio contro quello che è l'articolo 5 dell'Ai Act». 'E