OPINIO JURIS
LAW & POLITICS REVIEW

AI, privacy e riconoscimento facciale: verso una sorveglianza biometrica di massa?

Le associazioni europee per la tutela della privacy denunciano i rischi dell'uso massiccio di sistemi tecnologici di controllo a distanza.

A cura di Mariarita Cupersito

Varie associazioni per la tutela della privacy si sono mobilitate[1] per chiedere all'Europa di impedire l'uso indiscriminato di tecnologie per il controllo biometrico e facciale di massa, tendenza sempre più diffusa in varie nazioni e città che dopo i primi esperimenti in piazze e parchi hanno moltiplicato l'installazione di dispositivi di sorveglianza.
Gli attivisti sostengono che l'applicazione dell'Intelligenza Artificiale avrà come risultato quello di produrre un falso senso di sicurezza per i cittadini ma una vera ed effettiva società sorvegliata, ragion per cui hanno avviato la campagna europea Reclaim Your Face: Ban Biometric Mass Surveillance[2], con lo scopo di denunciare i possibili

[1] cfr. repubblica.it, "Rivoglio la mia faccia. No a una società della sorveglianza", 13/11/2020, https://www.repubblica.it/tecnologia/sicurezza/2020/11/13/news/rivoglio_la_mia_faccia_blade_runner_non_abita_piu_qui-274229155/
[2] cfr. Reclaimyourface.eu, "Reclaim Your Face: Ban Biometric Mass Surveillance", https://reclaimyourface.eu/

ISSN 2531-6931

effetti collaterali dell'uso massiccio di sistemi tecnologici di controllo a distanza.
Queste associazioni, tra cui European Digital Rights, Access Now e l'italiana Hermes Center, chiedono[3] che le autorità locali e nazionali europee facciano luce sui rischi connessi all'utilizzo di tali tecnologie e che rifiutino l'uso della sorveglianza biometrica negli spazi pubblici.
La delicata questione parte dall'assunto che i dispositivi biometrici dovrebbero costituire un deterrente per i criminali e al contempo facilitare il lavoro delle forze dell'ordine, ma vari studi dimostrano non solo che non ci sono dati che attestino la diminuzione dei reati nelle zone oggetto di sorveglianza ma che al contrario si segnalano numerose notizie di violazione della privacy mediante abusi delle telecamere installate. Stando ad alcune ricerche[4], l'impiego di tali tecnologie favorirebbe anche fenomeni discriminatori e la persecuzione di persone colpevoli solo di esercitare i propri diritti.
La criticità è preliminarmente di tipo tecnologico: alla base delle tecnologie di riconoscimento facciale c'è la machine perception, il settore di Intelligenza Artificiale che è stato maggiormente influenzato[5] dall'avvento del *deep learning*, e la disponibilità di grandi quantità di dati nonché il perfezionamento delle reti di algoritmi neurali hanno fatto sì che l'AI eseguisse compiti di classificazione visiva anche meglio di un operatore umano, ma non al punto da evitare possibili errori.
Negli Usa l'Associazione americana per le libertà civili ha scoperto che il software Rekognition[6] di Amazon identificava come pregiudicati i parlamentari del Congresso Usa, mentre IBM ha comunicato al Congresso Usa che l'azienda non fornirà più ai dipartimenti di polizia tecnologie di riconoscimento facciale per la sorveglianza di massa proprio per paura che possa essere impiegata per la violazione dei

[3] cfr. repubblica.it, "Rivoglio la mia faccia. No a una società della sorveglianza", 13/11/2020, https://www.repubblica.it/tecnologia/sicurezza/2020/11/13/news/rivoglio_la_mia_faccia_blade_runner_non_abita_piu_qui-274229155/

[4] cfr. euobserver.com, "EU warned over fast-tracking facial recognition", 27 novembre 2019, https://euobserver.com/science/146732

[5] cfr. repubblica.it, "Rivoglio la mia faccia. No a una società della sorveglianza", 13/11/2020, https://www.repubblica.it/tecnologia/sicurezza/2020/11/13/news/rivoglio_la_mia_faccia_blade_runner_non_abita_piu_qui-274229155/

[6] cfr. Amazon Rekognition, https://aws.amazon.com/it/rekognition/?blog-cards.sort-by=item.additionalFields.createdDate&blog-cards.sort-order=desc

diritti umani e delle libertà fondamentali [7], invitando al contempo all'apertura di un dibattito pubblico sul tema. L'appello è stato presto raccolto dai Democratici americani, i quali hanno presentato alcune leggi che mirano ad evitare tale impiego della tecnologia e che sono alla base della decisione di cinque grandi città degli Stati Uniti[8] di vietare l'uso del riconoscimento facciale.

Per quel che concerne l'Europa, invece, la Commissione non si è ancora pronunciata e continua a finanziare progetti di sorveglianza biometrica[9] per porti e aeroporti. In considerazione dei rischi connessi alla vulnerabilità delle grandi banche dati centralizzate, le associazioni invocano maggiore trasparenza sul loro impiego, sensibilizzando la società civile a rivelare e rifiutare l'utilizzo della sorveglianza biometrica che potrebbe avere un notevole impatto sui diritti e sulle libertà negli spazi pubblici.

Gli attivisti italiani, in particolare, nel rivolgersi all'Autorità Garante per la privacy chiedono di vigilare sull'utilizzo dei mezzi di riconoscimento biometrico[10] da parte dei comuni italiani e di considerare attentamente l'impatto dei sistemi che alcune città hanno intenzione di predisporre; si chiede inoltre a tutte le città metropolitane la sospensione di qualsivoglia progetto di riconoscimento facciale già avviato e che tali tecnologie non vengano introdotte nel contesto pubblico cittadino.

Il timore più diffuso delle associazioni che si sono mobilitate è che, qualora non si intervenga adesso, il passo ulteriore potrebbe essere quello già paventato da chi denuncia l'esistenza di iBorderCtrl, un progetto finanziato da Horizon 2020[11] e incentrato sulla misurazione delle micro-espressioni facciali per rilevare bugie ed incertezze di ogni individuo in procinto di entrare in Europa.

---

[7] cfr. Ibm.com IBM CEO's Letter to Congress on Racial Justice Reform, 8 giugno 2020 https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/

[8] cfr. European Digital Rights, Ban Biometric Mass Surveillance A set of fundamental rights demands for the European Commission and EU Member States, 13 maggio 2020 https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf/

[9] cfr. repubblica.it, "Rivoglio la mia faccia. No a una società della sorveglianza", 13/11/2020, https://www.repubblica.it/tecnologia/sicurezza/2020/11/13/news/rivoglio_la_mia_faccia_blade_runner_non_abita_piu_qui-274229155/

[10] cfr. repubblica.it, "Rivoglio la mia faccia. No a una società della sorveglianza", 13/11/2020, https://www.repubblica.it/tecnologia/sicurezza/2020/11/13/news/rivoglio_la_mia_faccia_blade_runner_non_abita_piu_qui-274229155/

[11] cfr. repubblica.it, "Rivoglio la mia faccia. No a una società della sorveglianza", 13/11/2020, https://www.repubblica.it/tecnologia/sicurezza/2020/11/13/news/rivoglio_la_mia_faccia_blade_runner_non_abita_piu_qui-274229155/

ISSN 2531-6931

Ha suscitato molte polemiche negli ultimi anni il progetto portato avanti dal Pentagono e noto come Algorithmic Warfare Cross-Functional Team (AWCFT) o anche Progetto Maven[12] finalizzato ad "accelerare l'integrazione di big data e machine learning presso il Department of Defense" utilizzando software di visione artificiale per analizzare in modo automatico i dati raccolti dai droni militari Usa. Google, tra i primi ad aderire al progetto Maven, nel 2018 ha annunciato il proprio ritiro[13] a seguito delle proteste dei dipendenti che si sono opposti al coinvolgimento del colosso nel war business. Prosegue invece l'attività di ClearView AI[14], che ha creato un database di circa 3 miliardi di foto raccogliendo da internet tutte le immagini disponibili.
Combinando insieme i dati presenti sui social e quelli a cui uno Stato potrebbe aver accesso sorvolando la normativa in materia di protezione dei dati, assume sempre maggiore concretezza l'ipotesi che strumenti di riconoscimento facciale attingano sia dalle foto personali di milioni di persone sul web che da quelle delle tante videocamere di sorveglianza sparse per il Paese, realizzando così l'identificazione e il tracking delle persone in tempo reale[15].
Un simile scenario è già stato in qualche modo realizzato con il progetto Skynet[16], attivo da tempo in Cina; il governo cinese mira inoltre ad espandere la rete di sorveglianza mediante la raccolta e catalogazione di milioni di campioni di DNA di cittadini incensurati

[12] cfr. DEPUTY SECRETARY OF DEFENSE 1010 DEFENSE PENTAGON WASHINGTON, DC 20301-1010, Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven) 26 aprile 2017 https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf
[13] cfr. hwupgrade.it, Google abbandonerà il progetto Maven per i droni con AI al servizio del Pentagono? 4 giugno 2018 https://www.hwupgrade.it/news/web/google-abbandonera-il-progetto-maven-per-i-droni-con-ai-al-servizio-del-pentagono_76276.html
[14] cfr. Clearview.ai, Computer vision for a safer world, https://clearview.ai/
[15] cfr. agendadigitale.eu, "Tecnologie per la sorveglianza di massa crescono. Che possiamo fare?", 30 luglio 2020, https://www.agendadigitale.eu/sicurezza/privacy/uno-scudo-globale-contro-la-sorveglianza-digitale-ma-prima-educhiamo-noi-stessi/
[16] cfr. Business Insider Italia, " Skynet, la Cina sperimenta l'intelligenza artificiale che ti segue ovunque e riconosce un volto tra un milione", 9 dicembre 2018, https://it.businessinsider.com/skynet-la-cina-sperimenta-lintelligenza-artificiale-che-ti-segue-ovunque-e-riconosce-un-volto-tra-un-milione/

mediante il progetto Dragnet[17], che ha tracciato e immagazzinato i dati di alcune minoranze etniche[18] già oggetto di video sorveglianza.
Se da un lato, quindi, alcuni regimi particolarmente duri non esitano ad utilizzare ogni mezzo per il tracciamento e controllo della popolazione, i Paesi democratici sembrano comunque muoversi nella stessa direzione,[19] facendo ricorso alle informazioni rese disponibili direttamente dai cittadini mediante l'utilizzo dei vari social network e all'acquisto da parte di agenzie governative di servizi di analisi delle informazioni da società specializzate[20].
Ed è proprio in questi Paesi che prosegue l'attivismo delle varie associazioni che invocano il rispetto delle normative in materia di tutela della privacy e dei dati personali facendo leva, in particolare, sul GDPR[21] predisposto in ambito europeo ma che si sta affermando in tutto il mondo come standard per la tutela dei dati.
Più in generale, come soluzione di più ampia portata ma la cui realizzazione appare al contempo poco probabile, è stata suggerita la costituzione di un organismo di governance mondiale[22] in ragione del carattere universale proprio delle libertà civili, tra cui la protezione dei dati personali[23]. Si auspica infine che il dibattito legato a questi temi possa favorire una maggiore consapevolezza sulle potenziali derive in tema di sicurezza e tutela della privacy e contribuire alla definizione di

[17] cfr. International Consortium of Investigative Journalism, "Exposed: China's Operating Manuals for Mass Internment and Arrest by Algorithmì", 24 novembre, https://www.icij.org/investigations/china cables/exposed-chinas-operating-manuals-for-mass-internment-and-arrest-by-algorithm/
[18] cfr. Australian Strategic Policy Institute, "Inside China's DNA dragnet", 17 giugno 2020, https://www.aspi.org.au/report/genomic-surveillance/
[19] cfr. agendadigitale.eu, "Tecnologie per la sorveglianza di massa crescono. Che possiamo fare?", 30 luglio 2020, https://www.agendadigitale.eu/sicurezza/privacy/uno-scudo-globale-contro-la-sorveglianza-digitale-ma-prima-educhiamo-noi-stessi/
[20] cfr. European Digital Rights, Ban Biometric Mass Surveillance A set of fundamental rights demands for the European Commission and EU Member States, 13 maggio 2020 https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf/
[21] cfr. agendadigitale.eu, "Tecnologie per la sorveglianza di massa crescono. Che possiamo fare?", 30 luglio 2020, https://www.agendadigitale.eu/sicurezza/privacy/uno-scudo-globale-contro-la-sorveglianza-digitale-ma-prima-educhiamo-noi-stessi/
[22] cfr. agendadigitale.eu, "Tecnologie per la sorveglianza di massa crescono. Che possiamo fare?", 30 luglio 2020, https://www.agendadigitale.eu/sicurezza/privacy/uno-scudo-globale-contro-la-sorveglianza-digitale-ma-prima-educhiamo-noi-stessi/
[23] cfr. European Digital Rights, Ban Biometric Mass Surveillance A set of fundamental rights demands for the European Commission and EU Member States, 13 maggio 2020 https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf/

ISSN 2531-6931

un'etica digitale[24] che disciplini compiutamente la materia, affinché i diritti dei cittadini non ne risultino compromessi.

[24] cfr. agendadigitale.eu, "Tecnologie per la sorveglianza di massa crescono. Che possiamo fare?", 30 luglio 2020, https://www.agendadigitale.eu/sicurezza/privacy/uno-scudo-globale-contro-la-sorveglianza-digitale-ma-prima-educhiamo-noi-stessi/