# CAMERA DEI DEPUTATI N. 3009

## PROPOSTA DI LEGGE

D'INIZIATIVA DEI DEPUTATI

**SENSI, ENRICO BORGHI, MADIA, QUARTAPELLE PROCOPIO, SERRACCHIANI, VERINI**

Sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici in luoghi pubblici o aperti al pubblico

*Presentata il 12 aprile 2021*

ONOREVOLI COLLEGHI ! – I sistemi di riconoscimento facciale (*facial recognition technology*) sono sempre più diffusi, malgrado le preoccupazioni crescenti in merito alla loro efficienza e ai rischi per la *privacy* e per i diritti civili dei cittadini.

Il regolamento sulla protezione dei dati (regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016) considera i « dati biometrici » tra quelli più complessi e prevede che il loro trattamento sia vietato, salvo alcune deroghe specifiche, perché la raccolta a distanza attraverso le telecamere è estremamente invasiva e – come ha evidenziato il dottor Giuseppe Busia, quando era Segretario generale del Garante per la protezione dei dati personali – realizza « una sorveglianza globale, continua e massiva » (« L'Ue stoppa il riconoscimento facciale: "No all'utilizzo nei luoghi pubblici" », *La Stampa*, 18 gennaio 2020). Queste tecnologie, infatti, « permettono il monitoraggio, la raccolta, la conservazione, l'analisi e l'utilizzo di altri dati personali sensibili (dati biometrici) di massa senza un ragionevole e individualizzato sospetto di reato », costituendo, di fatto, una « sorveglianza di massa indiscriminata », come sostiene *Amnesty International*.

Da tempo diverse organizzazione impegnate nella difesa dei diritti civili hanno denunciato all'opinione pubblica i pericoli derivanti dai sistemi di riconoscimento facciale, a causa dell'uso di algoritmi imprecisi e connotati da un'alta percentuale di er-

rori, in particolare quando sono utilizzati per il riconoscimento di volti femminili o di persone appartenenti a minoranze etniche, come nel caso dei soggetti afroamericani. Alle stesse conclusioni è arrivato anche il *National Institute of Standards and Technology,* che ha misurato gli effetti della razza, dell'età e del sesso sui principali sistemi di riconoscimento facciale utilizzati negli Stati Uniti d'America (USA).

La preoccupazione per un uso discriminatorio e razziale di questi sistemi e i rischi per la *privacy* a essi connessi, derivanti dal modo in cui vengono alimentati i *database* nei quali sono raccolti le immagini e i video necessari per il funzionamento degli stessi sistemi, hanno spinto diverse aziende a rinunciare o a sospendere le loro attività in questo settore.

La prima è stata l'*International Business Machines Corporation*, nota con l'acronimo di « IBM », storica azienda informatica americana che, in una lettera inviata al Congresso degli USA, ha dichiarato di abbandonare il *business* collegato ai sistemi di riconoscimento facciale e di opporsi all'utilizzo di tali sistemi ai fini della sorveglianza di massa e della profilazione razziale. In seguito, anche l'azienda di commercio elettronico statunitense Amazon ha previsto una moratoria di un anno sull'uso da parte delle Forze di polizia di *Rekognition*, il suo *software* di riconoscimento facciale basato sul c*loud*, utilizzato, tra l'altro, da numerose agenzie governative degli USA, tra le quali la *United States Immigration and Customs Enforcement*.

Infine, l'azienda informatica statunitense Microsoft *Corporation* ha comunicato la sua decisione di non vendere tecnologie di riconoscimento facciale ai dipartimenti di polizia americana finché non sarà approvata una legge che regolamenti tali tecnologie e che tenga conto dei diritti umani.

La stessa attenzione e sensibilità alla *privacy* e ai diritti civili non sembra, però, essere avvertita da alcuni amministratori locali italiani che, in assenza di norme sufficientemente chiare, stanno progettando l'installazione di massa nelle città di sistemi di riconoscimento facciale, che prevedono il trattamento senza autorizzazione dei dati biometrici.

Il comune di Como sembra essere tra quelli con il progetto più avanzato, come segnalato da diversi organi di stampa, tra i quali il sito *internet Wired* (*https://www.wired.it*) che, nel giugno 2020, ha dedicato alla discussa iniziativa una vera e propria indagine.

Un altro caso da citare (come già segnalato nell'interrogazione a risposta scritta n. 4-06107 del 23 giugno 2020 del primo firmatario della presente proposta di legge) è quello del comune di Udine, dove è stata annunciata l'installazione di un nuovo sistema di videosorveglianza, con 67 nuove telecamere, che vanno ad aggiungersi alle 75 telecamere già presenti nella città e agli 11 sistemi di lettura delle targhe dei veicoli. Ma la vera novità di questo intervento consiste nella volontà di « implementare gli strumenti di video-analisi, come il riconoscimento di mezzi e individui (e un domani il riconoscimento facciale) sulla base di filtri come l'età, il sesso, gli abiti, l'orario, attraverso l'utilizzo di software di analisi forense (...) ».

Sono ormai molti i comuni italiani, compresi i grandi capoluoghi, che progettano di trasformare i loro sistemi di videosorveglianza in veri e propri sistemi di riconoscimento facciale, con l'utilizzo di « dati biometrici ». Tutto questo in assenza di un quadro normativo che consenta di uniformare le condizioni per l'utilizzo dei dati biometrici da parte degli enti territoriali, in particolare per le funzioni di polizia giudiziaria riservate alla polizia locale, in modo da assicurare le necessarie garanzie per la tutela dei diritti costituzionali dei cittadini. Si consideri, inoltre, che il Comitato europeo per la protezione dei dati (*European Data Protection Board)* ha soltanto di recente, il 29 gennaio 2020, adottato la versione definitiva delle linee guida sui trattamenti di videosorveglianza – « *Guidelines* 3/2019 *on processing of personal data through video devices* » – che chiariscono in quali termini il citato regolamento (UE) 2016/679 si applichi al trattamento dei dati personali mediante dispositivi video e la raccolta di immagini fotografiche.

L'allarme sulla *privacy* dei cittadini è partito principalmente da un'inchiesta del quotidiano « *New York Times* », del 18 gennaio 2020, che ha rivelato che le Forze dell'ordine, dalla polizia locale in Florida al *Federal Bureau of Investigation* e al Dipartimento della sicurezza interna, farebbero uso di una « *app* » per il riconoscimento facciale, ideata da un'azienda privata, la Clearview AI. « Fai una foto a una persona, la carichi e vedi le foto pubbliche di quella persona, insieme ai *link* a dove sono apparse quelle foto ». Il sistema si baserebbe su un *database* di oltre 3 miliardi di immagini che l'azienda afferma di aver « raschiato » da *Facebook*, da *YouTube* e da milioni di altri siti *web*. Le Forze dell'ordine federali e statali hanno affermato che, pur avendo una conoscenza limitata dell'attività dell'azienda Clearview AI e delle sue finalità, avevano usato la sua « *app* » per risolvere diverse indagini riguardanti furto di identità, frode con carta di credito, omicidi e casi di sfruttamento sessuale dei minori.

Nel *database* dell'azienda Clearview AI sarebbero presenti anche le foto di cittadini italiani e di centinaia di milioni di altri cittadini europei, raccolte senza nessuna autorizzazione e utilizzate di fatto in modo illecito, anche da parte di alcune Forze di polizia europee.

L'autorità competente in materia di protezione dei dati personali di Amburgo, con una recente decisione che non ha precedenti nell'Unione europea, ha imposto all'azienda Clearview AI di cancellare le informazioni di un cittadino tedesco, mentre la competente autorità svedese ha inflitto all'autorità di polizia nazionale una multa di 250.000 euro per l'utilizzo illegale della tecnologia di riconoscimento facciale sviluppata dall'azienda Clearview AI.

La risoluzione 2020/2013(INI) del Parlamento europeo, del 20 gennaio 2021, sull'intelligenza artificiale, ha invitato la Commissione europea a prendere in considerazione l'introduzione di una moratoria sull'utilizzo dei sistemi di riconoscimento facciale da parte delle autorità degli Stati membri nei luoghi pubblici, quali gli aeroporti, e nei locali destinati all'istruzione e all'assistenza sanitaria, fino a quando le norme tecniche non saranno considerate pienamente conformi ai diritti fondamentali, i risultati ottenuti non saranno privi di distorsioni e di discriminazioni e non saranno previste rigorose garanzie contro gli utilizzi impropri in grado di assicurare la necessità e la proporzionalità dell'utilizzo di tali sistemi.

Con la presente proposta di legge accogliamo l'invito del Parlamento europeo e di molte organizzazioni per i diritti civili per una moratoria dell'utilizzo dei sistemi di riconoscimento facciale nei luoghi pubblici o aperti al pubblico, attraverso l'uso di dati biometrici, fino a quando non sarà adottata una normativa che assicuri il pieno rispetto dei diritti costituzionali dei cittadini, conformemente alle indicazioni delle autorità nazionali ed europee per la protezione dei dati personali.

Da questa moratoria sono esclusi i normali sistemi di videosorveglianza che non fanno uso di dati biometrici per il riconoscimento facciale e i sistemi installati su *smartphone*, *tablet* e altri *device* utilizzati per un uso privato.

# PROPOSTA DI LEGGE

—

## Art. 1.

*(Sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici in luoghi pubblici o aperti al pubblico)*

1. In considerazione di quanto disposto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, nonché dalla direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dell'esigenza di disciplinare conformemente i requisiti di ammissibilità, le condizioni e le garanzie relativi all'impiego di sistemi di riconoscimento facciale, nel rispetto del principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea, l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici di cui all'articolo 4, numero 14), del citato regolamento (UE) 2016/679 in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, sono sospese fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2021.

2. La sospensione di cui al comma 1 non si applica agli impianti di videosorveglianza che non usano i sistemi di riconoscimento facciale di cui al medesimo comma 1 e che sono conformi alla normativa vigente.

## Art. 2.

*(Sanzioni)*

1. In caso di installazione o di utilizzazione dei sistemi di cui all'articolo 1, dalla data di entrata in vigore della presente legge fino al 31 dicembre 2021, salvo che il fatto costituisca reato, si applicano le sanzioni amministrative pecuniarie stabilite dal-

l'articolo 166, comma 1, del codice di cui al decreto legislativo 30 giugno 2003, n. 196, e dall'articolo 42, comma 1, del decreto legislativo 18 maggio 2018, n. 51, in base al rispettivo ambito di applicazione.

PAGINA BIANCA

PAGINA BIANCA

*18PDL0137680*