La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il dissenso politico: osservazioni a partire dal caso *Glukhin c. Russia*

di Giuseppe Mobilio

Title: The European Court of Human Rights condemns the use of facial recognition technology to stifle political dissent: observations from the case of Glukhin v Russia

Keywords: facial recognition technology; surveillance; police activities.

1. – Il caso Glukhin c. Russia, del 4 luglio 2023, rappresenta la prima occasione in cui una Corte internazionale, nella specie la Corte europea dei diritti dell'uomo (Corte EDU), si è pronunciata sull'uso delle tecnologie di riconoscimento facciale (TRF) e su uno dei suoi impieghi più contestati, ovvero a scopi di polizia.

Queste tecnologie offrono un formidabile strumento di sorveglianza, poiché sfruttano sistemi di intelligenza artificiale (IA) e dati biometrici per identificare le persone a distanza e senza che queste ne abbiano necessariamente consapevolezza. È sufficiente integrare software basati su algoritmi di riconoscimento facciale con uno dei molteplici dispositivi a disposizione, come ad esempio telecamere a circuito chiuso o droni, per costruire una rete capillare di controllo a disposizione di soggetti privati o autorità pubbliche. A queste ultime, siano esse governi democratici o regimi autoritari, non sfuggono le enormi potenzialità offerte da queste tecnologie, tanto in termini investigativi e di repressione dei reati o di ricerca di persone scomparse, quanto di controllo della popolazione e di repressione del dissenso. Il prezzo di queste utilità, tuttavia, è la limitazione penetrante di molteplici libertà e diritti fondamentali, come la privacy e la tutela dei dati personali, o la libertà di espressione e di riunione delle persone sottoposte a sorveglianza (FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27 novembre 2019); da qui l'esigenza di una attenta regolazione di questi mezzi tecnologici per condizionarne l'impiego al rispetto di principi costituzionali e valori democratici (G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021).

Il dibattito su questi strumenti è diventato ancora più acceso a livello europeo in occasione del procedimento di approvazione del regolamento "che stabilisce regole armonizzate sull'intelligenza artificiale" (c.d. AI Act), presentato dalla Commissione nell'aprile 2021 e giunto oramai alle battute finali dopo il voto del Coreper del 26 gennaio 2024 (data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf). Varie voci si sono levate per limitare fortemente, se non bandire l'uso delle tecnologie di riconoscimento facciale per scopi di polizia, tanto dalle istituzioni – come accaduto con le proposte emendative del Parlamento

europeo (www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html) –, quanto dalla società civile – con le posizioni assunte da associazioni come EDRi (edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/) o Big Brother Watch (bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Biometric-Britain.pdf) –. A livello di Consiglio d'Europa il Committee on Artificial Intelligence (CAI) ha invece pubblicato nel luglio 2023 un Consolidated Working Draft che possa fungere da base per un futuro quadro normativo su "Artificial Intelligence, Human Rights, Democracy and the Rule of Law" (CAI(2023)18, 7 luglio 2023; rm.coe.int/cai-2023-18-consolidated-working-draft-framework-convention/1680abde66), il quale però non si sofferma su queste tecnologie di sorveglianza. È stato invece il Comitato consultivo della Convenzione 108 a pubblicare nel 2021, quali atti di *soft law*, delle "linee guida" espressamente dedicate alle TRF (rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751).

In un contesto normativo così complesso e in divenire, la Corte EDU è intervenuta con una pronuncia che ha condannato la Federazione Russa per aver fatto uso di queste tecnologie a scopo di repressione del dissenso politico. La Corte ha ravvisato una violazione degli articoli 10 (libertà di espressione) e 8 (diritto al rispetto della vita privata) della Convenzione europea dei diritti dell'uomo (CEDU). Con il presente contributo si vuole ricostruire la vicenda che ha originato questa pronuncia, mettendo in luce quanto possano essere insidiosi gli impieghi delle TRF e quanto grande il potere di sorveglianza che ne deriva. Nell'approfondire il ragionamento seguito della Corte, si evidenzierà in che modo il fattore tecnologico condizioni il tenore delle argomentazioni, ponendo in risalto pregi e limiti dell'approccio seguito. Sulla base dell'analisi svolta, si raffronteranno gli indirizzi espressi da questa pronuncia con la disciplina dell'AI Act di prossima adozione. L'obiettivo è sottolineare come questa sentenza rappresenti un tassello importante che si inserisce in un quadro normativo destinato a offrire maggior protezione ai diritti delle persone e ai sistemi democratici, ma anche a complicarsi notevolmente e mutare nel prossimo futuro.

2. – La Terza Sezione della Corte EDU si è pronunciata su un ricorso proposto da Nikolay Sergeyevich Glukhin, il quale era stato condannato da un tribunale russo a causa della esternazione del proprio dissenso nei confronti del governo. Il 23 agosto 2019 Glukhin aveva dato vita ad una manifestazione nella metropolitana di Mosca, portando con sé un cartellone a grandezza naturale che ritraeva un altro attivista politico, Konstantin Kotov, accompagnato dalla scritta «You must be f**king kidding me. I'm Konstantin Kotov. I'm facing up to five years [in prison] under [Article] 212.1 for peaceful protests». L'Unità anti-terrorismo della polizia di Mosca aveva quindi proceduto a indagini e rintracciato su un canale pubblico del social-media Telegram una immagine di Glukhin durante la sua manifestazione, andando poi ad acquisire le riprese delle telecamere a circuito chiuso della metropolitana (24 agosto 2019). Pochi giorni dopo (30 agosto 2019), Glukhin veniva arrestato per violazione della normativa sugli eventi pubblici del 2004, la quale impone di notificare all'autorità pubblica le manifestazioni isolate nelle ipotesi in cui si faccia uso di "oggetti rapidamente (de)assemblati". L'arresto era stato effettuato presso una stazione della metropolitana, sempre grazie alle riprese delle telecamere che hanno consentito alla polizia di identificare Glukhin sul posto ed intervenire tempestivamente. Le immagini erano state acquisite in base al Code of Administrative Offence (CAO) e al Police Act, che consentono di impiegare questo tipo di dati, qualora rilevanti, nei procedimenti che originano da illeciti amministrativi. Il 23 settembre 2019 faceva seguito la condanna di Glukhin da parte della Meshchanskiy District Court di Mosca, con la pena al pagamento di 20.000 rubli (circa 283 euro). A seguito di appello, il 30 ottobre 2019 la Moscow City Court

DPCE online
ISSN: 2037-6677

confermava in seconda istanza la condanna. Di conseguenza Glukhin ha convenuto la Federazione Russa davanti alla Corte EDU, sebbene dal 16 settembre 2022 essa non sia più parte della CEDU, a seguito dell'espulsione dal Consiglio d'Europa a causa dell'aggressione militare in Ucraina. La giurisdizione della Corte EDU, tuttavia, si estende alle presunte violazioni della Convenzione perpetrate fino al 16 settembre 2022 (*Glukhin v. Russia*, cit., §42), dando così origine alla pronuncia in commento.

3. – Come anticipato, la Corte EDU condanna la Russia per violazione degli articoli 10 e 8 della CEDU. Con riguardo al primo parametro, relativo alla libertà di espressione, la Corte è chiara nel rilevare come tale libertà copra anche le espressioni non verbali, mentre la condotta di Glukhin era del tutto idonea a esprimere un'opinione su questioni di interesse generale (ivi, §51). Ne deriva che l'accompagnamento alla stazione di polizia, l'arresto e la condanna costituiscono una forma di interferenza con tale libertà (ivi, § 52). Di conseguenza, la Corte svolge una indagine sulle condizioni alle quali sono ammesse limitazioni alla libertà di espressione (ivi, §§54-56), in accordo con la propria giurisprudenza consolidata (*Novikova e altri c. Russia*, nn. 25501/07 e altri 4, 26 aprile 2016, §110 ss.). Il test richiede, quindi, che una misura limitativa: sia «prevista dalla legge»; persegua almeno uno degli scopi legittimi indicati all'art. 10, par. 2 CEDU; sia «necessaria» nell'ambito di «una società democratica», ovvero che l'interferenza con la libertà sia giustificata da un "bisogno sociale impellente", sia "proporzionata allo scopo perseguito" e che le ragioni addotte siano "pertinenti e sufficienti".

Con riguardo alla "previsione dalla legge", la Corte EDU stabilisce che le previsioni della normativa sugli eventi pubblici del 2004 non rispondono ai requisiti di "qualità" che la legge deve possedere per limitare legittimamente le libertà, in quanto la previsione di "oggetti rapidamente (de)assemblati" non è sufficientemente chiara per consentire di prevedere di che tipo di oggetti si tratti. In ragione del tipo di dimostrazione realizzata dalla singola persona e in assenza di interpretazioni nella giurisprudenza che permettano di circoscrivere il significato di tali norme, la Corte sancisce come la regolazione nazionale non soddisfi il requisito della "prevedibilità" degli effetti conseguenti all'applicazione delle regole (richiesto fin da *Silver e altri c. Regno Unito*, nn. 5947/72 e altri, 25 marzo 1983, §87).

La Corte prosegue il suo giudizio specificando che, quand'anche si volesse ritenere che tale normativa soddisfi i requisiti qualitativi richiesti e consenta di perseguire scopi legittimi come «difesa dell'ordine» o «protezione dei diritti e delle libertà altrui», le interferenze così realizzate non risultano comunque "necessarie in una società democratica". Il ricorrente, infatti, ha svolto una dimostrazione individuale pacifica e non pericolosa, mentre l'illecito che gli è stato contestato riguardava solamente la mancata notifica all'autorità, senza integrare alcuna condotta riprovevole o contraria all'ordine pubblico. Ciò nonostante, le autorità non hanno mostrato un sufficiente livello di tolleranza, anche in considerazione delle libertà implicate nel gesto compiuto. Di conseguenza, i giudici russi, nell'emettere la condanna, non hanno fornito "ragioni pertinenti o sufficienti" per giustificare l'interferenza con la libertà di espressione di Glukhin.

4. – La Corte EDU dedica però maggiori argomenti alla violazione del secondo parametro, ovvero l'art. 8 CEDU. È per il diritto al rispetto della vita privata, infatti, che la Corte entra nel merito dell'impatto che le TRF producono su diritti e libertà delle persone e sui sistemi democratici.

La Corte innanzitutto si sofferma nel descrivere l'uso effettivo che è stato fatto di queste tecnologie (*Glukhin v. Russia*, cit., §68). In un primo momento l'Unità anti-terrorismo della polizia di Mosca ha sottoposto a riconoscimento facciale le

immagini catturate da Telegram per identificare in Glukhin il soggetto che ha dato vita alla dimostrazione nella metropolitana. In un secondo momento la polizia ha impiegato il riconoscimento facciale integrato nelle telecamere a circuito chiuso della metropolitana per rintracciare Glukhin e procedere al suo arresto. Si tratta, quindi, di due impieghi distinti delle TRF.

In generale, queste tecnologie si basano su algoritmi che sono in grado di effettuare una comparazione automatizzata tra le immagini raccolte – come detto – con i più svariati dispositivi, o anche scaricate da internet, e le immagini facciali raccolte in una galleria (c.d. watchlist), in cerca di una eventuale corrispondenza. Le persone presenti nella galleria sono state già identificate, così che una corrispondenza permette di collegare il volto della persona nell'immagine con le informazioni appartenenti alla persona nella galleria. Ai sensi della normativa dell'UE sulla protezione dei dati personali trattati per scopi di polizia (direttiva (UE) 2016/680, c.d. Direttiva di polizia), i dati processati da queste tecnologie sono qualificabili o come "dati personali", se si tratta di semplici immagini che ritraggono i volti, o come "dati biometrici", qualora ottenuti da un «trattamento tecnico specifico», come gli algoritmi in questione, con l'obiettivo di consentire «l'identificazione univoca» della persona (EDPB, *Guidelines 3/2019 on processing of personal data through video devices*, 2.0, 29 gennaio 2020, §74).

Nel caso in discussione, le autorità hanno fatto prima un uso c.d. "a posteriori" delle TRF, con il quale la cattura dell'immagine del volto (scaricata da Telegram) avviene a distanza di un certo lasso di tempo rispetto alla sua elaborazione, al confronto e all'identificazione della persona. Successivamente è stato fatto un uso "in tempo reale" delle TRF, con il quale l'acquisizione dell'immagine, la sua elaborazione, il confronto con la galleria e l'identificazione avvengono nella sostanza tutti istantaneamente; di conseguenza, in questa ipotesi, le immagini processate vengono catturate "dal vivo", mentre gli algoritmi consegnano all'operatore un risultato immediato circa la presenza o meno di una corrispondenza nella galleria, generando un alert che consente all'operatore di polizia di intervenire tempestivamente.

Alla luce di queste applicazioni tecnologiche, la Corte verifica se vi sia stata una interferenza con il diritto al rispetto della vita privata (*Glukhin v. Russia*, cit., §§64-67). Lo scrutinio ha buon gioco poiché, alla luce dei propri precedenti, la Corte abbraccia una nozione ampia di "vita privata", comprensiva di molteplici aspetti dell'identità fisica e sociale, fra cui anche quelli legati ad attività svolte negli spazi pubblici. Con riguardo alla protezione dei dati personali, che viene oramai considerata implicitamente coperta dall'art. 8 CEDU (v. *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, n. 931/13, 27 giugno 2017, §133), la Corte chiarisce che il monitoraggio di una persona in uno spazio pubblico attraverso uno strumento di videoripresa non costituisce di per sé una forma di interferenza; tuttavia, se vi è una registrazione dei dati, e soprattutto se tale registrazione è sistematica o permanente, allora possono sorgere problemi di interferenza con questo diritto. In aggiunta, l'interferenza è maggiore se riguarda l'immagine di una persona, la quale costituisce uno dei principali attributi distintivi della personalità (*Glukhin v. Russia*, cit., §66).

Poste queste premesse, anche in questo caso la Corte procede alla verifica del rispetto delle condizioni di ammissibiltà concernenti le limitazioni al diritto di cui all'art. 8 CEDU. Il test prevede sempre la verifica: che la misura sia «prevista dalla legge»; che essa persegua almeno uno degli scopi legittimi indicati all'art. 8, par. 2 CEDU; che sia «necessaria» nell'ambito di «una società democratica» (ivi, §78).

Quanto alla "previsione con legge", la Corte individua la base legale che consentirebbe il ricorso a questi strumenti nella citata disciplina nazionale di CAO e Police Act, oltre che nel Decreto n. 410/2017, sui requisiti di sicurezza nei trasporti, il quale autorizza l'istallazione di telecamere con TRF nella

DPCE online
ISSN: 2037-6677

metropolitana di Mosca con accesso alle forze dell'ordine. Tuttavia, anche in questa ipotesi, la normativa nazionale non rispetta i requisiti di "qualità" della legge. Occorre infatti che, nell'impiego di TRF, sia essenziale disporre di norme dettagliate che disciplinino la portata e l'applicazione di queste tecnologie, nonché di solide garanzie contro il rischio di abusi e arbitrarietà. La necessità di salvaguardie «sarà ancora maggiore» quando si tratta di utilizzare TRF "dal vivo" (ivi, §82). Di contro, la legislazione russa non soddisfa queste caratteristiche.

A disattendere i requisiti di "qualità" della legge è pure la normativa nazionale sulla protezione dei dati personali, ovvero il Personal Data Protection Act (no. 152-FZ del 27 luglio 2006). Tale disciplina consente di processare i dati biometrici senza il consenso dell'interessato "in relazione all'amministrazione della giustizia". Si prevede così una "formulazione ampia" (ivi, §83) che autorizza l'uso di questi formidabili strumenti di sorveglianza in relazione a qualsiasi procedimento giudiziario, senza alcuna limitazione concernente la natura della situazione di impiego concreto, lo scopo perseguito, la categorie di persone coinvolte, il trattamento di dati sensibili come quelli che rivelano le opinioni politiche, e senza individuare salvaguardie procedurali, come procedure di autorizzazione o riguardanti l'esame, l'uso e la conservazione dei dati, o ancora meccanismi di supervisione o rimedi disponibili (come anche richiesto in S. *e Marper c. Regno Unito*, nn. 30562/04 e 30566/04, 4 dicembre 2008, §99).

La Corte prosegue poi con il suo scrutinio sull'assunto che l'uso delle TRF possa anche perseguire lo scopo legittimo di prevenire i reati (*Glukhin v. Russia*, cit., §84), ma subito dopo puntualizza come il giudizio sul rispetto della CEDU non riguardi l'uso di queste tecnologie all'avanguardia in generale e in astratto, bensì si debba basare sul trattamento dei dati personali del ricorrente in concreto e nel caso specifico portato alla sua attenzione (ivi, §85).

A questo punto la Corte va a verificare il terzo requisito, ovvero si interroga se tale trattamento dei dati derivante dall'uso delle TRF sia "necessario in una società democratica" (ivi, §§86-89). Nel definire i criteri di giudizio, la pronuncia chiarisce come l'impiego di queste tecnologie da parte dell'autorità pubblica è "particolarmente intrusivo", specialmente "dal vivo", per cui occorre un "livello alto" di giustificazione per soddisfare questo requisito, il "più alto" in caso di TRF "dal vivo". Un livello di protezione maggiore è richiesto nel caso di dati sensibili come quelli idonei a rivelare opinioni politiche. Infine, nella valutazione circa la necessità in una società democratica occorre tenere conto della natura e della gravità degli illeciti in relazione ai quali le TRF sono impiegate.

Posti questi criteri, la Corte osserva come Glukhin sia stato assoggettato a riconoscimento facciale in ragione di una dimostrazione individuale, rispetto alla quale gli è stato imputato un illecito amministrativo senza aver integrato alcuna condotta reprensibile. Non solo, ma l'uso di TRF "altamente invasive" per identificare e arrestare i partecipanti ad azioni di protesta pacifiche potrebbe avere un effetto scoraggiante (*chilling effect*) nei confronti delle libertà di espressione e di riunione. Di conseguenza, l'impiego di TRF a posteriori e "a fortiori" in tempo reale non corrisponde a un "bisogno sociale impellente". Dunque, la Corte conclude stabilendo che l'uso di queste tecnologie "altamente intrusive" viola anche l'art. 8 CEDU, in quanto "incompatibile con gli ideali e i valori di una società democratica governata dalla *rule of law*, che la CEDU ha lo scopo di mantenere e promuovere" (ivi, §90).

Viene quindi dichiarata assorbita la censura relativa al contrasto con l'art. 6 CEDU, con la quale il ricorrente lamentava la violazione del diritto a un equo processo a causa della mancata costituzione della controparte processuale.

5. – Una volta richiamati i punti salienti della vicenda in questione e i contenuti della pronuncia in commento è possibile svolgere alcune considerazioni per mettere

in evidenza aspetti interessanti e limiti nell'approccio argomentativo seguito dalla Corte EDU.

Innanzitutto la Corte coglie bene un profilo legato alla diffusione di questi strumenti di sorveglianza che ha immediate ricadute sul piano sia sostanziale che processuale. Come anticipato introduttivamente, l'impiego delle TRF può avvenire in maniera discreta, senza la consapevolezza o il consenso degli interessati. Nella vicenda da cui scaturisce la sentenza, la Corte rileva (ivi, §§69-72) come la legislazione russa non preveda alcun obbligo per le forze dell'ordine di tenere traccia degli usi fatti di queste tecnologie, o di informare le persone sottoposte a riconoscimento. Né dai rapporti della polizia risulta formalmente che sia stato fatto impiego di riconoscimento facciale. Di conseguenza la Corte si mostra consapevole delle difficoltà che il ricorrente incontra nell'assolvere all'onere della prova per dimostrare la lesione dei suoi diritti. Tuttavia la Corte procede ad un ragionamento indiziario, per il quale, considerate le tempistiche rapide con cui le autorità hanno identificato e arrestato Glukhin, i rapporti di ONG che testimoniano il frequente uso di TRF come strategia per reprimere il dissenso politico (ivi, §40), nonché il fatto che il Governo russo in sede processuale non abbia contestato le affermazioni di Glukhin e dunque implicitamente abbia ammesso i citati usi di TRF, si ritiene plausibile che le autorità pubbliche abbiano fatto ricorso a tali tecnologie, pur senza che ciò sia stato specificatamente dimostrato (F. Palmiotto, N. Menéndez González, *Facial recognition technology, democracy and human rights*, in 50 *Computer Law & Security Review* 3 (2023)).

Secondariamente, la Corte EDU coglie una delle particolarità delle TRF, ovvero che si tratta di una famiglia di sistemi di IA che sfruttano *computer vision* e dati biometrici a scopi di sorveglianza, ma che al loro interno presentano caratteristiche, possibili applicazioni e impieghi diversificati (J. Buolamwini et al., *Facial Recognition Technologies in the Wild: A Primer*. Algorithmic Justice League. 29 maggio 2020, disponibile su: global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf). Di conseguenza viene distinto tra i citati impieghi di TRF "a posteriori" e "in tempo reale". Per ciascuno di questi la Corte mette in luce alcuni aspetti problematici.

Nel primo caso, legato all'analisi delle immagini scaricate da Telegram per identificare Glukhin come autore della protesta, la pronuncia sottolinea che la tutela del diritto alla vita privata si estenda anche alle attività svolte in luogo pubblico (*Glukhin v. Russia*, cit., §67). In questo caso si pone il problema di stabilire quale sia la tutela dei dati e delle immagini che ritraggono comportamenti in luoghi pubblici e che potenzialmente possono essere pubblicate e condivise sui social media. La Corte richiama la normativa per la protezione dei dati personali rilevante sotto questo profilo, ovvero la c.d. Direttiva di polizia (direttiva (UE) 2016/680), che all'art. 10 autorizza il trattamento di dati biometrici intesi a identificare in modo univoco una persona, come quelli prodotti dalle TRF, o i dati personali idonei a rivelare le opinioni politiche di una persona, solamente se ciò avviene sulla base del diritto dell'UE o di uno Stato membro e nell'eventualità, fra l'altro, che i dati siano stati «resi manifestamente pubblici dall'interessato». Tuttavia, come chiarito dall'allora Gruppo di lavoro Articolo 29, una videoripresa che avvenga in un luogo pubblico potrebbe ricadere entro tale regime solamente in seguito ad «un'interpretazione restrittiva», dalla quale emerga che «l'interessato abbia volontariamente rinunciato alla protezione speciale per i dati sensibili rendendoli disponibili al pubblico, autorità comprese» (Gruppo di lavoro Articolo 29, *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, WP 258, 29 novembre 2017, 10). È dubitabile che Glukhin abbia consapevolmente reso disponibili i propri dati per essere processati

DPCE online
ISSN: 2037-6677

dalle TRF, per cui giustamente la Corte EDU ravvisa una violazione del suo diritto alla vita privata.

Nel secondo caso, relativo all'uso delle TRF "in tempo reale" per identificare e arrestare Glukhin, la Corte EDU rimarca in qualche modo le differenze e la ancora maggiore pericolosità per i diritti e i sistemi democratici. Non a caso la Corte fa riferimento a una necessità "maggiore" di salvaguardie (*Glukhin v. Russia*, cit., §82), o del "più alto" livello di giustificazione, con riguardo a misure "particolarmente intrusive" (ivi, §86). A questo proposito un parallelo utile può essere svolto con quanto stabilito dal Garante della privacy italiano, il quale ha messo in guardia contro l'impatto che un uso sistematico di queste tecnologie può produrre. L'occasione è offerta da una recente decisione che ha impedito al Governo italiano di utilizzare un sistema di riconoscimento facciale "in tempo reale" per scopi di polizia. Il Garante ha chiarito come il «trattamento di immagini volte ad identificare le persone nel contesto pubblico [sia] di estrema delicatezza», perché si risolve in un trattamento che coinvolge i dati biometrici di chiunque sia sottoposto a riconoscimento tra la folla, seppure non oggetto di attenzione da parte delle forze dell'ordine: il rischio è che tali sistemi di IA producano una «evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui» (Garante per la protezione dei dati personali, *Parere sul sistema Sari Real Time*, 25 marzo 2021, p. 3). In definitiva, mentre le TRF "a posteriori" potrebbero essere assimilate a mezzi di indagine conosciuti negli ordinamenti giuridici e rivolti a singoli individui, le TRF "in tempo reale" interessano chiunque sia esposto alla portata delle riprese (I. Neroni Rezende, *Glukhin and the EU regulation of facial recognition: Lessons to be learned?*, in *European Law Blog*, 19 settembre 2023, disponibile su: europeanlawblog.eu/2023/09/19/glukhin-and-the-eu-regulation-of-facial-recognition-lessons-to-be-learned/).

6. - Tuttavia, il percorso argomentativo seguito dalla Corte EDU presenta dei limiti, sia per quanto affermato espressamente, sia per quanto ammesso implicitamente o non detto. Al di là dell'utilizzo di aggettivi o avverbi, infatti, la Corte rimane sulla superficie della distinzione tra TRF "a posteriori" e "in tempo reale", senza cogliere le diverse implicazioni sul piano giuridico che ne scaturiscono. È vero che la Corte dichiara espressamente di volersi mantenere aderente al caso specifico e di non voler giudicare in generale sull'ammissibilità delle TRF (*Glukhin v. Russia*, cit., §85). Ciononostante, la troppa genericità di questi passaggi espone la Corte ad un rischio di astrattezza e di equivocità.

Da una parte, non è possibile negare in assoluto che l'uso di TRF "a posteriori" sia meno invasivo di quello "in tempo reale". Come è stato autorevolmente sottolineato, l'impatto sui diritti non dipende necessariamente dalla distanza di tempo con la quale avviene il trattamento dei dati biometrici, visto che un sistema di identificazione di massa è in grado di identificare migliaia di persone in poche ore (EDPB & EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 2021, § 31). Per cui, se si vuole davvero cogliere la pericolosità delle TRF, occorre considerare complessivamente le politiche e gli usi effettivi che vengono fatti di questi mezzi di sorveglianza biometrica.

Dall'altra, l'uso "in tempo reale" di queste tecnologie e la sua insidiosità impone di prestare particolare attenzione alle forme di tutela che occorre effettivamente offrire ai cittadini. Per questo sarebbe forse valsa la pena spendere maggiori considerazioni su profili che, proprio a livello di Consiglio d'Europa, il Committee on Artificial Intelligence sottolineava contestualmente alla pronuncia della Corte EDU. Basti pensare all'esigenza di garantire maggiore trasparenza

nell'uso di queste tecnologie o un regime chiaro di responsabilità per la violazione dei diritti (C. Nardocci, *Il riconoscimento facciale sul "banco" degli imputati. Riflessioni a partire, e oltre, Corte EDU Glukhin c. Russia*, in corso di pubblicazione in *BioLaw Journal*, 1, 2024); aspetti che, anche in relazione all'uso segreto che le autorità russe fanno delle TRF, potrebbero contribuire a definire un regime più stringente di tutela.

Questa esigenza è particolarmente avvertita nei confronti delle TRF "in tempo reale" anche a causa di ulteriori specificità sul piano tecnico che non possono essere trascurate per le conseguenze che producono. Basti pensare al problema dell'accuratezza del riconoscimento, che, sebbene nel caso di specie non ricorra, rappresenta comunque una delle maggiori criticità di questo particolare uso delle TRF. Occorre infatti sempre ricordare che le TRF non offrono certezze, poiché la corrispondenza risultante dal confronto tra le immagini acquisite e la galleria con i volti identificati è sempre un processo probabilistico. Il tasso di probabilità varia a causa di molti fattori tecnici (P. Fussey, B. Davies, M. Innes, *'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing*, in 61(2) *The British Journal of Criminology* 337 (2021)), fra cui la qualità delle immagini. Un conto è se l'acquisizione delle immagini avviene con la cooperazione degli interessati e in ambiente controllato, come accade per le foto segnaletiche; altro è se l'acquisizione avviene involontariamente e in ambienti non controllati, come nel caso delle videocamere che riprendono "dal vivo" (J. Buolamwini et al., *Facial Recognition Technologies in the Wild: A Primer*, cit., 9 ss.). In questa seconda ipotesi vi sono molti elementi che condizionano questo tasso di probabilità, come il riflesso della luce o il movimento della persona ripresa, con implicazioni importanti sull'efficacia del riconoscimento e, di conseguenza, con il rischio che si creino disparità di trattamento e discriminazioni a danno delle persone sottoposte a controllo (C. Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, in *Georgetown Law, Center on Privacy and Technology*, 16 maggio 2019). In definitiva, sarebbe stato opportuno che la Corte EDU scendesse un po' più nel dettaglio dei rischi cui queste tecnologie espongono.

Da ultimo – anche in relazione all'ultimo aspetto appena sottolineato – si può notare come la Corte fondi le proprie argomentazioni in ordine alla violazione dei diritti prestando molta attenzione all'aspetto della "qualità" della disciplina che può limitare i diritti fondamentali, oltre che all'esigenza di prevedere misure di salvaguardia o garanzie procedurali. Con ciò la Corte è stata criticata per aver trascurato la legalità sostanziale dei regimi di sorveglianza a beneficio di un approccio troppo schiacciato sugli aspetti "procedurali" (M. Zalnieriute, *Glukhin v. Russia. App. No. 11519/20. Judgment*, in 117(4) *American Journal of International Law* 699 (2023)). Per cui, ad esempio, ove si censura l'uso di TRF perché, durante la manifestazione di Glukhin, non sono state realizzate condotte violente, la Corte, non fornendo maggiori precisazioni di natura sostanziale, sembrerebbe legittimare indirettamente la possibilità di impiegare le TRF ove le attività di polizia fossero dirette a colpire reati più gravi. In realtà questo tipo di considerazioni non sembrano colpire nel segno, perché comunque la Corte EDU calibra le proprie argomentazioni soppesando gli interessi sostanziali in gioco: basti pensare a come, nel valutare se le interferenze delle TRF sui diritti siano "necessarie in una società democratica", la Corte faccia riferimento proprio alla gravità degli illeciti nei cui confronti è ammesso l'utilizzo di queste tecnologie o al carattere pacifico della manifestazione; alla presenza di un trattamento automatizzato; al trattamento o meno di dati biometrici o tali da rivelare le opinioni politiche; alla possibilità che si verifichi un *chilling effect* ai danni di coloro che legittimamente vorrebbero esercitare i propri diritti; e così via. È sulla base di questi fattori, di natura sostanziale, che poi la Corte EDU impone la necessità di un regime formale più stringente. Spetta piuttosto al decisore politico, e non alla Corte EDU, costruire regole con cui

DPCE online
ISSN: 2037-6677

perseguire concretamente interessi e valori, fino a decidere se vietare l'uso di certe tecnologie o bandire certi impieghi.

Anche per questo, quindi, è interessante volgere lo sguardo all'Unione europea e guardare al recente progetto di AI Act per capire se, e in che modo, il caso Glukhin sia destinato ad orientare l'interpretazione e l'applicazione della nuova normativa.

7. - Come anticipato, mentre la Corte EDU si pronunciava con la sentenza in commento le istituzioni europee erano impegnate a portare avanti le trattative per l'approvazione dell'AI Act, che dovrebbe giungere a conclusione nel giro di pochi mesi (F. Paolucci, *Whatever it takes? The AI Act regulatory crucible*, in *Diritti Comparati*, 22 gennaio 2024). I due regimi non potranno che interagire perché, sul versante della tutela della vita privata e dei dati personali, l'art. 52, par. 3, della Carta dei diritti fondamentali dell'UE (CDFUE) prevede che, laddove vi sia una corrispondenza tra i diritti tutelati da CDFUE e CEDU, debba anche esservi una comune interpretazione quanto a significato e portata. Le spiegazioni alla CDFUE (GUUE, Spiegazioni relative alla Carta dei diritti fondamentali, C303/02, 14 dicembre 2007), unitamente alla giurisprudenza della Corte di giustizia (CGUE, *J. McB. c. L.E.*, C-400/10 PPU, 5 ottobre 2010, §53), chiariscono come l'art 7 CDFUE trovi corrispondenza nell'art. 8 CEDU, e dunque anche la giurisprudenza della Corte EDU è destinata a orientare l'interpretazione del diritto UE.

Il testo dell'AI Act votato dal Coreper è – al momento in cui si scrive – il documento ufficiale più recente, e per questo è ad esso che si farà riferimento nel prosieguo. Il nuovo regolamento dedica spazio, meritoriamente, agli usi delle TRF per scopi di polizia (G. Mobilio, *Your face is not new to me – Regulating the surveillance power of facial recognition technologies*, in 12(1) *Internet Policy Review* 1-31 (2023)), in uno scenario analogo a quello considerato dal caso Glukhin.

Quanto all'uso della TRF "dal vivo", come noto, il futuro regolamento considera "l'uso di sistemi di identificazione biometrica remota 'in tempo reale' in spazi accessibili al pubblico a fini di attività di contrasto" tra i sistemi vietati (art. 5.1.d AI Act). Il regolamento, tuttavia, prevede eccezioni a questo divieto che aprono ad una diffusione di questi strumenti. Le forze di polizia, infatti, potranno impiegare le TRF quando "strettamente necessario" per gli obiettivi di: ricerca delle vittime di alcuni reati gravi; prevenzione di una "minaccia specifica, sostanziale e imminente" alla vita delle persone o un attacco terroristico; perseguimento degli autori o dei sospettati di reati indicati nell'Allegato IIa e puniti negli Stati membri con una determinata pena non inferiore a sei anni.

L'impiego effettivo delle TRF (art. 5.2 AI Act) dovrà inoltre tenere conto di diversi elementi: la natura della situazione che dà origine al possibile utilizzo e le conseguenze per i diritti e le libertà. La polizia dovrà rispettare "le tutele e le condizioni necessarie e proporzionate", per quanto riguarda "le limitazioni temporali, geografiche e personali". Prima del loro utilizzo, e salvo casi di urgenza, i sistemi impiegati dovranno essere sottoposti a una "valutazione di impatto sui diritti fondamentali" e registrati nel database europeo.

Inoltre, ogni singolo utilizzo delle TRF deve essere autorizzato da un'autorità giudiziaria nazionale o da un'autorità amministrativa indipendente (ad eccezione dei casi urgenti, per i quali la convalida deve comunque essere richiesta "senza indebito ritardo"), sulla base di "prove oggettive" e di "indicazioni chiare" in termini di necessità e proporzionalità rispetto agli obiettivi (art. 5.3 AI Act). Nessuna decisione giudiziaria che produce "effetti giuridici negativi" potrà essere presa sulla sola base di un riscontro di questi sistemi. Ogni uso, infine, dovrà essere comunicato all'autorità di sorveglianza del mercato e al garante nazionale per la protezione dei dati.

Gli Stati membri dovranno specificare le regole per la citata autorizzazione e potranno anche prevedere la possibilità di limitare l'impiego delle TRF in relazione ai reati da perseguire (Art. 5.4 AI Act). Le norme nazionali saranno indispensabili, poiché l'AI Act non potrà essere invocato come base giuridica sufficiente ai sensi delle disposizioni della Direttiva di polizia (cons. 23 AI Act.).

Quanto all'uso delle TRF "a posteriori", il nuovo regolamento qualifica tale ipotesi nella categoria degli usi "ad alto rischio" dell'IA (allegato III.1 AI Act). Il nuovo regime si ispira a quello del "New Legislative Framework" e impone numerosi oneri a tutti i partecipanti alla catena del valore. I fornitori, in particolare, prima di poter immettere queste tecnologie sul mercato, devono dimostrare il rispetto di tutti gli obblighi sottoponendo i propri prodotti a una "valutazione di conformità", quale verifica interna che, una volta superata, consente di apporre il marchio CE ai sistemi di IA ad alto rischio (art. 43 AI Act) (European Parliamentary Research Service, *Regulating facial recognition in the EU*, PE 698.021, 2021).

Leggere queste regole dell'AI Act avendo nello sguardo i paletti fissati dal caso Glukhin fa emergere spunti interessanti. Da una parte, se si guarda alla legislazione russa che, con formulazione del tutto generica, consente l'utilizzo "in relazione all'amministrazione della giustizia", è possibile osservare come la normativa europea compia indubbiamente un passo in avanti, fornendo un elenco di reati perseguibili tramite TRF che potrà anche essere ristretto dalla normativa nazionale.

Dall'altra, gli indirizzi della Corte EDU consentono di mitigare alcuni rischi che erano emersi durante le discussioni sulla proposta di regolamento e che riguardano l'ampiezza del rinvio alla disciplina nazionale (I. Barkane, *Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance*, in 27 *Information Polity* 155 (2022)). Quest'ultima, infatti, potrebbe non fornire sufficienti garanzie ai cittadini, ad esempio per quanto riguarda l'intervento dell'autorità giudiziaria o dell'autorità amministrativa indipendente. La sentenza nel caso Glukhin è chiara invece nell'esigere che la normativa nazionale specifichi – come detto – la natura della situazione di impiego concreto, lo scopo perseguito, la categorie di persone coinvolte, nonché prevedere salvaguardie procedurali, come procedure di autorizzazione e riguardanti l'esame, l'uso e la conservazione dei dati, o i meccanismi di supervisione e i rimedi disponibili.

Indicazioni ancor più rilevanti si ricavano per l'uso delle TRF "a posteriori". Come detto, l'AI Act considera queste ultime solamente come sistemi di IA ad "alto rischio". In questo modo si pongono requisiti diversi da quelli previsti per l'uso delle TRF "in tempo reale", poiché non si chiama in causa l'autorità giudiziaria o, di per sé, non si impone una valutazione circostanziata sull'utilizzo concreto che si basi sui principi di proporzionalità e necessità – salvo operare una interpretazione sistematica con la diversa disciplina sulla protezione dei dati personali, che esige invece questo tipo di valutazioni (V.L. Raposo, *The use of facial recognition technology by law enforcement in Europe: A non-Orwellian draft proposal*, in *European Journal on Criminal Policy and Research* 6 ss. (2022)). In base agli indirizzi della sentenza in commento, invece, la Corte EDU è chiara nel declinare in relazione all'uso delle TRF *tout court* l'esigenza di regole chiare, precise e accessibili che disciplinino la portata e l'applicazione delle misure di sorveglianza, più di quanto immediatamente previsto dall'AI Act, anche in termini, ad esempio, di autorizzazione da parte di una autorità giudiziaria o di rimedi disponibili.

8. - La Corte EDU, in definitiva, adotta una sentenza con cui, condivisibilmente, condanna un uso eccessivamente arbitrario di strumenti di sorveglianza invasivi come le TRF. La pronuncia coglie alcuni aspetti problematici che rendono particolarmente insidiose queste tecnologie, come il potenziale uso segreto o le

DPCE online
ISSN: 2037-6677

differenti applicazioni che se ne possono fare, pur rimanendo, tuttavia, ad un livello di genericità tale da rischiare di non fornire indicazioni univoche. Si tratta comunque di indirizzi utili a orientare l'interpretazione di una normativa di prossima approvazione, come l'AI Act, destinata a fornire una cornice regolatoria all'uso delle TRF.

Pur essendo un giudizio legato al caso concreto, la Corte EDU conferma il proprio impegno – testimoniato da ultimo dal caso *Podchasov c. Russia*, n. 33696/19, del 13 febbraio 2024, in tema di accesso alle comunicazioni criptate – nel censurare ogni tipo di legislazione che si riveli insufficiente a proteggere i diritti e limitare gli abusi delle forze dell'ordine, specie nei confronti dell'uso di tecnologie idonee a interferire con i diritti delle persone con una portata amplissima e creare le condizioni illegittime per un regime sorveglianza di massa.

Certo, si tratta di un approccio che manifesta un certo *self-restraint*, in linea con altre decisioni – come quella della Grande Camera nel caso *Big Brother Watch e altri c. Regno Unito*, nn. 58170/13 e altri, del 25 maggio 2021; o la giurisprudenza della Corte di giustizia nel caso *La Quadrature du Net*, C-511/18 e C-512/18, del 6 ottobre 2020 (I. Neroni Rezende, *Glukhin and the EU regulation of facial recognition: Lessons to be learned?*, cit.) – perché comunque non esclude in linea di principio, sulla base di una presunzione assoluta di sproporzionalità, che possano essere ammesse forme di sorveglianza capillari e generalizzate. Proprio alla luce di questa continuità negli indirizzi, però, non pare ci siano i presupposti per affermare che la Corte EDU abbia deciso di adottare un approccio più stringente nei confronti di ordinamenti non democratici, come quello russo.

Piuttosto, gli Stati che intenderanno implementare l'utilizzo di questi strumenti biometrici di riconoscimento dovranno decidere se rimanere o meno nel solco della tradizione del costituzionalismo liberal-democratico (A. Simoncini, *Sovranità e potere nell'era digitale*, in T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (cur.), *Diritti e libertà in Internet*, Firenze, 2017, 26 ss.). In questo caso, occorre la consapevolezza che la semplice possibilità materiale, offerta dal progresso scientifico-tecnologico, non autorizza di per sé il dispiegamento di simili apparati e strumenti, né può fornire il pretesto per cedere ad una forma di "dataismo" che implichi una fiducia cieca e incondizionata verso gli agenti istituzionali che raccolgono, elaborano e utilizzano i dati delle persone per scopi più o meno legittimi (E. Longo, *La ricerca di un'antropologia costituzionale della società digitale*, in *Rivista italiana di informatica e diritto*, 2, 2023, 151).

Giuseppe Mobilio
Dipartimento di Scienze Giuridiche
Università degli Studi di Firenze
giuseppe.mobilio@unifi.it