Tecnologie di riconoscimento facciale e diritti fondamentali a rischio: il caso *Glukhin c. Russia* dinanzi alla Corte europea dei diritti dell'uomo*

Giuseppe Gallo

Corte europea dei diritti dell'uomo, 4 luglio 2023, ric. 11519/20, *Glukhin c. Russia*

Il trattamento dei dati personali del ricorrente, un cittadino russo autore di una manifestazione solitaria di natura pacifica, effettuato tramite strumenti di riconoscimento facciale specificatamente utilizzati per identificarlo e procedere al suo arresto, non può essere ritenuto – secondo la Corte – necessario nel contesto di una società democratica. L'uso di detti sofisticati sistemi di riconoscimento facciale, da parte delle autorità della Federazione Russa, a parere dei giudici, risulta lesivo anche del diritto alla libertà di espressione del ricorrente e appare, di conseguenza, del tutto incompatibile con i valori essenziali di una società democratica – governata dai principi basilari dello stato di diritto – per il cui mantenimento e per il cui sviluppo progressivo la Convenzione stessa è stata concepita.

Sommario

Keywords

tecnologie di riconoscimento facciale – libertà di espressione – art. 10 CEDU – diritto al rispetto della vita privata – art. 8 CEDU

*Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

1. Introduzione

Le tecnologie di riconoscimento facciale consentono di individuare e distinguere un determinato soggetto a partire dall'esatta immmagine del suo volto[1]. Il ricorso a queste peculiari tecnologie di tipo biometrico risulta, nelle società contemporanee, sempre meno costoso e più diffuso, anche per via della versatilità e facilità dei loro impieghi[2].
Tali nuove tecnologie, come recentemente messo in evidenza dalla Corte europea dei diritti dell'uomo, nella sentenza inerente all'affare *Glukhin. c. Russia*, su cui la presente riflessione intende soffermarsi, danno origine a inedite e insidiose forme di sorveglianza di massa[3].
Dette forme di sorveglianza elettronica possono essere perpetrate, a ben vedere, per le più molteplici finalità, tanto da soggetti pubblici quanto da imprese e soggetti privati. Esse sono, quindi, alla portata di chiunque.
In ambito pubblico, le tecnologie in oggetto vengono sfruttate principalmente – ma non solo – dalle forze dell'ordine con la finalità di garantire la sicurezza e tracciare le persone in luoghi pubblici o per perseguire coloro che sono sospettati di un crimine nonché per svolgere controlli alle frontiere e, dunque, come strumento di gestione delle politiche migratorie e di rimpatrio[4].
In ambito privato analoghi strumenti sono a disposizione sia di grandi industrie che di compagnie bancarie o assicurative[5]. Questi sistemi sono inoltre utilizzati per scopi di sicurezza all'interno di comuni esercizi commerciali nonché sovente da un crescente numero di cittadini per effettuare talune tipologie di pagamenti[6].
Nell'uso degli strumenti di riconoscimento facciale, un ruolo di primo piano è svolto, tuttavia, dalle grandi piattaforme del *web* e dai cosiddetti *Big Tech*[7]. Si pensi, a titolo di esempio, al noto sistema *"Rekognition"* di Amazon oppure a quello *"Deepface"* di Face-

---

[1] S. Z. Li - A. K. Jain (eds.), *The Handbook of Face Recognition*, Berlin, 2005; K. A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*, New York, 2011; J. Tanaka, *Face Recognition. The Effects of Race, Gender, Age and Species*, London, 2015; I. Berle, *Face Recognition Technology Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images*, Cham, 2020; P. Dauvergne, *Identified, Tracked, and Profiled. The Politics of Resisting Facial Recognition Technology*, Cheltenham, 2022.

[2] Cfr. *Where is facial recognition used? 11 use cases for facial recognition*, in *Thales*, 11 giugno 2023.

[3] D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, 2002; G. Ziccardi, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015; S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019; D. Lyon, *La cultura della sorveglianza. Come la società del controllo ci ha reso tutti controllori*, Roma, 2020; P. Perri, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Milano, 2020.

[4] Sulle complesse problematiche sollevate, in tema di diritti dei rifugiati, dall'uso di sistemi di riconoscimento facciale come specifico strumento di *governance* delle politiche migratorie e di rimpatrio, si veda, su tutti, L. Jasmontaite-Zaniewicz and J. Zomignani Barboza, *Automated Decisions in Asylum Applications in the EU?* in *International Journal of Refugee Law*, 33, 2021, 89 ss.

[5] G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021, 18.

[6] *Ivi*, 19.

[7] Per quanto concerne i cosiddetti colossi della rete si tende, di solito, ad individuarli nelle americane "GAFA", ovvero Google (e la collegata Alphabet), Amazon, Facebook ed Apple (cui si aggiungono solitamente Microsoft e IBM), e nelle cinesi "BAT" (Baidu, Alibaba e Tencent).

book e, non da ultimo, a quello *"FaceNet"* di Google[8].
Più di recente, nel corso dell'emergenza pandemica da Covid-19, i predetti sistemi di riconoscimento facciale sono stati adottati da alcuni Paesi per misurare la temperatura dei cittadini tra la folla e rilevare coloro che risultassero potenzialmente infetti[9].
Infine, vi sono Stati in cui le tecnologie in questione sono attualmente adoperate, in maniera del tutto sistematica, al fine di realizzare determinate politiche, influenzare il comportamento di massa oppure, addirittura, identificare oppositori politici e minoranze etniche o religiose[10].
Ora, le suddette tecnologie di riconoscimento facciale sono, a ben guardare, in grado di limitare le libertà fondamentali di singoli o dei gruppi sociali a cui essi appartengono e di incidere, su larga scala, sulla tutela di alcuni diritti essenziali, per via delle pervasive capacità di monitoraggio dalle stesse offerte[11].
In quest'ottica, la sentenza della Corte europea dei diritti dell'uomo assume rilevanza in quanto sancisce per la prima volta il principio secondo cui l'uso della tecnologia di riconoscimento facciale, in occasione di manifestazioni pubbliche, ma non solo naturalmente, da parte delle autorità governative, si rivela altamente invasivo e, in determinate circostanze, come quella in esame, potrebbe avere un effetto dissuasivo sull'esercizio di taluni diritti basilari della persona umana quali quello alla libertà di espressione e quello al rispetto della propria vita privata.

2. La vicenda all'origine della sentenza

Il 12 agosto 2019, un attivista politico avente cittadinanza russa, *Konstantin Kotov*, era stato arrestato, ai sensi dell'art. 212, c. 1, del Codice penale della Federazione, con l'accusa di avere ripetutamente violato le norme nazionali in tema di manifestazioni ed eventi pubblici[12]. La susseguente detenzione dello stesso ed il procedimento penale instaurato a suo carico hanno, tuttavia, attirato una grande attenzione sia da parte dei media che da parte dell'opinione pubblica, suscitando una intensa ondata di proteste nell'ambito della società civile[13].
Il 23 agosto dello stesso anno, il ricorrente, *Nikolay Sergeyevich Glukhin*, aveva viaggiato nella metropolitana della città di Mosca con una sagoma di cartone raffigurante il signor *Kotov* che reggeva nelle mani uno striscione in cui lamentava il fatto di essere stato

[8] Cfr. *Facial recognition: top 7 trends (tech, vendors, markets, use cases & latest news)*, in *Thales*, 20 febbraio 202.

[9] Sul punto vedi M. van Natta *et al.*, *The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic*, in *Journal of Law and the Biosciences*, 7, 2020, 1 ss,

[10] È quanto sta avvenendo, ad esempio, con la popolazione palestinese nei territori occupati da Israele, secondo quanto denunciato da un recente rapporto di Amnesty International intitolato *"Israel and Occupied Palestinian Territories: Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT"*. Il rapporto in parola è consultabile all'indirizzo https://www.amnesty.org/.

[11] Riguardo al loro funzionamento, il riconoscimento facciale avviene tramite sofisticati strumenti di rilevazione capaci carpire immagini anche a distanza, in movimento e, di frequente, senza alcuna volontà cooperativa dell'interessato.

[12] *Mosca: 4 anni di reclusione per l'attivista Kotov*, in *Euronews*, 6 settembre 2019.

[13] *Russian court jails protester for 'repeatedly' taking part in rallies*, in *Reuters*, 5 settembre 2019.

condannato per aver preso parte a proteste pacifiche.
Attraverso l'impiego delle tecnologie di riconoscimento facciale installate nelle stazioni della metropolitana[14] e, mediante la visione di taluni audio e video, diffusi sui canali pubblici di *Telegram*, che riprendevano la suesposta scena, l'unità anti-estremismo della polizia di Mosca era riuscita a risalire al ricorrente accusandolo, ai sensi dell'art. 20, c. 2, par. 5, del Codice degli illeciti amministrativi della Federazione, di aver violato la vigente procedura in materia di svolgimento di eventi pubblici.
La normativa in discorso non richiede alcuna notifica preventiva alle competenti autorità statali nelle ipotesi di dimostrazioni individuali, eccezion fatta per i soli casi in cui il manifestante intenda fare uso di «quickly (de)assembled objects»[15].
La polizia ha però ritenuto che la sagoma di cartone utilizzata rientrasse nella citata categoria di oggetti e, conseguentemente, che il ricorrente avrebbe dovuto dare tempestivo preavviso della sua intenzione di svolgere la dimostrazione individuale.
Il tribunale distrettuale *Meshchanskiy* di Mosca, chiamato a pronunciarsi sulla questione, ha giudicato il ricorrente colpevole condannandolo al pagamento di una multa ammontante a 20.000 rubli russi ((RUB), corrispondenti a circa 283 euro[16].
Il ricorrente ha proposto ricorso in appello davanti al tribunale di Mosca contestando di aver svolto una manifestazione pacifica e che la condanna subita violasse il suo diritto alla libertà di espressione[17]. Il tribunale ha però respinto il ricorso avanzato confermando quindi la condanna in appello. Secondo il tribunale l'arresto era da considerarsi legittimo e la raccolta delle relative prove[18] era avvenuta in conformità con quanto contemplato dalla legge sulla polizia[19].
L'interessato si è allora rivolto alla Corte europea dei diritti dell'uomo sostenendo che i suoi diritti di cui all'art. 10 e all'art. 8 della Convenzione europea erano stati violati.

[14] Nel maggio 2017, il sito ufficiale del sindaco di Mosca contava che all'interno della città erano state installate più di 3.500 telecamere di videosorveglianza a circuito chiuso. Nel settembre del medesimo anno, secondo diverse fonti ufficiali, più di 3.000 di queste erano state dotate di un sistema di riconoscimento facciale in tempo reale.

[15] L. n. FZ-54 del 19 giugno 2004, sezione 7(1.1).

[16] L'art. 20, c. 2, par. 5, del Codice degli illeciti amministrativi prevede infatti che la violazione da parte di un manifestante della procedura sullo svolgimento di eventi pubblici, che non abbia tuttavia causato danni alla salute o alla proprietà di nessuno, sia punibile con il pagamento di una multa compresa tra i 10.000 e i 20.000 RUB o, in alternativa, con l'imposizione di un numero massimo di ore di servizio civile pari a 48.

[17] Il ricorrente in particolare lamentava che le attività di ricerca operativa svolte dalla polizia al fine di identificarlo erano da considerarsi illegittime poiché la relativa legge interna non consente tali attività per indagare illeciti di carattere amministrativo come quello in esame ma, al contrario, le ammette solamente in presenza di illeciti aventi natura penale. Come, del resto, affermato dalla Corte costituzione russa nella sentenza n. 86-O del 14 luglio 1998, qualora durante attività di ricerca operativa risulti evidente che l'infrazione oggetto d'indagine non sia classificabile come reato, simili attività devono essere immediatamente interrotte.

[18] A tal proposito, il capitolo 26 del Codice sugli illeciti amministrativi dispone che documenti, registrazioni audio e video, database e qualsiasi altra forma di dati sensibili possono sempre essere impiegati come prove processuali nei procedimenti amministrativi se contengono informazioni rilevanti ai fini della soluzione del caso.

[19] La legge in discorso (l. n. 3-FZ del 7 febbraio 2011) prevede, in generale, che la polizia adotti misure atte a individuare e perseguire gli illeciti amministrativi di sua competenza nonché misure miranti a prevenire e reprimere le attività estremiste.

3. L'attuale impianto normativo internazionale in materia di TFR

Prima di procedere all'analisi della decisione della Corte – esaminati i fatti all'origine della stessa – appare opportuno ricostruire, in via preliminare, lo scarno *corpus* normativo internazionale ed europeo e i numerosi atti di soft law che potrebbero venire in rilievo, nella maggior parte dei casi, quando si discorre di tecniche di riconoscimento facciale.

A tal proposito, occorre ricordare, in primo luogo, il rapporto dell'Alto Commissario per i diritti umani delle Nazioni Unite, del 24 giugno 2020, inerente all'impatto delle suindicate tecnologie sulla promozione e la protezione dei diritti umani nel contesto delle assemblee, ivi comprese le proteste pacifiche[20].

Il rapporto afferma, in sintesi, che il ricorso all'utilizzo della tecnologia di riconoscimento facciale con la sola finalità di identificare tutti coloro i quali prendono parte a una manifestazione pubblica, in assenza di apposite misure di garanzia, può determinare una oggettiva violazione del diritto alla privacy nonché una lesione delle libertà di espressione e di riunione pacifica. Secondo il suddetto rapporto l'immagine di un individuo costituisce, a tutti gli effetti, uno degli elementi chiave della sua personalità, in quanto rivela quell'insieme di caratteristiche fisiche uniche che concorrono a contraddistinguerlo dai suoi pari. Di conseguenza, la raccolta delle immagini del volto di una persona, effettuata in mancanza del suo esplicito consenso, costituisce una violazione del suo diritto alla privacy. Pertanto, qualsiasi utilizzo di sistemi di riconoscimento facciale dovrebbe necessariamente essere soggetto a idonei meccanismi di supervisione, sia di natura giudiziaria che non giudiziaria[21].

Nell'ambito del Consiglio d'Europa assumono rilevanza le linee guida in tema di riconoscimento facciale, adottate il 28 gennaio 2021, nella Giornata europea per la protezione dei dati personali, dal Comitato Consultivo della Convenzione per la protezione delle persone rispetto al trattamento automatizzato dei dati personali del 1981[22].

Tali linee guida[23] si fondano sui principi del Protocollo di modifica alla citata Convenzione adottato il 18 maggio 2018 a Elsinore (cosiddetta Convenzione 108+)[24]. Esse forniscono un'ampia serie di misure di riferimento che governi, sviluppatori e produttori di siffatti strumenti di riconoscimento facciale nonché enti pubblici e fornitori di servizi dovrebbero adottare al fine di garantire che il loro impiego non pregiudichi

[20] UN Doc. A/HRC/44/24.

[21] Il rapporto sottolinea come l'impiego di sistemi di riconoscimento facciale, nel contesto delle assemblee, comporti una lesione del diritto alla privacy su vasta scala, poiché permette la raccolta indiscriminata del volto di tutti i soggetti catturati dalla telecamera dotata o collegata a un simile modello di riconoscimento.

[22] La Convenzione (comunemente nota anche come Convenzione 108) è stata ratificata, in Italia, con la legge del 21 febbraio 1989 n. 98. Essa riveste centrale importanza poiché copre il trattamento dei dati in tutti i settori, sia pubblici che privati.

[23] Cfr. Consultative Committee of the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data - Convention 108, *Guidelines on Facial Recognition*, 28 January 2021.

[24] L'Italia ha ratificato la suindicata Convenzione che tuttvia non è ancora entrata in vigore.

la dignità della persona, i suoi diritti e le sue libertà fondamentali. Le suindicate linee guida coprono tutti gli impieghi delle tecnologie in parola e statuiscono, in sostanza, che la loro integrazione nei sistemi di sorveglianza preesistenti rappresenta un serio rischio per il diritto alla privacy così come per altri diritti essenziali della persona dal momento che il loro funzionamento molto spesso non richiede la consapevolezza o la cooperazione dei soggetti i cui dati biometrici vengono trattati.

Un importante riferimento alle tecnologie di riconoscimento facciale è altresì contenuto nel testo del Regolamento sull'Intelligenza Artificiale proposto dalla Commissione europea nell'aprile 2021 e approvato, con diversi emendamenti, dal Parlamento in sessione plenaria nel giugno 2023[25].

Infine, merita di essere rammentato il focus dell'Agenzia per i diritti fondamentali (FRA) dal titolo *"Facial recognition technology: fundamental rights considerations in the context of law enforcement"*. Lo studio elenca una serie di diritti della persona su cui le suesposte tecnologie sarebbero in grado di incidere e con quali modalità ciò possa concretamente verificarsi[26]. Tra i diritti elencati rientrano l'emergente diritto ad un buon governo[27], il consolidato diritto a non subire discriminazione[28] e, da ultimo, la libertà di associazione e di riunione[29].

Tra le libertà su cui le tecnologie di riconoscimento facciale sarebbero maggiormente in grado di impattare deve essere annoverata, a nostro avviso, anche la libertà di manifestazione del pensiero, verso la quale le libertà di riunione e di associazione possiedono una dimensione e una funzione strutturale. Come affermato dal Consiglio per i diritti umani delle Nazioni Unite nel rapporto del 2019 sul ricorso da parte degli Stati a tecniche di sorveglianza sempre più sofisticate, queste tecnologie possono svolgere un notevole effetto deterrente e inibitorio anche sul versante della libertà di manifestazione del pensiero[30].

---

[25] Sul punto vedi A. Alaimo, *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso ilpensiero pessimistico?*, in *Federalismi.it*, 2023, 133 ss.

[26] Cfr. Fundamental Rights Agency, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27 November 2019.

[27] Il diritto ad una buona amministrazione, nel contesto in oggetto, implica in favore dei destinatari di misure di riconoscimento facciale la titolarità di una vasta categoria di diritti quali quello di accesso agli atti, quello di essere sentiti, il diritto di ottenere una decisione motivata da parte del potere pubblico interessato e, ancora, quello di difesa attraverso un giudice. Il diritto ad un ricorso effettivo davanti a un organismo giurisdizionale copre invero anche le decisioni e le misure assunte con il supporto delle tecnologie di riconoscimento facciale.

[28] I test condotti sugli algoritmi di riconoscimento facciale hanno dimostrato come vi sia un incremento del tasso di errore in relazione alla maggiore o minore età dei soggetti i cui dati biometrici sono oggetto di trattamento. Come osservato nel rapporto, le TFR potrebbero produrre, a causa del loro peculiare funzionamento, anche discriminazioni nei confronti degli individui in base al sesso o alla razza e avere conseguenze sfavorevoli sulle persone affette da disabilità. Un algoritmo di riconoscimento facciale potrebbe oltretutto non valutare accuratamente le caratteristiche di un determinato gruppo demografico con la conseguenza che date minoranze etniche potrebbero essere esposte a un maggior numero di controlli da parte delle forze dell'ordine.

[29] Gli effetti negativi dell'uso di tale tecnologia sulla libertà di associazione sono di enorme portata. Numerose persone invero potrebbero sentirsi scoraggiate dal manifestare in luoghi pubblici ed esprimere liberamente le proprie opinioni nel timore di essere identificate e subire conseguenze negative.

[30] Cfr. Human Rights Council, A/HRC/41/35, *Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 28 May 2019.

4. L'articolata decisione della Corte

Passando all'esame della sentenza, la Corte ha prima di tutto accertato la propria competenza rispetto alla particolare situazione russa. Constatato che le presunte violazioni si sarebbero verificate antecedentemente al 16 settembre 2022, data in cui la Federazione Russa ha cessato, come noto, di essere parte contraente della Convenzione, i giudici hanno ritenuto il ricorso ammissibile poiché né manifestamente infondato né tanto meno irricevibile ai sensi dell'art. 35[31].

Come chiarito nel caso *Ucraina e Paesi Bassi c. Russia*, gli artt. 38, 41 e 46 della Convenzione, continuano a trovare piena applicazione anche dopo la data in questione e, di conseguenza, l'eventuale mancata partecipazione del Governo russo nei procedimenti che lo coinvolgono non impedisce ai giudici di Strasburgo di proseguire con l'esame delle domande pendenti avanzate contro di esso[32].

Ciò poiché – come ricordato nel caso *Svetova e altri c. Russia*[33] – ai sensi dell'art. 58, par. 2, della Convenzione la denuncia di uno Stato membro della stessa «non può avere l'effetto di svincolare l'Alta Parte contraente interessata dagli obblighi contenuti nella presente Convenzione per quanto riguarda qualunque fatto suscettibile di costituire una violazione di tali obblighi, da essa posto in essere anteriormente alla data in cui la denuncia è divenuta efficace»[34].

Una volta stabilita la sua giurisdizione, la Corte ha poi proseguito con l'accertamento della presunta violazione, da parte delle autorità governative russe, sia della libertà di espressione del ricorrente che del suo diritto al rispetto della propria vita privata.

Per quanto riguarda la contestata violazione dell'art. 8, i giudici hanno ribadito, in primo luogo, come la nozione di "vita privata" sia un concetto piuttosto ampio e, come tale, non suscettibile di un'unica definizione[35].

---

[31] Le condizioni di ricevibilità dei ricorsi dinanzi alla Corte europea dei diritti dell'uomo sono rispettivamente: il previo esaurimento dei ricorsi interni da parte dell'individuo ricorrente o da parte dell'individuo vittima della violazione e la presentazione del ricorso entro il termine perentorio di quattro mesi, decorrente dalla data di ricevimento della notifica della decisione finale interna. Inoltre, nei ricorsi individuali si richiede altresì che il ricorso proposto non sia anonimo, non riguardi una questione già presentata davanti alla Corte o ad un altro organo internazionale di controllo e, ancora, che non costituisca un abuso del diritto di ricorso. Infine, una condizione di ricevibilità che è stata aggiunta di recente è quella secondo cui il ricorrente debba poi aver subito un significativo pregiudizio. Sul funzionamento della Corte europea dei diritti dell'uomo si veda, in generale, P. van Dijk (ed.), *Theory and Practice of the European Convention on Human Rights*, Antwerpen, 2018; D. J. Harris (ed.), *Law of the European Convention on Human Rights*, Oxford, 2018; A. Nussberger, *The European Court of Human Rights*, Oxford, 2020.

[32] CEDU, Grande Camera, *Ucraina e Paesi Bassi c. Russia*, ric. 8019/16 (2022), § 435 ss.

[33] CEDU, *Svetova e altri c. Russia*, ric. 54714/17 (2023), § 39.

[34] Inoltre, in base al par. 3 della citata disposizione «alla stessa condizione, cesserebbe d'esser parte alla presente Convenzione qualunque Parte contraente che non fosse più membro del Consiglio d'Europa». La versione italiana del testo della Convenzione è reperibile al link *echr.coe.int*.

[35] La concezione di "vita privata" non si limita, invero, alla sola integrità fisica, mentale o morale del soggetto, ma si estende anche a quelle interferenze suscettibili di ledere la sua identità sociale. In altri termini, l'art. 8 della Convenzione non si limita al solo diritto alla riservatezza, inteso come diritto a non vedere apprese e diffuse notizie inerenti alla propria sfera privata, ma ricomprende anche il diritto per l'individuo di condurre una "vita sociale privata", cioè la possibilità di stabilire e sviluppare rapporti con altri individui, anche beninteso nell'ambito della pluralità di attività che si svolgono in un contesto

Sulla base di questa premessa, hanno evidenziato che qualsiasi ingerenza nella sfera privata dell'individuo può essere giustificata ai sensi dell'art. 8, par. 2, solo se è conforme alla legge, persegue uno o più degli scopi legittimi in esso contenuti e appare, infine, necessaria in una società democratica per raggiungere tali scopi[36].

A tal proposito, la Corte ha ritenuto che «the questions of lawfulness and of the existence of a legitimate aim cannot be dissociated from the question of whether the interference was "necessary in a democratic society."» e – per tale ragione – «It will therefore examine them together…»[37].

Nella misura in cui il ricorrente ha sostenuto che il diritto interno non soddisfacesse il requisito della "qualità del diritto", i giudici hanno affermato come sia essenziale – nel contesto della tecnologia di riconoscimento facciale – disporre di norme sufficientemente dettagliate che disciplinino la portata e l'applicazione delle misure assunte e, allo stesso tempo, di forti garanzie contro il fondato rischio di eventuali abusi[38]. Essa ha rilevato, riguardo questo primo punto, che la legge statale russa non definiva affatto la finalità e i destinatari della raccolta dei dati, le circostanze che legittimano tale raccolta, le informazioni di cui è rispettivamente ammessa o vietata la memorizzazione, le procedure da seguire per la raccolta o, ancora, la durata della conservazione dei dati elaborati. Inoltre, il governo russo non aveva disposto alcuna garanzia di tipo procedurale che accompagnasse l'utilizzo della tecnologia di riconoscimento facciale nel suo territorio[39].

La Corte ha evidenziato come la questione oggetto del contendere non era se l'uso di tecniche di riconoscimento facciale possa ritenersi ammesso ai sensi della Convenzione bensì, in specie, se il trattamento dei dati personali[40] del ricorrente, tramite detta sofisticata tecnologia, era giustificabile ai sensi dell'art. 8, par. 2, e dunque necessario in una società democratica[41].

Uno dei fattori da tenere in conto ai fini di questa valutazione è la natura e la gravità delle offese poste in essere[42].

A tal proposito, la Corte ha osservato che il ricorrente era stato perseguito soltanto per un illecito minore classificato, peraltro, come illecito amministrativo e non come reato ai sensi dell'ordinamento russo[43].

Di conseguenza, la Corte ha concluso che l'utilizzo della tecnologia di riconoscimento

pubblico (CEDU, *Pretty c. Regno Unito*, ric. 2346/02 (2002), § 61).

36 Cfr. § 74.

37 Cfr, § 78.

38 Cfr. § 82.

39 Cfr. § 83.

40 Si ricorda che, ai sensi dell'art. 2, lett. *a)*, della direttiva 95/46/CE, i dati personali sono definiti come «qualsiasi informazione concernente una persona identificata o identificabile» mediante «riferimento ad uno o più elementi caratteristici della sua identità fisica, fisiologica, psichica, economica, sociale o culturale». Diversi sono poi i cosiddetti dati sensibili, ossia quei dati personali che rivelano l'origine razziale o etnica, le convinzioni religiose o filosofiche, le opinioni politiche, le appartenenze sindacali o che sono relativi alla salute o alla vita sessuale dell'individuo.

41 Cfr. § 85.

42 CEDU, *P. N. c. Germania*, ric. 74440/17 (2020), § 72.

43 Cfr. § 88.

facciale per identificare il signor *Glukhin* non corrispondeva a un "urgente bisogno sociale"' e costituiva, per tale motivo, una grave violazione del suo diritto alla privacy e alla protezione dei dati personali ai sensi dell'art. 8[44].

Con riferimento alla violazione dell'art. 10 la Corte di Strasburgo ha invece ribadito – in primo luogo – il principio secondo cui la protezione offerta dalla norma in commento non si limiterebbe soltanto all'insieme delle idee manifestate, nella realtà fenomenica, tramite il mero linguaggio orale o scritto, dal momento che le opinioni possono essere da chiunque espresse anche attraverso strumenti di comunicazioni non verbali o mediante determinati comportamenti[45].

Data la natura della condotta del ricorrente e il contesto in cui questa è stata attuata, i giudici hanno ritenuto che l'interessato, attraverso le sue azioni, abbia unicamente provato ad esprimere la propria opinione su una questione di interesse pubblico, rispetto alla quale le restrizioni prescritte nel secondo paragrafo dell'art. 10 ricevono, in concreto, scarsa applicazione[46].

Secondo il ragionamento seguito dai giudici, anche ammettendo che l'ingerenza potesse essere considerata conforme alla rilevante normativa statale perseguendo uno degli obiettivi legittimi della «difesa dell'ordine e prevenzione dei reati» o della «protezione della reputazione e dei diritti altrui», essa non appariva però «necessaria» in «una società democratica»[47].

La dimostrazione individuale del ricorrente, infatti, si era svolta in modo pacifico. L'illecito per cui il medesimo è stato condannato – come predetto – consisteva soltanto nell'omessa dovuta notifica, alle autorità nazionali competenti, della manifestazione tenuta[48].

Non è stato dimostrato che le azioni del ricorrente abbiano causato una grave perturbazione nello svolgimento della vita pubblica in misura superiore a quella ordinaria, né tanto meno che esse abbiano rappresentato un reale pericolo per l'ordine pubblico o la sicurezza nazionale nonché quella dei trasporti. Pertanto, i giudici – in mancanza di ulteriori elementi aggravanti – non hanno rinvenuto pertinenti o sufficienti ragioni suscettibili di giustificare l'interferenza subita dal ricorrente nel godimento del suo diritto alla libertà di espressione[49].

---

[44] Cfr, § 89.

[45] CEDU, *Karuyev c. Russia*, ric. 4161/13 (2022), § 18.

[46] Cfr. § 51.

[47] Se si guarda alla passata giurisprudenza della Corte in questa materia, si può desumere come i limiti imposti dagli ordinamenti interni, affinché possano essere valutati come strettamente necessari in una società democratica, devono essere statuiti da una normativa che li renda prevedibili ai loro potenziali destinatari, devono rispondere poi ad un bisogno sociale effettivo e preminente, apparire proporzionati allo scopo legittimo perseguito (bilanciando, di volta in volta, i diversi interessi in gioco) nonché risultare motivati in maniera convincente ed adeguata.

[48] M. Zalnieriute, *Glukhin v. Russia. App. No. 11519/20. Judgment*, in *AJIL*, 117, 2023, 697.

[49] Cfr. § 56.

5. Osservazioni conclusive

Alla luce della disamina appena svolta, è possibile, a nostro giudizio, affermare che la sentenza – la quale rappresenta il primo caso in cui le tecnologie di riconoscimento facciale siano state portate davanti ad un tribunale internazionale per dar conto delle comprovate limitazioni ai diritti essenziali che esse sono in grado di provocare – costituisca indubbiamente un importante precedente nella futura giurisprudenza della Corte sul tema della sorveglianza di massa.

Per quanto concerne la violazione dell'art. 8, abbiamo visto come i giudici di Strasburgo abbiano dichiarato pienamente applicabile anche per le suesposte tecniche di sorveglianza elettronica il principio – in precedenza affermato, ad esempio, nel caso *S. e Marper c. Regno Unito* – secondo cui al fine di valutare se le limitazioni alla tutela della vita privata e alla protezione dei dati di carattere personale siano legittime occorre congiuntamente, oltre ad una chiara e precisa previsione normativa, che la restrizione posta sia realmente «necessaria» all'interno di «una società democratica» per il perseguimento dei fini elencati nel testo dell'art. 8 della Convenzione. Per effettuare una corretta valutazione su quest'ultimo punto essenziale, l'ingerenza deve ritenersi ammessa solamente se risponde ad un bisogno sociale imperativo, se risulta proporzionata allo scopo legittimo perseguito nonché se le motivazioni addotte dalle competenti autorità nazionali per giustificare la sua applicazione appaiono oggettivamente rilevanti, pertinenti e sufficienti.

Con riferimento all'accertata lesione della libertà di espressione del ricorrente invece la Corte ha sostenuto che, pur volendo ammettere che il caso possa aver superato con esito positivo il test di legalità di cui all'art. 10, par. 2, della Convenzione, la manifesta limitazione della libertà in commento non può certamente considerarsi strettamente necessaria nel contesto di una società democratica. La restrizione lamentata dal ricorrente è illegittima poiché sproporzionata in funzione dell'obiettivo legittimo perseguito, nella specie, completamente assente o, comunque, particolarmente difficile da individuare.

Dalla pronuncia è allora possibile desumere il principio fondamentale in base al quale le summenzionate misure di riconoscimento facciale dovrebbero essere impiegate solo se legali, giustificate da un obiettivo legittimo necessario, proporzionato e adeguatamente motivato. In particolare, ci sembra che la Corte abbia respinto una mera qualificazione astratta dei motivi di ordine pubblico, richiedendo una verifica caso per caso, con la conseguenza che un generale utilizzo delle tecniche di riconoscimento facciale per motivi di ordine pubblico non sembra compatibile con alcuni diritti convenzionali se l'utilizzo concreto comporta una limitazione dei diritti umani.

Come abbiamo visto, gli strumenti di riconoscimento facciale hanno un forte impatto, diretto o indiretto, su tutta una serie di diritti fondamentali, sanciti sia a livello interazionale sia sul piano dell'Unione Europea, che possono andare ben oltre il diritto alla privacy e alla protezione dei dati personali, come tali intendendosi, ad esempio, il diritto a non subire discriminazioni, la libertà di movimento, la libertà di riunione e di associazione nonché quella di espressione e di opinione.

Ne consegue, così, che i governi che decidono di ricorrere all'impiego di una siffatta tecnologia devono, a nostro avviso, assicurarsi di farlo sulla base di un quadro norma-

tivo interno solido e conforme agli standard previsti dai principali trattati posti a tutela dei diritti umani, che contenga puntuali disposizioni idonee a proteggere efficacemente tutti i dati personali e sensibili, anche beninteso le immagini facciali e le informazioni private da esse derivanti. Tutte le persone interessate dovrebbero avere, inoltre, il diritto di accesso a tali informazioni nonché quello di chiederne la legittima rettifica o la cancellazione immediata, se necessario, qualora la loro raccolta sia stata effettuata in assenza di un'adeguata motivazione e, soprattutto, nella totale inosservanza del suindicato tripartito test di legalità, necessarietà e proporzionalità. Resta da vedere se la Corte confermerà quest'orientamento[50].

[50] La pronuncia è definitiva ma non è escluso che in altri casi vi sia l'intervento della Grande Camera.