Il riconoscimento facciale sul "banco" degli imputati. Riflessioni a partire, e oltre, Corte EDU *Glukhin c. Russia*

Costanza Nardocci*

CHALLENGING FACIAL RECOGNITION SYSTEMS BEFORE COURTS. FROM AND BEYOND ECTHR *GLUKHIN V. RUSSIA*

ABSTRACT: The Article examines the first judgment delivered by the European Court of Human Rights against Russia on the use of facial recognition systems, finding a violation of Articles 8 and 10 ECHR. The Article frames the discussion in the context of the recent developments in the regulation of artificial intelligence technologies, alongside a comparative analysis of a number of judgments issued by a selection of European and non-European States. The paper highlights the approach of the EDU Court towards the use of biometric identification systems to verify whether, and to what extent, these systems comply with the fundamental rights set forth under the European Convention.

KEYWORDS: Facial Recognition; European Court of Human Rights; private life; interference; risks

ABSTRACT: Il saggio analizza la prima pronuncia della Corte europea dei diritti dell'uomo di condanna della Russia per l'impiego di sistemi di riconoscimento facciale, accertando la violazione degli articoli 8 e 10 CEDU. L'articolo inquadra la disamina nel contesto degli sviluppi in tema di regolamentazione delle tecnologie di intelligenza artificiale, proponendo anche un raffronto con alcune pronunce decise a livello domestico da alcuni Stati europei ed extra-europei. Il saggio pone in evidenza l'orientamento della Corte EDU di fronte all'impiego dei sistemi di identificazione biometrica al fine di verificare se, e se sì in quale misura, tali sistemi siano rispettosi dei diritti convenzionali.

PAROLE CHIAVE: Riconoscimento facciale; Corte europea dei diritti dell'uomo; vita privata; interferenza; rischi

SOMMARIO: 1. Il riconoscimento facciale tra Consiglio d'Europa e Unione Europea: considerazioni di apertura – 2. Una Corte sovranazionale censura, per la prima volta, un sistema di riconoscimento facciale: *Glukhin c. Russia* – 3. Interferenza illegittima nella vita privata, ma assenza di incompatibilità ipso iure con la Convenzione: dove si

* *Professoressa associata in Diritto costituzionale, Dipartimento di diritto pubblico italiano e sovranazionale, Università degli Studi di Milano. Mail: costanza.nardocci@unimi.it.* *Contributo sottoposto a doppio referaggio anonimo.*

ISSN 2284-4503

va? – 3.1. Una sentenza "*Country-Specific*"? Quanto "conta" il carattere autoritario dello Stato – 4. Oltre la giurisprudenza convenzionale: altre risposte e altre condanne in prospettiva comparata – 5. Conclusioni: tempo di convergenze "continentali"?

1. Il riconoscimento facciale tra Consiglio d'Europa e Unione Europea: considerazioni di apertura

Il 2023 sarà ricordato per le numerose iniziative e novità, che hanno investito i tentativi di regolamentazione dei sistemi di intelligenza artificiale. Dal continente europeo, a quello asiatico, agli Stati dell'America del Nord, per tutti Canada e Stati Uniti, si sono registrati numerosi avvicendamenti caratterizzati, però, almeno da tre dati essenziali.

Il primo attiene al definitivo (per ora?) abbandono dell'approccio, inizialmente sostenuto oltreoceano, favorevole alla *self-regulation* delle tecnologie di intelligenza artificiale, sul presupposto della esigenza di non imbrigliare entro un quadro legislativo potenzialmente rigido lo sviluppo di tali sistemi, con un deciso spostamento dell'attenzione in favore di modalità più o meno strutturate di positivizzazione di norme di legge volte a disciplinarne l'impiego soprattutto nella sfera pubblica. Il secondo investe il metodo.

Se sul fronte asiatico e nord-americano, prevale una impostazione che vuole lo Stato protagonista della definizione della legislazione da adottare in materia, con una concentrazione quindi della potestà legislativa a livello domestico, il continente europeo ha, invece, abbracciato una tendenza di segno opposto. Ciò vale sia per gli Stati membri dell'Unione Europea, sia per quelli contraenti del Consiglio d'Europa, che hanno mantenuto negli ultimi anni una posizione comune a carattere, potrebbe dirsi, "attendista" e deferente rispetto a scelte, sì, negoziate, ma, in fondo, demandate integralmente al livello sovranazionale. Un livello sovranazionale che, come si avrà modo di approfondire, tra l'accordo raggiunto sull'*Artificial Intelligence Act* (c.d. *AI Act*) del 9 dicembre 2023 da parte dell'Unione Europea[1], poi riconfermato nel febbraio del 2024[2], e la pubblicazione del *Committee on Artificial Intelligence* (CAI) del Consiglio d'Europa del *Consolidated Working Draft*[3] del primo trattato in tema di IA, ha finalizzato tra il 2023 e il 2024 i testi più significativi e, forse, questo lo dirà il 2024, in modo addirittura definitivo.

[1] Per una sintesi dell'accordo raggiunto e che fa seguito a più di due anni di negoziazione dopo la presentazione della prima proposta di Regolamento del 21 aprile 2023, si veda il seguente link: https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/.

[2] Il riferimento è alla approvazione unanime del testo dell'*AI Act* da parte del Consiglio dei Ministri dell'Unione Europea in data 2 febbraio 2024.

[3] Il testo può essere consultato al seguente link: https://rm.coe.int/cai-2023-18-consolidated-working-draft-framework-convention/1680abde66. Per un commento, anche in prospettiva comparativa, tra l'azione delle istituzioni europee e del Consiglio d'Europa, per opera del CAI, si consenta il rinvio a C. NARDOCCI, *Artificial intelligence at the crossroads between the European Union & the Council of Europe: who safeguards what & how?*, in *Italian Journal of Public Law*, 2024, in corso di pubblicazione. Più in generale, approfondiscono, tra gli altri, le criticità del ricorso a sistemi di intelligenza artificiale nel quadro della dottrina costituzionale nazionale, C. CASONATO, *Intelligenza artificiale e giustizia: potenzialità e rischi*, in *DPCE Online*, 2020, 3369 ss. e, dello stesso A., anche, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *DPCE*, 2019, 101 ss.; F. DONATI, *Intelligenza artificiale e giustizia*, 2020, 415 ss.; A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *Rivista di BioDiritto*, 2019, 3 ss.; B. CARAVITA, *Principi costituzionali e intelligenza artificiale*, in U. RUFFOLO (a cura

Il terzo elemento da sottolineare attiene, infine, alla *ratio* delle differenti discipline oggetto di discussione ai vari livelli, siano essi nazionali oppure sovranazionali.

Eterogenee tra di loro sono, così, le esigenze sottese alle regolamentazioni adottate oppure in corso di approvazione. Se il continente europeo ha pressoché da sempre guardato al fenomeno dell'intelligenza artificiale con qualche diffidenza tentando, non senza difficoltà e contraddizioni, di delinearne i rischi sul piano del suo impatto sulla società e sui diritti delle persone, diversa è stata ed è tuttora la *ratio* alla base delle ipotesi normative discusse ed approvate negli altri continenti. Non necessariamente, cioè, sono emerse, in modo analogo oppure non sempre, esigenze di tutela dei diritti umani di fronte a tecnologie considerate "sospette" o, seguendo la terminologia ormai diffusa a livello continentale europeo, "ad alto rischio"[4]. In Cina, ad esempio, l'ultima regolamentazione in materia di c.d. "*Generative AI*" dell'agosto 2023 continua a preferire ad una impostazione *human-centered* oppure *human rights-based* un massiccio controllo statale sulle tecnologie di IA, più che una sensibilità ai pregiudizi che ne potrebbero derivare a scapito della società e dei singoli individui[5]. Gli Stati Uniti, da parte loro, mostrano un andamento ondivago, non omogeneo anche in ragione di alcune iniziative autonome intraprese dai singoli Stati, sebbene i recenti *Executive Orders* del Governo federale mostrino una progressiva consonanza con l'approccio europeo, cioè una minore tensione verso la *self-regulation* dei sistemi di IA[6].

Non meno interessanti, infine, sono i tentativi di ricondurre ad unità la disciplina del fenomeno, come si è tentato di fare in occasione del *Global Summit* di novembre 2023, a cui ha fatto seguito la c.d. dichiarazione di *Bletchley*[7].

---

di), *Intelligenza artificiale*, *Il diritto, i diritti, l'etica*, Giuffrè, Milano, 451 ss.; T. GROPPI, *Innovazione tecnologica e intelligenza artificiale*, in *Giurcost.*, 2020, 675 ss.

[4] Più di recente, sulla impostazione europea, si sono espresse anche le Nazioni Unite nel dicembre 2023 tramite il c.d. *Interim Report* dal titolo "Governing AI for Humanity", reperibile al seguente link: *https://www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf*. Interessa, in particolare, segnalare la preferenza mostrata dalle Nazioni Unite per una impostazione che, più che individuare *ex ante* le tecniche di IA da vietare, si preoccupi di definire quali sono i beni giuridici e le categorie meritevoli di protezione. Si veda, in questo senso, il par. 30.

[5] Si veda, in tema, la recente disciplina approvata nell'agosto del 2023, che segue una serie di iniziative adottate negli anni precedenti. Per una ricostruzione della regolamentazione esistente in epoca precedente l'approvazione della legge in esame, si veda il Report pubblicato da CEIMIA, *A comparative Framework for AI Regulation Policy*, febbraio 2023, consultabile al seguente link: *https://ceimia.org/wp-content/uploads/2023/05/a-comparative-framework-for-ai-regulatory-policy.pdf*. Il testo della nuova regolamentazione cinese, in lingua originale, può essere letto al seguente link: *http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm*.

[6] Il riferimento è, anzitutto, all'*Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, del 30 novembre 2023 il cui testo può essere consultato al seguente link: *https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/#:~:text=The%20Executive%20Order%20establishes%20new,around%20the%20world%2C%20and%20more*.

[7] La Dichiarazione è stata adottata all'esito del *Global AI Safety Summit*, svoltosi in data 1-2 novembre 2023. Il testo della Dichiarazione può essere consultato al seguente link: *https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023*.

Se qualcuno è mancato all'appello, almeno sino all'agosto del 2023, sono state le Nazioni Unite[8]. Oltre ad alcune preliminari linee guida, non ha mai voluto varcare la soglia della regolamentazione dell'intelligenza artificiale, lasciando al Consiglio d'Europa il ruolo di prima organizzazione di diritto internazionale dei diritti umani ad occuparsi in modo specifico del tema in esame. Viceversa, seguendo l'impostazione già sperimentata dal Consiglio d'Europa, nell'agosto del 2023, e per la prima volta, anche le Nazioni Unite hanno avviato la costituzione di un organismo *ad hoc*, denominato *High-Level Advisory Body on Artificial Intelligence*, che ha avviato le prime consultazioni nel novembre del 2023[9].

Se le precedenti riflessioni hanno interessato le relazioni "istituzionali" tra intelligenza artificiale, diritto e diritti, il discorso muta in parte se si volge lo sguardo alle problematiche proprie delle metodiche *machine learning* e ai sistemi di riconoscimento facciale[10], in particolare.

Su queste tecnologie di intelligenza artificiale, il dibattito è stato piuttosto acceso, soprattutto in considerazione dell'utilizzo sempre più massiccio di tali sistemi per ragioni di sorveglianza pubblica[11], dove le esigenze di sicurezza dovrebbero essere adeguatamente bilanciate con diritti fondamentali di primo piano, dalla *privacy*, all'eguaglianza, all'autodeterminazione individuale[12], sino ai classici diritti ad esercizio collettivo, come le libertà di riunione e di associazione.

---

[8] Sulle precedenti iniziative adottate dalle Nazioni Unite, si rinvia al Report *United Nations Activities on Artificial Intelligence (AI)*, 2022, che può essere letto nella sua versione integrale al seguente link: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2022-PDF-E.pdf.

[9] Maggiori dettagli sulle attività dello *High-Level Advisory Body on Artificial Intelligence* possono essere consultate al seguente link: https://www.un.org/techenvoy/ai-advisory-body.

[10] Sulle implicazioni in punto di tutela dei diritti umani derivanti dal ricorso a sistemi di identificazione biometrica, si vedano i rapporti della FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, consultabile al seguente link: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf; in dottrina, tra gli altri, si rinvia a D. DUSHI, *The Use of Facial Recognition Technology in EU Law Enforcement: Fundamental Rights Implications*, in *Policy Brief*, 2020, reperibile al seguente link: https://repository.gchumanrights.org/server/api/core/bitstreams/51d86ab3-1cb5-45f6-b141-64c06dcef5d8/content; E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto penale uomo*, 2022, 1 ss., che si sofferma in modo particolare sulle implicazioni che derivano nella prospettiva del diritto penale, così come, anche, M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale*, 2022, 23 ss. Più ampiamente, e nel quadro della dottrina costituzionalistica, si rinvia, diffusamente, a G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021. Per un approfondimento nella letteratura anglosassone delle problematiche proprie di tali tecnologie di intelligenza artificiale in prospettiva globale, si rinvia a P. DAUVERGNE, *Identified, Tracked, and Profiled. The Politics of Resisting Facial Recognition Technology*, Regno Unito, 2022.

[11] Emblematico di questa tendenza l'esempio cinese. In questo senso, lo *High Commissioner for Human Rights* delle Nazioni Unite nel 2022 ha dichiarato che il Governo cinese ha sviluppato e utilizza un «sophisticated, large-scale and systematized surveillance system" which scrutinises online and offline behaviour, and is "driven by an ever-present network of surveillance cameras, including deploying facial recognition capabilities». Si veda il report *Assessment of Human Rights Concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China*, consultabile nella sua versione integrale al seguente link: https://www.ohchr.org/sites/default/files/documents/countries/2022-08-31/22-08-31-final-assesment.pdf.

[12] Il tema delle implicazioni sul piano dei diritti fondamentali del ricorso all'utilizzo di sistemi di riconoscimento facciale è discusso in letteratura. Tra i molti, si rinvia di recente a D. MURRAY, *Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework*, in *The Modern Law Review*, 2023, 1 ss., che distingue in due categorie le tipologie di violazioni dei diritti umani, separando, da un lato, la lesione del diritto alla *privacy*, dai c.d. "chilling effects" di lungo termine

Nonostante si siano susseguiti tentativi tesi a porre in discussione la fruibilità del ricorso a tali tecnologie, il 2023 si conclude con alcuni punti fermi almeno sul versante europeo.

Ci si riferisce, anzitutto, alla presa di posizione dell'Unione Europea che non ha disposto il divieto assoluto dell'impiego di tali sistemi nella versione dell'*Artificial Intelligence Act* su cui il Parlamento e il Consiglio hanno raggiunto un accordo nel dicembre del 2023, poi seguito dall'approvazione da parte del Consiglio dei Ministri dell'UE del 26 gennaio del 2024[13], inquadrandole piuttosto, nel novero dei sistemi c.d. «ad alto rischio». Di diverso avviso è stata, invece, la presa di posizione dello *High Commissioner for Human Rights* delle Nazioni Unite, che ha qualificato le tecnologie in esame come «*particularly high-risk*», discostandosi in parte dall'impostazione dell'*AI Act*, ma accorciando allo stesso tempo le distanze nella parte in cui suggerisce, analogamente a quanto prevede ad oggi la versione ultima dell'AI Act, l'istituzione di un *International Advisory Board* operante a livello globale per il monitoraggio di tali sistemi[14].

che andrebbero, viceversa e dall'altro, ad investire una pluralità di diritti ulteriori simultaneamente, in particolare 8 ss. Si tratta, in altri termini, di pregiudizi che, secondo l'A., si produrrebbero ai danni di diritti ulteriori a motivo delle modifiche ai rispettivi comportamenti adottati dai singoli individui per effetto del timore di essere soggetti a controllo ad opera di sistemi di riconoscimento facciale.

[13] Il testo può essere consultato al seguente link: https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf.

[14] Il riferimento è alle dichiarazioni rilasciate il 12 luglio 2023, il cui testo integrale può essere letto nella sua versione integrale al seguente link: https://www.ohchr.org/en/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner. In senso analogo, si vedano, anche, le dichiarazioni rilasciate nel 2020 nella dichiarazione intitolata *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, di cui al seguente link: https://www.ohchr.org/en/documents/thematic-reports/ahrc4424-impact-new-technologies-promotion-and-protection-human-rights. Si veda, anche, la dichiarazione resa il 3 agosto 2018, sui rischi connessi all'impiego dei sistemi di riconoscimento facciale, *The right to privacy in the digital age*, A/HRC/39/29, in cui l'*High Commissioner for Human Rights* osservava, che: «[e]nsure that data-intensive systems, including those involving the collection and retention of biometric data, are only deployed when States can demonstrate that they are necessary and proportionate to achieve a legitimate aim». La dichiarazione nella sua versione integrale è consultabile al seguente link: https://www.ohchr.org/en/documents/thematic-reports/ahrc3929-right-privacy-digital-age-report-united-nations-high. La posizione dello *UN High Commissioner for Human Rights* non è, peraltro, del tutto isolata. In prospettiva comparata e sul versante statunitense, si segnalano, ad esempio, alcune anche se scarne, iniziative promosse da alcuni Stati e città volte ad introdurre divieti all'impiego di sistemi di riconoscimento facciale. Un esempio, per tutti, è costituito dalla decisione adottata dallo Stato di New York di proibire il ricorso ai sistemi di riconoscimento facciale all'interno degli istituti scolastici pubblici. Ancora, la città di San Francisco, nel 2019, è stata la prima città statunitense a porre un divieto rispetto all'impiego di tali tecnologie da parte delle autorità di polizia tramite l'approvazione della «'Stop Secret Surveillance' ordinance», seguita, tra le altre, dalla città di Boston che ha introdotto analogo divieto nel giugno del 2020. Informazioni dettagliate sulle iniziative statali e locali adottate sino ad oggi, si consulti il seguente link: https://www.banfacialrecognition.com/map/. Recentissima è l'approvazione di una legge che limita l'impiego pubblico dei sistemi di riconoscimento facciale nello Stato della California. Il testo è consultabile al seguente link: https://a19.asmdc.org/press-releases/20240111-new-legislation-assemblymember-ting-targets-law-enforcement-use-facial. Gli Stati Uniti non sono gli unici a mettere in discussione l'impiego di tali sistemi a livello domestico e senza attendere decisioni adottate a livello sovranazionale. Il Canada, ad esempio, nel 2022, era stato presentato in Parlamento un report (Link: https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf), in cui la commissione parlamentare, lo *Standing Committee on Access to Information, Privacy and Ethics*, sottolineava l'urgenza di una limitazione dei sistemi di riconoscimento facciale nel settore privato.

In senso, invece, maggiormente conforme all'Unione Europea, si è mosso anche il Consiglio d'Europa, tramite i già citati Comitati istituiti *ad hoc*, il CAHAI, prima, il CAI, poi, e, in modo ancora più netto, tramite le linee guida pubblicate nel 2021 con le quali il Consiglio d'Europa sottolineava l'urgenza di un intervento normativo da parte degli Stati contraenti per i pregiudizi ai diritti umani connessi all'impiego di tali sistemi[15].

Nemmeno, la pronuncia della Corte europea dei diritti dell'uomo, resa sul caso *Glukhin c. Russia*[16] e a cui si dedicano le riflessioni che seguono, si discosta da simile orientamento. Una sentenza che si segnala, anzitutto, perché per la prima volta e a livello globale una Corte sovranazionale dei diritti si è pronunciata sulla conformità rispetto al diritto internazionale dei diritti umani dei sistemi di riconoscimento facciale, ma anche, e forse soprattutto, a motivo della ritenuta assenza di una incompatibilità *ipso iure* di tali tecnologie rispetto alla Convenzione europea dei diritti dell'uomo.

Si tratta di una pronuncia che si muove tra luci e ombre e che sollecita più di un interrogativo. Da un lato, una condanna, che potrebbe chiudere il dibattito sulla conformità dei sistemi di riconoscimento facciale almeno rispetto al sistema convenzionale, schiudendo le porte all'interrogativo relativo alle relazioni tra questa presa di posizione e l'opzione dell'Unione Europea nel testo finale dell'*AI Act*; dall'altro, una sentenza che, però, ritaglia la motivazione sulle specificità dello Stato contraente, con un andamento che si ritiene superi la natura eminentemente casistica della giurisprudenza della Corte di Strasburgo, investendo anche il merito. Ci si chiede, detto altrimenti, se, e se sì, fino a che punto, la condanna secca e unanime della Russia non poggi in modo forse preponderante sul carattere autoritario dello Stato contraente, peraltro, negli ultimi anni espulso dal Consiglio d'Europa.

In estrema sintesi, il tema e l'interrogativo che si pone sullo sfondo è quanto la sentenza in commento costituisca l'espressione di un orientamento giurisprudenziale destinato a consolidarsi negli anni a venire oppure la risposta in senso negativo all'utilizzo di sistemi di riconoscimento facciale nel contesto di ordinamenti giuridici autoritari.

[15] Il riferimento è alle *Guidelines on Facial Recognition*, pubblicate il 28 gennaio 2021 e redatte dal *Consultative Committee of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Il testo delle linee guida è consultabile al seguente link: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.

[16] Corte EDU, *Glukhin c. Russia*, [Terza Sezione], n. 11519/20, 4 luglio 2023. La sentenza è stata adottata all'unanimità ed è divenuta definitiva lo scorso 4 ottobre 2023. Una prima lettura, sintetica, della pronuncia è offerta da I. NERONI REZENDE, *Glukhin and the EU regulation of facial recognition: Lessons to be learned?*, in *European Law Blog*, consultabile al seguente link: https://europeanlawblog.eu/2023/09/19/glukhin-and-the-eu-regulation-of-facial-recognition-lessons-to-be-learned/. A commento della sentenza, si vedano, anche, F. PALMIOTTO, N. MENANDEZ GONDALEZ, *Facial recognition technology, democracy and human rights*, in *Computer Law & Security Review*, 2023, 1 ss.; C. COCITO, *Glukhin v. Russia: facial recognition considered highly intrusive but not inconsistent with fundamental rights*, in Strasbourgobserver.com, 2024; M. ZALNIERIUTE, *Glukhin v. Russia. App. No. 11519/20. Judgment*, in *American Journal of International Law*, 2023, 695 ss.

2. Una Corte sovranazionale censura, per la prima volta, un sistema di riconoscimento facciale: *Glukhin c. Russia*

Nel dibattito sintetizzato poco sopra, si inserisce la prima presa di posizione sulla conformità dei sistemi di riconoscimento facciale rispetto al diritto internazionale dei diritti umani e alla Convenzione europea dei diritti dell'uomo.

In una delle sue ultime pronunce contro la Russia, la Corte di Strasburgo ha, infatti, stabilito che l'arresto e la successiva sanzione amministrativa inflitta al ricorrente, *reo* di aver condotto una protesta individuale e pacifica e, in seguito, identificato dalle forze di pubblica sicurezza tramite sistemi biometrici di riconoscimento facciale[17], costituisce una violazione del diritto alla vita privata, *ex* art. 8 CEDU[18], nonché una illegittima compressione della libera manifestazione del pensiero protetta dall'art. 10 della Convenzione.

Ad avviso delle autorità russe e a fondamento delle misure intraprese dallo Stato, l'attivista avrebbe violato la disciplina relativa alle modalità di realizzazione di proteste o manifestazioni nello spazio pubblico, ancorché individuali, a nulla rilevandone la natura pacifica.

Viceversa, il ricorrente, dopo aver esaurito senza successo le vie di ricorso interne[19], ha portato la vicenda dinanzi alla Corte europea dei diritti dell'uomo lamentando, per prime, le violazioni degli artt. 10 e 11 CEDU.

A suo avviso, il denunciato difetto di previa notifica alle autorità nazionali sarebbe stato sprovvisto di base legale non essendo normativamente imposto, qualora la protesta non abbia carattere collettivo. La caratterizzazione pacifica della manifestazione avrebbe dovuto andare esente da previa notifica e, in ogni caso, la reazione dello Stato sarebbe stata espressione di un approccio a «tolleranza zero» e sproporzionata[20].

Riprendendo le argomentazioni di parte ricorrente, pure volendosi ammettere che anche una dimostrazione individuale e pacifica fosse soggetta all'obbligo di previa notifica, e la l'interferenza nei propri

[17] In letteratura, approfondisce le criticità che il ricorso a sistemi di identificazione biometrica riverbera sul piano dei diritti fondamentali, M. AKHTAR, *Police use of facial recognition technology and the right to privacy and data protection in Europe*, in *Nordic Journal of Law and Social Research*, 2019, 325 ss.

[18] In senso conforme, si vedano, quali precedenti, Corte EDU, *Gaughran c. Regno Unito*, [Prima Sezione], n. 45245/15, 13 febbraio 2020, in cui la Corte ha sancito la violazione dell'art. 8 CEDU a motivo della raccolta e della conservazione per un arco temporale indefinito dati biometrici – in questo caso, impronte digitali e il profilo DNA – e le fotografie di soggetti condannati per reati puniti con la pena della reclusione. Cfr., in particolare, § 70; Corte EDU, *Breyer c. Germania* [Quinta Sezione], n. 50001/12, 30 gennaio 2020, § 88; Corte EDU, *Szabó and Vissy c. Ungheria*, [Quarta Sezione], n. 37138/14, 12 gennaio 2016, in cui la Corte EDU ha accertato la violazione dell'art. 8 CEDU, a motivo della raccolta, da parte delle pubbliche autorità, di dati personali raccolti tramite sistemi di sorveglianza segreta, § 88; Corte EDU, *Roman Zakharov c. Russia*, [GC], n. 47143/06, 4 dicembre 2015, §§ 302 – 305, in cui la Grande Camera ha condannato la Russia per l'impiego da parte della pubblica autorità di un sistema di sorveglianza segreta di massa avente ad oggetto comunicazioni telefoniche realizzate via cellulare; Corte EDU, *S. e Marper c. Regno Unito*, [GC], nn. 30562/04, 30566/04, 4 dicembre 2008, §112, il caso è famoso per avere la Corte censurato le modalità con cui il *National DNA Database* disponeva la conservazione di campioni di DNA e dei relativi dati.

[19] Il riferimento è, in primo grado, alla decisione del *Meshchanskiy District Court* della città di Mosca e, in appello, dalla pronuncia di *Moscow City Court*.

[20] Cfr. § 49.

diritti si sarebbe comunque rivelata sproporzionata e non giustificata da alcuna prevalente esigenza di protezione sociale (c.d. *pressing social need*).

Ad avviso dello Stato, e viceversa, la norma di legge presenterebbe un tenore letterale chiarissimo, tale da non potersene escludere l'applicabilità nei confronti della condotta del ricorrente e a prescindere dalla sua natura pacifica.

Da parte sua ed in relazione agli artt. 10 e 11 CEDU, la Corte europea compie una prima scelta di campo, delimitando il *thema decidendum* al solo art. 10 CEDU, dichiarando assorbita la violazione dell'art. 11 CEDU[21].

Sul punto, come di consueto, la Corte è laconica, rimanendo, quindi, sullo sfondo il tema dell'applicabilità dell'art. 11 CEDU anche a proteste «individuali», non connotate, cioè, dalla dimensione collettiva che, di regola, caratterizza la nozione di riunione e il diritto, ad esercizio collettivo appunto, che vi accede; un profilo, che, forse, avrebbe portato alla inapplicabilità della norma e di inammissibilità del ricorso nella prospettiva dell'art. 11 CEDU[22].

In relazione all'art. 10 CEDU e con riferimento alla sussistenza della base legale a fondamento della interferenza lamentata dal ricorrente, la Corte concorda con lo Stato quanto alla piena operatività dell'obbligo di previa notifica, sposandone la tesi e ritenendo, pertanto, che il ricorrente ben avrebbe dovuto rendere edotte le autorità nazionali della propria intenzione di procedere alla manifestazione[23].

Non è, quindi, nella prospettiva del criterio della base legale che si fonda l'accertamento della violazione. Secondo la Corte, pure ammettendo la legittimità della finalità perseguita dalla norma, cioè, la salvaguardia di esigenze di pubblica sicurezza e la protezione dei diritti altrui, l'ingerenza nel diritto alla libera manifestazione del pensiero del ricorrente non può considerarsi «necessaria in una società democratica».

La Corte, quindi, seppure sinteticamente, considera tutti i requisiti di cui all'art. 10, § 2, giungendo ad escludere la convenzionalità del regime sanzionatorio applicato nei confronti del ricorrente poiché incompatibile con il criterio della «necessità in una società democratica»[24].

---

[21] Norma parametro evocata dal ricorrente, che rimane, quindi, scoperta, non pronunciandosi il Giudice di Strasburgo sulla conformità della condotta statale in relazione alla libertà di riunione. Cfr. § 47. La Corte, però, e questo è un aspetto interessante, non esclude del tutto la rilevanza del diritto di cui all'art. 11 CEDU, dichiarando di voler procedere ad un'analisi del caso che passi dall'art. 10 CEDU tenendo in considerazione i principi generali che ha enucleato nella propria giurisprudenza sull'art. 11 CEDU.

[22] Cfr. § 47. La Corte europea, tuttavia, non esclude del tutto il riferimento all'art. 11 CEDU almeno dal punto di vista argomentativo, dichiarando di ricomprendere nel sindacato sulla dedotta violazione dell'art. 10 CEDU anche i principi sanciti ai sensi dell'art. 11 CEDU secondo l'orientamento inaugurato in Corte EDU, *Novikova e altri c. Russia*, [Terza Sezione], nn. 25501/07 e altri 4, 26 aprile 2016, § 91, in cui la Corte si esprime nel senso di non dover procedere ad un esame della invocata lesione dell'art. 11 CEDU trattandosi di proteste individuali e non poste in essere insieme ad altri soggetti e, tuttavia, sottolinea al tempo stesso l'esigenza di non escludere una lettura estensiva dell'art. 10 CEDU che valorizzi, se rilevanti, anche i principi di cui all'art. 11 CEDU.

[23] Cfr., in particolare, § 120, ma, anche, §§ 112 ss.

[24] Cfr. § 49 ss. In letteratura viene sottolineata la difficoltà nel valutare il carattere non necessario dell'interferenza, considerata l'assenza di precedenti e, in aggiunta, quella di identificare i c.d. interessi contrapposti e bilanciabili con il ricorso da parte delle forze di polizia a una tecnologia così intrusiva come quella costituita dai sistemi di riconoscimento facciale. In questo senso, si rinvia a D. MURRAY, *Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework*, cit., 25.

A nulla rileverebbe la base legale e la legittimità delle finalità perseguite dalla norma poiché né la prima, né le seconde sarebbero sufficienti a giustificare la compressione del diritto del ricorrente.
Più interessante, perché direttamente incentrata sulla convenzionalità dei sistemi di riconoscimento facciale, è, invece, la parte della motivazione sulla invocata lesione del diritto alla vita privata del ricorrente.
Il tema diventa, qui, la legittimità, non previamente autorizzata da alcuna autorità giurisdizionale, né da autorità di pubblica sicurezza del ricorso a sistemi di identificazione biometrica accompagnato dall'assenza di qualsiasi regolamentazione circa la raccolta, la conservazione e l'utilizzo dei dati, da impiegare quale strumento di prova per fondare l'arresto, prima, e la condanna del ricorrente, poi.
La Corte europea si sofferma sulla sussumibilità della fattispecie entro l'ambito applicativo dell'art.8 CEDU. Pacifica è la riconducibilità della vicenda entro la nozione di vita privata, poiché, precisa la Corte, essa ben comprende le attività poste in essere dal singolo nella sfera pubblica.
Non è, però, sui profili di applicabilità e di ammissibilità che si sofferma la Corte di Strasburgo. Venendo al merito, la Corte preferisce piuttosto muovere dalla constatazione secondo cui la raccolta e la conservazione di dati personali costituisce sempre e di per sé stessa una ingerenza nel diritto alla vita privata. Il tema, allora, chiarisce la Corte, è se tale ingerenza possa ritenersi giustificata alla luce delle circostanze del caso concreto[25]. Esiste, infatti, una varietà di ipotesi in cui il singolo, volontariamente e consapevolmente, è coinvolto e realizza attività che possono essere registrate o riprese, sì da trasformare o, almeno, attenuare la portata e la "forza" della nozione di *privacy* e, quindi, le relative aspettative di rispetto della riservatezza[26]. Si tratta di ipotesi, che rendono opportuna una valutazione puntuale delle circostanze del caso di specie, al fine di verificare quale debba essere la gradazione dell'invocato diritto al rispetto per la vita privata dalla prospettiva della tutela del diritto alla *privacy*[27].
Venendo all'impiego delle tecniche di riconoscimento facciale a scopo di identificazione del singolo individuo, la Cote europea prende una posizione netta e precisa. Chiarisce, così, che l'impiego tali sistemi, a motivo della propria natura ontologica, non si traduce in una automatica violazione dei principi convenzionali. Il che equivale ad escludere, che i sistemi di identificazione debbano essere fatti oggetto

[25] La Corte precisa, infatti, che: «[t]he mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding. However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained», § 65.
[26] Sul punto, tuttavia, la Corte precisa che: «[p]rivate-life considerations may arise, however, once any systematic or permanent record of such personal data comes into existence, particularly pictures of an identified person. A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right of each person to the protection of his or her image is thus one of the essential components of personal development and presupposes the right to control the use of that image», Cfr. § 66.
[27] In proposito, merita di essere precisato che la Corte europea dei diritti dell'uomo ha già avuto occasione di precisare che il diritto alla riservatezza comprende anche il diritto ad essere informato circa la propria soggezione a sistemi di controllo e che tale ulteriore corollario del diritto alla *privacy* è coperto dalla nozione di vita privata di cui all'art. 8 della Convenzione. In questo senso, si vedano, Corte EDU, *Gaskin c. Regno Unito*, [Commissione], n. , 7 luglio 1989, § 49; *M.G. c. Regno Unito*, [Seconda Sezione], n. 39393/98, 24 settembre 2002, § 27; *Odièvre c. Francia*, [GC], n. 42326/98, §§ 41-47; *Guerra e altri c. Italia*, [GC], n. 14967/89, 19 febbraio 1998.

di un divieto assoluto e generalizzato quando utilizzati per "monitorare" i movimenti di una persona nello spazio pubblico.

Diverse dal monitoraggio e, quindi, potenzialmente oggetto di uno scrutinio più severo, sono, al contrario, per la Corte europea la raccolta e, soprattutto, la conservazione dei dati e delle immagini così ottenute.

Nella misura in cui tali tecnologie catturano e conservano immagini, esse incidono sull'elemento che più di ogni altro contraddistingue la personalità dell'individuo, poiché, precisa la Corte, «[t]he right of each person to the protection of his or her image is […] one of the essential components of personal development [it] presupposes the right to control the use of that image»[28].

Il contenuto di questa ulteriore declinazione del diritto alla vita privata – come pretesa, cioè, del singolo individuo al controllo della propria immagine – viene, poi, sviluppato dalla Corte nell'*iter* argomentativo. Si dice, così, che: «[w]hile in most cases the right to control such use involves the possibility for an individual to refuse publication of his or her image, it also covers the individual's right to object to the recording, conservation and reproduction of the image by another person»[29].

Questo passaggio della motivazione merita di essere sottolineato.

La Corte europea allarga il contenuto del diritto alla vita privata, specificandone i tratti quando associato all'impiego di tecnologie di intelligenza artificiale, come quelle di identificazione biometrica.

Nel riprendere la propria giurisprudenza sulla raccolta e conservazione di dati ed immagini individuali, la Corte di Strasburgo non incontra difficoltà nel riferire tali principi anche al caso in esame, concludendo per la illegittimità della ingerenza subita dal ricorrente. Sistemi di riconoscimento facciale sarebbero stati evidentemente utilizzati sia per la identificazione del ricorrente durante la protesta, sia, successivamente, per rintracciarlo al fine dell'arresto.

Come richiede l'articolo 8 CEDU, tuttavia, al fine di appurare il contrasto con la Convenzione occorre verificare che l'interferenza nell'esercizio del diritto non soddisfi alcuno dei criteri posti dal secondo paragrafo della norma convenzionale. Sotto questo profilo, è di sicura centralità l'insistenza con cui la Corte di Strasburgo si sofferma sulla opportunità o doverosità di sistemi normativi adeguati nel disciplinare l'impiego di tali tecnologie[30]. Una regolamentazione, quella invocata dalla Corte, che diviene tanto più urgente dinanzi al rapido e sempre più sofisticato sviluppo delle tecnologie di intelligenza artificiale. Una presa di posizione netta ed esplicita, che va inserita in un contesto globale e continentale (internazionale e domestico) che, faticosamente, sta raggiungendo quello standard minimo di garanzie per la tutela dei diritti individuali che la Corte considera imprescindibile[31].

[28] Cfr. § 66.

[29] *Ibidem*.

[30] Cfr. § 83. La Corte, in particolare, osserva che le norme vigenti entro l'ordinamento giuridico russo sono «widely formulated». Ancora, che «[t]he domestic law does not contain any limitations on the nature of situations which may give rise to the use of facial recognition technology, the intended purposes, the categories of people who may be targeted, or on processing of sensitive personal data. Furthermore, the Government did not refer to any procedural safeguards accompanying the use of facial recognition technology in Russia, such as the authorisation procedures, the procedures to be followed for examining, using and storing the data obtained, supervisory control mechanisms and available remedies».

[31] Cfr., § 77, «[i]n the context of the collection and processing of personal data, it is therefore essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concern-

La presenza di una disciplina dettagliata è per la Corte ancora più essenziale ed urgente quando ci si confronti con sistemi di identificazione facciale.

Le specificità della tecnologia in esame giustificano l'approccio della Corte al caso in esame in cui il sindacato sulla dedotta violazione dell'art. 8 CEDU non può procedere analizzando partitamente legittimità, ragionevolezza della finalità perseguita dalla norma e sua adeguatezza rispetto alla democraticità dell'ordinamento giuridico considerato.

E, invero, se è indubbio che lo scopo ultimo dell'impiego di tali sistemi da parte delle autorità di pubblica sicurezza sia la prevenzione del crimine, la questione che la Corte afferma di voler accertare è solo il carattere o meno eccessivamente intrusivo, ossia non convenzionale, dell'ingerenza sofferta e denunciata dal ricorrente.

In considerazione della fattispecie incriminatrice di particolare tenuità per la quale le autorità russe hanno fatto ricorso a sistemi di identificazione biometrica, la Corte ha gioco facile nel concludere per la sproporzione e per la incompatibilità di tali tecnologie rispetto all'art. 8 CEDU.

Una valutazione casistica, certo, ma non solo.

La Corte delinea, infatti, una serie di criteri da prendere in esame ogniqualvolta occorra e occorrerà appurare la conformità o meno dell'impiego di tali tecnologie rispetto all'art. 8 CEDU.

La Corte tenta, così, di introdurre elementi di astrattezza potenzialmente applicabili a casi futuri, affrancandosi dalla caratura eminentemente casistica della propria giurisprudenza. La Corte non si limita, cioè, a censurare il diritto alla vita privata, ma va oltre considerando quelli che in dottrina si definiscono i c.d. «chilling effects»[32], generati, appunto, dall'impiego su vasta scala di tali tecnologie e che, a cascata, potrebbero pregiudicare altri diritti fondamentali, come la libertà di espressione e la libertà di riunione, che, curiosamente, ritorna sebbene solo incidentalmente nel ragionamento della Corte. Si tratta, in altri termini, di effetti che conseguirebbero alla consapevolezza da parte dei singoli individui della soggezione a monitoraggio dei propri comportamenti tramite meccanismi di pubblica sorveglianza e che, quale conseguenza, sarebbero suscettibili di influenzare, modificandole, le abitudini e condotte dei consociati proprio per effetto di detto controllo esterno.

In definitiva, pure ridimensionando l'affermazione di apertura sulla convenzionalità *in astratto* dei sistemi di riconoscimento facciale, l'altro principio generale che si ricava dalla sentenza è la "messa in guardia", questa sì generalizzabile, del rischio che il ricorso a tali tecnologie sia suscettibile di produrre in relazione ad altri diritti, libertà di espressione e di riunione per primi[33].

---

ing, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness».

[32] In letteratura, si vedano, diffusamente, J.W. PENNEY, *Understanding Chilling Effects*, in *Minnesota Law Review*, 2022, 1451 ss.; D. MURRAY ET AL., *How Does a Surveillance-Related Chilling Effect Impact on Human Rights Law? Insights from Qualitative Research in Uganda and Zimbabwe*, in *Journal of Human Rights Practice*, 2023, consultabile al seguente link: *https://academic.oup.com/jhrp/advance-article/doi/*. Per uno studio, si rinvia al report *London Policing Ethics Panel, Final Report on Live Facial Recognition*, pubblicato nel Maggio 2019, link: *http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf*.

[33] La Corte afferma, infatti, così che: «the use of highly intrusive facial recognition technology to identify and arrest participants of peaceful protest actions could have a chilling effect in regard of the rights to freedom of

3. Interferenza illegittima nella vita privata, ma assenza di incompatibilità *ipso iure* con la Convenzione: dove si va?

Il primo aspetto da mettere in evidenza della pronuncia attiene, senza dubbio, all'approccio della Corte europea, che non condanna *in astratto* e, forse, nel merito (?), l'impiego delle tecnologie di riconoscimento facciale.

L'affermazione, a tutta prima di forte impatto nel contesto del dibattito sulla legittimità di simili strumenti, merita qualche precisazione.

Alla affermazione in cui dichiara testualmente che il monitoraggio delle azioni e dei movimenti di un individuo nello spazio pubblico non costituisce di per se stesso una interferenza nella vita privata, la Corte precisa che criticità, sul piano della loro convenzionalità, può profilarsi in costanza di registrazioni e raccolte sistematiche di dati personali[34]. Sarebbe, cioè, la conservazione e l'utilizzo successivo dei dati a fondare la a violazione potenziale della Convenzione e non il mero ricorso a sistemi di identificazione biometrica.

In apertura di motivazione, la Corte non esplicita quale sia oppure dovrebbe essere il rapporto tra il ricorso all'impiego di sistemi di riconoscimento facciale ed esigenze di sicurezza e sorveglianza pubblica, limitandosi ad una affermazione che appare a tutta prima teorica e potenzialmente slegata dalle ragioni per le quali comunemente si ricorre a tali sistemi da parte degli ordinamenti giuridici contemporanei.

E, tuttavia, se letta unitariamente allo sviluppo successivo dell'*iter* argomentativo, simile dichiarazione potrebbe anche essere interpretata in senso estensivo, sì da ritenere che, secondo la Corte, nel bilanciamento tra salvaguardia di esigenze collettive di pubblica sicurezza e tutela del diritto alla vita privata, occorra preferire una lettura temperata delle implicazioni di tali sistemi sul piano della loro compatibilità rispetto ai diritti convenzionali da subordinare ad un attento scrutinio delle circostanze del caso concreto.

Se inserita nel quadro del dibattito continentale e globale sull'ammissibilità dell'impiego di tali tecnologie, la valutazione della Corte europea non sorprende.

Nonostante non siano in tutto sopite le voci che vorrebbero vietare in modo assoluto l'utilizzo dei sistemi di riconoscimento facciale per ragioni di sorveglianza pubblica, specie quando prodromiche all'attuazione di misure limitative della libertà personale, l'orientamento prevalente sembra essersi spostato in favore di una ammissibilità condizionata. Né l'*Artificial Intelligence Act*, nel testo del gennaio 2024 poi condiviso dai 27 Stati membri lo scorso febbraio, né il *Consolidated Working Draft* della, probabilmente, prima Convenzione di diritto internazionale in tema di intelligenza artificiale del luglio

expression and assembly», Cfr. 88. Per un approfondimento delle relazioni e interazioni tra tecniche di intelligenza artificiale e libertà di manifestazione del pensiero, si vedano C.M. REALE, M. TOMASI, *Libertà d'espressione, nuovi media e intelligenza artificiale: la ricerca di un nuovo equilibrio nell'ecosistema costituzionale*, in *DPCEOnline*, 2022, 325 ss.

[34] Cfr. § 66.

dello stesso anno vietano in via assoluta i sistemi di identificazione biometrica[35]. Entrambi i testi preferiscono, così, un approccio che ne ammetta l'impiego in costanza di determinate garanzie di ordine anzitutto procedurale.

La Corte europea si dimostra, quindi, in sintonia rispetto ai contenuti discussi e probabilmente oggetto delle future e prime regolamentazioni europee. Non un divieto assoluto, ma un impiego soggetto a limitazioni e rispettoso dei diritti individuali grazie alla tipizzazione di specifici requisiti procedurali.

Non è, allora, un caso, che al primo punto fermo, di cui si è detto, – la non incompatibilità *in astratto* dei sistemi di riconoscimento facciale con la Convenzione europea dei diritti dell'uomo e con il diritto alla vita privata, in particolare –, il Giudice europeo ne accosti un secondo.

La Corte sottolinea, cioè, il carattere imprescindibile di una regolamentazione normativa che autorizzi l'impiego di tali tecnologie, prima, e che ne assicuri la supervisione da parte delle autorità giurisdizionali competenti, dopo, secondo una impostazione che preveda un controllo *ex ante*, in ossequio al principio di legalità, ed *ex post*, di supervisione rimesso all'autorità giurisdizionale. Anche qui, la conclusione della Corte non si discosta dalle scelte di Unione Europea e Consiglio d'Europa. Una legittimità che riposa ed è condizionata alla esistenza di una normativa in materia, che la Corte europea, precisa, non solo deve esistere, ma deve essere, come detto, «dettagliata»[36]: una sorta di riserva di legge rinforzata, però aspecifica, a voler utilizzare una terminologia propria del costituzionalismo.

Questi punti fermi sono sufficienti per spiegare l'esito dell'accertamento della violazione dei principi convenzionali. La non convenzionalità riposa sulla insussistenza entro l'ordinamento giuridico russo di una qualsiasi normativa che ne legittimi a monte l'impiego e che delinei *a priori* i criteri in base ai quali si può procedere *ex lege* alla raccolta ed alla successiva conservazione dei dati così ottenuti.

---

[35] Di avviso diverso era stato, inizialmente, il Parlamento europeo, sulla scia delle sollecitazioni di alcune Organizzazioni Non Governative, tra cui *Amnesty International* e *Article 19*. La dichiarazione con cui veniva rivolto alle istituzioni dell'Unione Europea l'invito a vietare il ricorso a sistemi di riconoscimento facciale può essere letta al seguente link: *https://www.amnesty.eu/wp-content/uploads/2023/09/Regulate-police-technology-EU-AI-Act-Statement-19-September.pdf*. In questo senso, si veda, anche, lo *Statement* intitolato *EU Trilogues: The AI Act must protect people's rights. A civil society statement on fundamental rights in the EU Artificial Intelligence Act*, pubblicato prima della pubblicazione della versione definitive dell'*AI Act* nel dicembre 2023. Il testo può essere consultato al seguente link: *https://edri.org/wp-content/uploads/2023/07/Civil-society-AI-Act-trilogues-statement.pdf*. In particolare, le *NGOs* firmatarie ponevano l'attenzione sui seguenti aspetti ed esigenze, all'epoca rivolte alle istituzioni dell'Unione Europea: «1. Empower affected people with a framework of accountability, transparency, accessibility and redress»; «2. Draw limits on harmful and discriminatory surveillance by national security, law enforcement and migration authorities»; «3. Push back on Big Tech lobbying: remove loopholes that undermine the regulation». Le *NGOs* firmatarie dell'appello sono 151.

[36] Cfr., § 77. La Corte precisa, così, che: «[i]n the context of the collection and processing of personal data, it is therefore essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness». La Corte ritorna sull'esigenza che l'impiego delle tecnologie di intelligenza artificiale sia soggetto ad una regolamentazione dettagliata al § 82 che più direttamente investe la posizione del ricorrente, laddove chiarisce che: «[i]n so far as the applicant alleged that the domestic law did not meet the 'quality of law' requirement, the Court considers that it is essential in the context of implementing facial recognition technology to have detailed rules governing the scope and application of measures as well as strong safeguards against the risk of abuse and arbitrariness. The need for safeguards will be all the greater where the use of live facial recognition technology is concerned».

Ciò che emerge in modo evidente è, in definitiva, l'enfasi posta dalla Corte sui rischi connessi al difetto di una regolamentazione nazionale che disciplini l'impiego delle tecnologie in esame secondo una impostazione che certa dottrina ha definito di «procedural fethishism»[37]. Detto altrimenti, in luogo di una pronuncia sul merito la Corte si sarebbe limitata a considerare sufficiente ai fini di eludere potenziali violazioni della Convenzione la positivizzazione di regole di procedura preposte al loro utilizzo.

Sulla portata delle richiamate affermazioni di principio possono darsi letture in parte divergenti.

Da un lato, si potrebbe sposare una interpretazione minimale della sentenza, che ne enfatizzi e contestualmente ne limiti la portata esterna alla dimensione c.d. "procedurale", secondo il già richiamato meccanismo del c.d. «feticismo procedurale»[38]. Similmente a quanto si verifica di fronte a violazioni degli artt. 2 e 3 CEDU, in cui la giurisprudenza convenzionale distingue tra violazioni procedurali e sostanziali[39], si potrebbe argomentare che, in senso analogo, si sarebbe mossa la Corte europea in *Glukhin*. Non una lesione del dettato convenzionale nel merito, non uno sfavore nei confronti del ricorso al riconoscimento facciale, bensì l'accertamento di una "mera" lacuna procedurale[40].

Nonostante la condanna, questa modalità di sindacato viene da parte della letteratura ancorata alla più estesa valorizzazione del margine di apprezzamento statale e della c.d. *deference* alle autorità nazionali[41]. A tale approccio potrebbero essere attribuire due conseguenze: la sufficienza di una regolamentazione, a cui subordinare l'impiego delle tecnologie di intelligenza artificiale, per scongiurare la violazione della Convenzione; il limitato impatto della sentenza in esame, il cui dato sostanziale sarebbe in verità assai circoscritto dal momento che la Corte si sarebbe limitata a richiedere la sussistenza di norme di procedura, senza esprimersi sul contenuto precettivo delle prime e, prima ancora, sulla *ratio* a cui dovrebbero sottostare le norme invocate.

---

[37] A proposito della sentenza in commento, utilizza questa espressione M. ZALNIERIUTE, *Glukhin v. Russia App. No. 11519/20 Judgment,* in *American Journal of International L*aw, 2023, 695 ss. Sulla nozione di *procedural fetishism*, che nasce nel contesto del diritto amministrativo, si veda più in generale N. BAGLEY, *The Procedure Fetish*, in *Michigan Law Review*, 2019, 345 ss. Utilizza diffusamente il concetto di feticismo procedurale riferito alla giurisprudenza più recente della Corte EDU in tema di *privacy* e di sorveglianza di massa, M. ZAINIERIUTE, *Procedural Fetishism and Mass Surveillance under the ECHR Big Brother Watch v. UK*, 2021, in https://verfassungsblog.de/big-b-v-uk/.

[38] Per un approfondimento in letteratura della tendenza della Corte europea dei diritti dell'uomo a privilegiare letture "procedurali" in luogo di scrutini sul merito delle violazioni invocate, si vedano, diffusamente, J. GERARDS, E. BREMS (a cura di), *Procedural Review in European Fundamental Rights Cases*, 2017; O.M. ARNARDÓTTIR, *The "procedural turn" under the European Convention on Human Rights and presumptions of Convention compliance*, in *International Journal of Constitutional Law*, 2017, 9 ss.

[39] In tema, si veda, diffusamente, E. BREMS, *Procedural Protection. An Examination of Procedural Safeguards Read into Substantive Convention Rights*, in E. BREMS, J. GERARDS (a cura di), *Shaping Rights in the EChR. The Role of the European Court of human Rights in determining the scope of human rights*, 2013, 161.

[40] Detto altrimenti, sarebbe la sola circostanza che le autorità russe non si sarebbero avvalse di una normativa che disciplinasse in modo adeguato l'*an* e il *quomodo* del ricorso alle tecnologie di riconoscimento facciale a fondare la condanna e la conseguente lesione dei diritti invocati dal ricorrente e non l'impiego di per sé delle prime.

[41] Sul collegamento tra scrutinio c.d. procedurale e ampliamento del margine di apprezzamento statale, si veda, diffusamente, ancora, O.M. ARNARDÓTTIR, *The "procedural turn" under the European Convention on Human Rights and presumptions of Convention compliance*, cit.

Dall'altro, e invece, si staglia una lettura, che vorrebbe irrobustire e riempire di contenuti la sentenza del Giudice europeo, così come la sua capacità di imporsi quale precedente e vincolo interpretativo per gli Stati contraenti e per la stessa Corte.

Secondo questa seconda opzione interpretativa, il difetto di norme preposte a disciplinare l'impiego dei sistemi di riconoscimento facciale nello spazio pubblico non costituirebbe soltanto una garanzia procedurale, espressiva della tendenza a privilegiare il dato procedurale su quello sostanziale, come appunto ritengono i sostenitori della oramai diffusa tendenza verso il c.d. «procedural fetishism». Piuttosto, l'impostazione sposata dalla Corte e l'insistenza sulla soggezione di tali tecniche a norme di legge rappresenterebbe la conseguenza diretta ed immediata della qualifica di tali sistemi come potenzialmente ed altamente lesivi dei diritti fondamentali, sì da renderne doverosa ed imprescindibile una regolamentazione. La dimensione procedurale sarebbe soltanto la manifestazione esterna della implicita e prioritaria risposta della Corte, questa sì sul piano sostanziale e di merito, ai rischi delle tecnologie in esame.

Quale delle due visioni della sentenza meglio risponda alle intenzioni dalla Corte non è dato saperlo. Certamente, la seconda rafforzerebbe la natura di precedente della pronuncia anche oltre il recinto del Consiglio d'Europa e ne assicurerebbe un più coerente coordinamento con l'attività delle istituzioni del Consiglio d'Europa così attente alle implicazioni maggiormente pericolose per i diritti umani dell'intelligenza artificiale[42].

E, peraltro, la distinzione tra dimensione procedurale e sostanziale della violazione della norma convenzionale si coglie nella giurisprudenza della Corte europea in relazione a principi che presentano una struttura eterogenea rispetto agli artt. da 8 a 11 CEDU, che non contemplano, cioè, in via espressa un riferimento a circostanze che potrebbero fare ritenere legittima una compressione del diritto in esame[43]. Ipotesi che, viceversa, non ricorre nelle ipotesi degli artt. da 8 a 11 CEDU, accomunati dalla previsione esplicita, al secondo paragrafo, di una serie di condizioni che possono rendere legittima e, dunque, sottratta alla censura della Corte, l'ingerenza nel diritto individuale.

In definitiva, voglia la sentenza non chiarisce fino in fondo l'orientamento della Corte europea. Se, cioè, ci si trovi di fronte ad una presa di pozione che vorrebbe ridurne al massimo l'utilizzo oppure se, viceversa, tali sistemi, se non in specifiche circostanze, potrebbero anche non presentare criticità così pesanti da doverne escludere l'impiego o, per lo meno, assoggettarlo a regole stringenti.

Se è vero che la pronuncia si apre con la inequivocabile affermazione dell'assenza di una preclusione assoluta nei confronti del loro impiego, la motivazione che segue tempera l'assolutezza della dichiarazione che finisce, forse, addirittura per perdere reale pregnanza di significato.

[42] Il riferimento è al ruolo del CAHAI, prima, e del CAI, dopo, in entrambi i casi attenti alle implicazioni più pericolose per i diritti umani dell'intelligenza artificiale. Qui il riferimento è, ancora una volta, alla bozza di trattato attualmente in discussione in seno al Consiglio d'Europa su cui si veda, *supra*, nota n. 2 e par. n. 1.

[43] Si pensi alla giurisprudenza della Corte europea dei diritti dell'uomo sugli artt. 2 e 3 CEDU e, in particolare, alla casistica in tema di violenza razziale perpetrata nei confronti della popolazione di etnia rom nell'Est Europa. Tra tutti, può richiamarsi, in questa sede, Corte EDU, *Nachova e altri c. Bulgaria*, [GC], nn. 43577/98, 43579/98, 26 febbraio 2004, che appare particolarmente illustrativa della modalità di scrutinio di cui si discute e della differenza tra accertamento di una violazione procedurale oppure sostanziale del diritto convenzionale invocato. Più di recente, in una vicenda che riguardava invece abusi perpetrati nei confronti di minori, si veda Corte EDU, *X e altri c. Bulgaria*, [GC], n. 22457/16, 2 febbraio 2021.

Si potrebbe, cioè, sostenere che non vi sia differenza tra: considerare in astratto lecito l'impiego di tali tecnologie e, subito dopo, subordinarne, però, in concreto la legittimità alla previa definizione di norme di legge che ne assicurino la conformità ai diritti fondamentali, da un lato; e sancire, sin dall'inizio, che l'utilizzo dei sistemi di riconoscimento facciale può ammettersi solo previa definizione di una regolamentazione puntuale e dettagliata che ne legittimi l'utilizzo. Detto altrimenti, l'accento posto sulla dimensione procedurale e, quindi, sulla necessità che vi siano regole che disciplinino l'impiego dei sistemi di riconoscimento facciale, non equivarrebbe ad una omessa presa di posizione nel merito della Corte sui rischi connessi alle tecnologie in esame. Non ci troveremmo, cioè, dinanzi ad un «procedural turn»[44] della Corte che minimizzerebbe il "peso" della sentenza.

Al contrario, la Corte ci dice che una regolamentazione è necessaria proprio perché i sistemi in esame rischiano di violare i diritti fondamentali specie quando impiegati nello spazio pubblico e da parte della pubblica autorità.

Da altra angolazione, vi è, invece, chi ritiene deludente la pronuncia proprio perché affetta da quel feticismo procedurale di cui si è detto in precedenza, che consentirebbe alla Corte di bypassare "la domanda" del ricorrente, non soffermandosi, cioè, la Corte sulla legittimità sostanziale dei sistemi in esame, e radicando la sentenza sul solo dato procedurale.

La laconicità di alcuni passaggi della sentenza non rende agevole l'avallo dell'una oppure dell'altra interpretazione. La verità, forse, come spesso accade, sta nel mezzo.

In ragione del legame inscindibile tra innovazione tecnologica, che di frequente presenta ricadute potenzialmente lesive di diritti fondamentali, e diritto, l'accento posto sulla doverosità di disporre di un quadro normativo solido potrebbe non leggersi a senso unico ed espressiva di un, sicuramente riduttivo, feticismo procedurale.

Allo stato dei fatti, forse, e in un contesto sprovvisto di normative puntuali, potrebbe "prendersi" dalla sentenza in commento quello che vi è di certo e di dichiarato in modo esplicito: l'invito, che sa di monito, a che i legislatori, nazionali e sovranazionali, si attivino a normare un fenomeno, che non può più permettersi di essere lasciato nella disponibilità né di coloro che costruiscono tali sistemi, né di coloro che li immettono nel mercato, né, tanto meno, di chi ne fan uso, siano essi enti privati o pubblici.

3.1. Una sentenza "*Country-Specific*"? Quanto "conta" il carattere autoritario dello Stato

Vi è, poi, secondo aspetto da non sottovalutare e che potrebbe ridimensionare il contenuto della pronuncia in esame e, con esso, la sua capacità di imporsi quale precedente nella giurisprudenza della Corte europea dei diritti dell'uomo. Ci si riferisce alle specificità del contesto ordinamentale dello Stato rispondente, che, in ragione dei tratti autoritari che lo contraddistinguono e che lo distanziano dalla

[44] Così si esprime, ancora, O.M. ARNARDÓTTIR, *The "procedural turn" under the European Convention on Human Rights and presumptions of Convention compliance*, cit. Per un ulteriore approfondimento di questa evoluzione potenziale delle modalità di scrutinio della Corte europea dei diritti dell'uomo, si vedano, anche, J. ERDMAN, *The Procedural Turn: Abortion and the European Court of Human Rights*, in R.J. COOK, J.N. ERDMAN, B.M. DICKENS (a cura di), *Abortion law in Transnational Perspective*, 2014; J. PETTER RUI, *The Interlaken, Izmir and Brighton Declarations: Towards a Paradigm Shift in the Strasbourg Court's Interpretation of the European Convention on Human Rights*, in *Nordic Journal of Human Rights*, 2013, 54 ss.

maggioranza degli Stati contraenti del Consiglio d'Europa, potrebbero avere favorito l'esito della pronuncia rendendo più stringente lo scrutinio della Corte di Strasburgo[45].

Nel censurare l'impiego dei sistemi di riconoscimento facciale nel caso di specie, la Corte europea prende, come detto, le mosse dalla loro non necessità (e adeguatezza) in una società democratica alla luce della natura pacifica della protesta messa in atto dal ricorrente.

Se queste sono le premesse – il carattere autoritario dello Stato, da un lato, e la natura pacifica della protesta, dall'altro – l'interrogativo, che si pone è duplice.

In primo luogo, viene da domandarsi se, all'opposto, la Corte sarebbe incline a qualificare, invece, convenzionalmente conforme il ricorso a tali tecnologie in costanza di proteste, viceversa, non pacifiche. Se, cioè, la Corte europea sarebbe giunta a conclusioni diverse, ammettendo quindi l'utilizzo dei sistemi di riconoscimento facciale per ragioni di sicurezza, qualora *Glukhin* si fosse reso protagonista di una protesta violenta.

In secondo luogo, se e quanto la condanna così piana del ricorso a tali sistemi di intelligenza artificiale sia stata in qualche misura agevolata dalla qualità autoritaria dell'ordinamento giuridico russo e se, di conseguenza, un simile standard di scrutinio, qui più severo, sarebbe stato applicato anche nei confronti di ordinamenti giuridici reputati al contrario democratici, dove minore sarebbe il rischio di una volontà dello Stato di sopprimere il dissenso, servendosi dei sistemi di intelligenza artificiale.

Sebbene non difettino altri casi paragonabili a quello in esame, almeno sul piano del ricorso a meccanismi di intelligenza artificiale, qualche spunto è, però, offerto dalla giurisprudenza convenzionale recente in materia di intercettazioni di massa per ragioni di sorveglianza pubblica. Ci si riferisce, cioè, alle c.d. *bulk interceptions* protagoniste di alcune recenti pronunce del Giudice di Strasburgo[46].

[45] Come noto, la Russia è stata espulsa dal Consiglio d'Europa quale conseguenza dell'invasione dell'Ucraina in forza dell'art. 8 dello Statuto del Consiglio d'Europa. La cessazione della qualità di parte contraente dello Stato russo ha iniziato a decorrere dal 15 marzo 2022. La decisione adottata dall'Assemblea Parlamentare può essere consultata al seguente link: https://pace.coe.int/en/files/29885/html. Per un commento all'approccio della Corte europea dei diritti dell'uomo e della sua giurisprudenza nei confronti di regimi autoritari, tra i molti, si rinvia di recente a B. ÇALI, *Autocratic Strategies and the European Court of Human Rights*, in *European Convention on Human Rights Law Review*, 2021, 11 ss. Sulle relazioni tra la Corte europea dei diritti dell'uomo e la Russia prima e a seguito della sua recente espulsione dal Consiglio d'Europa, si vedano A. MÜLLER, *The European Court of Human Rights and the Rise of Authoritarianism in Russia*, in J. VIDMAR (a cura di), *European Populism and Human Rights*, BRILL, 2020, 215 ss.; D. KURNOSOV, *No easy way out: the Strasbourg Court and the legacy of Russian cases*, in *Strasbourg Observer*, 2023, link: https://strasbourgobservers.com/2023/03/24/no-easy-way-out-the-strasbourg-court-and-legacy-russian-cases/; sulle conseguenze derivanti dall'espulsione della Russia, si rinvia a K. DZEHTSIAROU, L. HELFER, *Russia and the European human rights system: Doing the right thing… but for the right legal reason?*, in *EJIL Talk*, 2022, link: https://www.ejiltalk.org/russia-and-the-european-human-rights-system-doing-the-right-thing-but-for-the-right-legal-reason/.

[46] La Corte europea dei diritti dell'uomo anche in passato aveva avuto occasione di esprimersi in relazione ad alcuni casi, che riguardavano le interferenze nel diritto alla riservatezza scaturenti dal ricorso allo strumento delle intercettazioni, appuntando l'attenzione sull'esigenza che tali meccanismi di ingerenza nel diritto alla vita privata siano sorretti da una base legale solida ed affiancati da altrettanto puntuali garanzie procedurali. Si richiamano, in questa sede, a titolo esemplificativo, Corte EDU, *Z c. Finlandia*, [Camera], n. 22009/93, 25 febbraio 1997, § 95; Corte EDU, *M.S. c. Svezia*, [Camera], n. 20837/92, 27 agosto 1997, § 41.

In questo senso, un posto di primo piano va riservato alla recente pronuncia della Grande Camera in *Big Brother Watch c. Regno Unito*[47]. In quell'occasione, la Corte europea si è espressa sul merito del ricorso a sistemi di intercettazioni di massa, accettandone l'impiego, ritenuto convenzionalmente conforme, laddove motivato da ragioni di contrasto di atti di terrorismo oppure di crimini aventi carattere transnazionale, cioè di conversazioni intrattenute tra soggetti che risiedano in Stati diversi.

Pure accertando la violazione del diritto alla vita privata, la Grande Camera ha, tuttavia, sottolineato due aspetti centrali a sostegno del legittimo impiego delle intercettazioni di massa per ragioni di sicurezza nazionale.

In primo luogo, la Corte ha riaffermato che rientra nel margine di apprezzamento dello Stato la decisione se adottare o meno tali sistemi in costanza di minacce alla pubblica sicurezza. In secondo, più fondamentalmente, che è di tutta evidenza che le intercettazioni di massa costituiscono uno strumento assai utile per raggiungere lo scopo perseguito, cioè la salvaguardia della pubblica sicurezza, alla luce del tasso crescente di rischi di attentati terroristici[48]. Una violazione dell'articolo 8 CEDU potrebbe scorgersi, allora, solo in relazione alle modalità con cui lo Stato utilizza tali sistemi, cioè laddove difettino alcune precise garanzie di procedura che la Corte ha avuto occasione di dettagliare.

Big Brother Watch palesa, quindi, un approccio diverso rispetto a *Glukhin*[49].

In *Glukhin*, la Corte non condona l'utilizzo dei sistemi di riconoscimento facciale. Non ricorre, così, alcun riferimento alla potenziale legittimità di un simile utilizzo quando accompagnato da esigenze di salvaguardia della sicurezza come in *Big Brother Watch*.

Più sfumato, se non assente in *Glukhin*, è poi quel "feticismo procedurale", viceversa evidente e altrettanto criticabile in *Big Brother Watch*.

In definitiva, il raffronto tra i due casi sembra corroborare quella tesi che vorrebbe spiegare la disinvoltura della Corte europea nel condannare la Russia con la coloritura autoritaria delle sue istituzioni[50]. Se in *Big Brother Watch*, la condanna del Regno Unito è circoscritta alle modalità di impiego delle intercettazioni di massa (peraltro solo quelle transnazionali), in *Glukhin*, la censura non si riassume nel solo difetto di salvaguardie procedurali, lasciando piuttosto spazio, come detto, ad un – seppure implicito e laconico – avallo della pericolosità dei sistemi di riconoscimento facciale.

---

[47] Corte EDU, *Big Brother Watch e altri c. Regno Unito*, [GC], nn. 58170/13, 62322/14 and 24969/15, 25 maggio 2021. In tema, si segnala anche Corte EDU, *Wieder and Guarnieri c. Regno Unito*, [Quarta Sezione], nn. 64371/16 64407/16, 12 settembre 2023; nonché due casi che attualmente pendono contro la Polonia, entrambi relativi alla convenzionalità di sistemi di sorveglianza tramite intercettazioni telefoniche di massa. Si tratta di *Pietrzak c. Polonia* e *Bychawska-Siniarska e altri c. Polonia*. A commento di *Big Brother Watch*, si veda, tra gli altri, F. ZORZI GIUSTINIANI, *La normalizzazione della sorveglianza di massa nel contesto della CEDU e il Quarto Oxford Statement sulle tutele offerte dal diritto internazionale nel cyberspazio*, in *Nomos*, 2021, 1 ss.

[48] Cfr., § 386, laddove la Corte così afferma: «it is clear that bulk interception is a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime».

[49] Altri casi paragonabili a *Big Brother Watch* sono offerti da Corte EDU, *Catt c. Regno Unito*, [Prima Sezione], n. 43514/15, 24 gennaio 2019; Corte EDU, *Ben Faiza c. Francia*, [Quinta Sezione], n. 31446/12, 8 febbraio 2018.

[50] In questo senso, si veda, M. ZALNIERIUTE, *Glukhin v. Russia. App. No. 11519/20. Judgment*, cit., che osserva come «the ECtHR's findings that Russia had violated Articles 8 and 10 of the Convention may be more reflective of the Court's increased austerity toward authoritarian regimes regarding government surveillance, rather than symbolic of any increased recognition of the dangers FRT poses».

Potrebbe anche sostenersi privo di pregio il parallelismo proposto per la eterogeneità delle tecnologie considerate. Tuttavia, si ritiene che, almeno, la caratterizzazione "*Country-Specific*" o, perlomeno, politica del caso in commento non sia da sottovalutare anche in considerazione della espulsione della Russia dal Consiglio d'Europa e della diffidenza che certamente influenza, anche sul piano politico e pubblico, le sentenze della Corte europea dei diritti dell'uomo.

4. Oltre la giurisprudenza convenzionale: altre risposte e altre condanne in prospettiva comparata

Se la sentenza della Corte europea dei diritti dell'uomo lascia irrisolti alcuni interrogativi, primo tra tutti quello della reale compatibilità con la Convenzione dei sistemi di riconoscimento facciale quando impiegati per ragioni di pubblica sorveglianza e di sicurezza, spunti interessanti sono offerti dalle sinora poche, ma interessanti, decisioni adottate da alcuni Corti e tribunali nazionali con riferimento all'utilizzo di tecnologie di riconoscimento facciale nello spazio pubblico[51].

Pochi casi giudiziari che, tuttavia, si collocano in un quadro globale che vede tutta una serie di iniziative talvolta adottate da singoli Stati di ordinamenti federali, talaltra da autorità indipendenti od istituzioni pubbliche, che si sono espressi in senso sfavorevole alla diffusione di tali sistemi quali meccanismi di pacifico impiego, tra le altre, per la identificazione di sospettati per la commissione di crimini o di atti di terrorismo, cioè, in termini più ampi, per ragioni di politica criminale e di salvaguardia della pubblica sicurezza.

Non si procederà, in questa sede, ad un'analisi esaustiva delle specificità di ogni singola pronuncia.

Piuttosto, si intende mettere in evidenza quale sia, se ve ne uno, l'orientamento che si sta consolidando a livello domestico e, ancora prima: quali sono le circostanze in cui i sistemi in esame sono stati impiegati e poi censurati, come i giudici comuni hanno risolto le criticità in punto di accertamento della responsabilità individuale soprattutto quanto alla definizione dei criteri a cui fare ricorso ai fini della identificazione del soggetto "*liable*"; infine, come questi casi pilota sono stati, con successo, portati davanti alle autorità giurisprudenziali.

[51] La disamina che qui si offre è limitata alle più significative pronunce di organismi giurisdizionali, mentre non si occupa delle decisioni adottate da autorità indipendenti, per tutte, dal Garante per la protezione dei dati. Sul versante dell'ordinamento giuridico nazionale, possono, ciò nonostante, ricordarsi, sebbene non direttamente aventi ad oggetto sistemi di identificazione biometrica, ma interessanti per le ricadute sul piano dei principi di eguaglianza e non discriminazione, le ordinanze di ingiunzione, del 10 giugno 2021 e 22 luglio 2021, con cui il Garante ha censurato la violazione di alcune disposizioni del Regolamento generale sulla protezione dei dati (Regolamento (UE) 2016/679, c.d. GDPR, nel primo caso, da parte della società spagnola di consegna di beni alimentari e di altri servizi, Foodinho s.r.l., in relazione al trattamento dei dati degli individui impiegati come *riders* dalla società Glovo App23 sul territorio italiano, nella seconda, di Deliveroo s.r.l. Per un commento, si consenta il rinvio a C. NARDOCCI, *Quando "manca" il giudice… il Garante della Privacy, l'algoritmo e la profilazione*, in *Forum di Quaderni Costituzionali*, 2021, 1 ss. Più interessante, nella prosopettiva che qui interessa perché direttamente afferente al sistema di identificazione biometrica *Clearview AI*, su cui si tornerà poi nel testo, è la decisione sempre del Garante con cui il 10 febbraio 2022 è stata disposta una sanzione di 20 milioni di euro nei confronti della società statunitense per aver monitorato il movimento di soggetti che si trovavano sul territorio italiano. Il testo del provvedimento può essere consultato al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751362.

Tra questi, il più famoso risale al 2020, deciso dalla Corte d'Appello del Regno Unito, che ha condannato l'impiego, da parte delle forze di polizia del sud del Galles, del software di riconoscimento facciale *AFR Locate*[52]. *AFR Locate* consentiva alle forze di polizia del sud del Galles, sin dal 2017, di collocare sistemi di riconoscimento facciale in luoghi pubblici discrezionalmente selezionati allo scopo di verificare se i volti selezionati dal *software* coincidessero o meno con quelli di soggetti ricercati oppure presenti all'interno di liste di soggetti considerati pericolosi. Finalità ultima di tale sistema voleva essere quella di allertare la pubblica autorità per procedere all'arresto del soggetto identificato quale sospettato.
In questa occasione, superando la pronuncia di primo grado che aveva viceversa escluso il carattere intrusivo del software risolvendo il bilanciamento in favore delle garanzie di pubblica sicurezza, la Corte d'Appello ha ritenuto che *AFR Locate* violasse l'art. 8 della Convenzione europea dei diritti dell'uomo. In difetto di una regolamentazione puntuale tesa a legittimarne il ricorso, le forze di pubblica sicurezza si sarebbero avvalse del *software* con eccessiva discrezionalità[53]. Ad avviso della Corte d'Appello, quindi, l'impiego di AFR Locate sarebbe stato sprovvisto di qualsiasi base legale e, ancora, che le forze di polizia non avrebbero condotto alcuna verifica per appurare l'assenza di *bias* o di malfunzionamento del sistema prima di disporne l'uso su vasta scala.
L'aspetto su cui forse vale la pena di insistere, soprattutto perché la Corte europea non ne fa cenno in *Glukhin,* è dato dall'enfasi con cui la Corte d'Appello censura la negligenza delle forze di polizia che ignoravano all'epoca dell'utilizzo del *software* in esame tanto il contenuto, i dati inclusi nel *dataset*, quanto le modalità di *tranining* e, in definitiva, di funzionamento del *software*. In estrema sintesi, la responsabilità o *liability* dell'utilizzatore finale, cioè delle forze di polizia, viene fatto poggiare dal giudice sulla lesione del c.d. *right to know*[54], corollario dei requisiti di *explainability* e *transparency* che

[52] Corte d'Appello del Regno Unito, *R (on the application of Bridges) v. Constable of South Wales Police*, 11 agosto 2020, consultabile al seguente link: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf. A commento della pronuncia, tra gli altri, si vedano B. KEENAN, *Automatic Facial Recognition and the Intensification of Police Surveillance*, in *Modern Law Review*, 2021, 886 ss.; nell'ambito della letteratura nazionale, commentano la decisione in esame J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Diritto Penale Contemporaneo*, 2020, 231 ss., e A. PIN, *Non esiste la "pallottola d'argento": l'"*artificial face recognition*" al vaglio giudiziario per la prima volta*, in *DPCE online*, 2019, 3175 ss. Più in generale, approfondiscono il tema dell'impiego dei sistemi di identificazione biometrica da parte delle forze di polizia, Z. GUO, L. KENNEDY, *Policing based on automatic facial recognition*, in *Artificial Intelligence and Law*, 2023, 397 ss. In tema, si segnala che, nonostante la decisione in commento che ha fatto in qualche modo da apripista illuminando sulle criticità connesse ai sistemi di sorveglianza di massa ancorché impiegati per esigenze di. Pubblica sicurezza, il Regno Unito sta discutendo l'approvazione di una nuova disciplina che consente, entro certi limiti, l'impiego dei sistemi identificazione biometrica da parte delle forse di polizia quali strumenti ausiliari nel settore della giustizia penale. Il testo della proposta può essere letto al seguente link: https://publications.parliament.uk/pa/bills/cbill/58-04/0010/230010.pdf.

[53] La Corte d'Appello così si è espressa in proposito nel passaggio della propria decisione: «[t]he fundamental deficiencies, as we see it, in the legal framework currently in place relate to two areas of concern. The first is what we called the 'who question' at the hearing before us. The second is the 'where question'. In relation to both of those questions too much discretion is currently left to individual police officers. It is not clear who can be placed on the watchlist nor is it clear that there are any criteria for determining where AFR can be deployed», § 91.

[54] Il tema, cioè, è quello del consenso che dovrebbe prestare il singolo individuo alla propria soggezione ad un sistema di intelligenza artificiale. Peraltro, su questo profilo collegato al diritto alla *privacy* e al diritto alla vita privata, si era a suo tempo espresso lo *UN Human Rights Committee* nel suo Commento Generale n. 16, dell'8 aprile 1988, dedicato all'art. 17 del Patto sui diritti civili e politici, che può essere consultato al seguente link:

devono presiedere all'uso di sistemi di IA secondo l'orientamento che si sta affermando entro il continente europeo[55].

Sarebbe, cioè, la non conoscenza delle modalità di funzionamento del sistema a fondare la responsabilità, dissociando la posizione del programmatore da quella dell'utilizzatore, unico soggetto responsabile, appunto, di eventuali lesioni derivanti dall'impiego della tecnologia di intelligenza artificiale. Il criterio suggerito in *AFR Locate* è da sottolineare in quanto, per la prima volta, un giudice ha introdotto per via pretoria una regola volta a fondare la responsabilità individuale derivante da violazioni di diritti fondamentali legate al ricorso alle tecnologie di IA.

Il caso di *AFR Locate* non è rimasto isolato.

Altri esempi utili per vagliare le modalità con cui i giudici e le Corti nazionali hanno nel corso degli anni più recenti scrutinato l'utilizzo dei sistemi di riconoscimento facciale proviene dalla Francia.

Nel 2020, il Tribunale amministrativo di Marsiglia ha censurato l'impiego di tali sistemi quali strumenti di controllo in due scuole superiori. Accanto alla illegittimità dell'impiego di tali sistemi, rispetto ai quali difettava all'epoca una normativa a cui subordinarne il ricorso, il Tribunale ha posto l'accento sul difetto di una valutazione preliminare di impatto al fine di verificarne i potenziali effetti, anche e soprattutto lesivi di diritti fondamentali[56].

Sempre la Francia, sulla scia di altri ordinamenti UE[57] ed *extra* EU[58] ha vietato l'impiego del *software Clearview AI* a seguito di una decisione del Garante della *Privacy* francese. Più di recente e, viceversa, il *Conseil d'Etat* ha escluso la illegittimità del ricorso ai sistemi di riconoscimento facciale per valutare i rischi di recidiva, c.d. TAJ (*traitement des antécédents judiciaires*)[59].

Questo orientamento del *Conseil d'Etat* ha segnato uno spostamento di approccio piuttosto significativo da parte dell'ordinamento francese che, nel 2023, si è dimostrato maggiormente permissivo

---

https://www.refworld.org/pdfid/453883f922.pdf. In particolare, si veda quanto si affermava al § 10, dove si legge quanto segue: «[i]n order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination».

[55] Pure decisiva, gli effetti della decisione sono stati di recente ridimensionati dalla re-introduzione del medesimo software da parte delle forze di polizia del Galles del Sud che hanno deciso di riprenderne l'impiego. Sarà, quindi, opportuno tenere monitorata la vicenda e, soprattutto, occuparsi di appurare quali sono state, se ve ne sono, le modifiche apportate al sistema di IA e se la nuova introduzione ha seguito l'adozione di linee guida tese a circoscrivere la sanzionata discrezionalità delle autorità.

[56] Tra le violazioni, il Tribunale rilevava anche il contrasto con l'articolo 8 della Convenzione europea dei diritti dell'uomo.

[57] Si pensi, anche, all'Italia, dove il Garante per la protezione dei dati personali ha emesso nel 2022 una multa pari a 20 milioni di euro nei confronti dell'azienda. Interessa, a questo proposito, richiamare anche il parere del Garante pubblicato in data 25 marzo 2021, con il quale il Garante si esprimeva in senso negativo rispetto all'utilizzo del sistema di identificazione biometrica SARI Real Time. Cfr., il testo al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575877.

[58] Tra questi: Canada, Australia, Regno Unito.

[59] *Conseil d'Etat*, pronuncia n. 442364, 26 Aprile 2022, consultabile al seguente link: https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-04-26/442364.

quanto al ricorso a sistemi biometrici di identificazione. Basti, qui, richiamare il decreto[60] e il disegno di legge[61], adottati rispettivamente nell'aprile e nel dicembre 2023, con cui la Francia ha deciso di consentire l'impiego di droni dotati di sistemi di video sorveglianza da parte delle forze di polizia in occasione della celebrazione dei prossimi giochi olimpici previsti per il 2024.

Volgendo lo sguardo oltre i confini europei, altre vicende aventi ad oggetto l'impiego e gli effetti distorsivi dei sistemi di riconoscimento facciale sono state portate davanti alle Corti.

Negli Stati Uniti, in *New Jersey c. Arteaga*[62], la Corte d'Appello dello Stato del New Jersey ha, così, condannato l'impiego di un sistema di riconoscimento facciale utilizzato dalla polizia della città di New York (NYPD) per l'identificazione di un sospettato, di colore, accusato di aver compiuto una rapina in un esercizio commerciale. A fronte del diniego opposto dallo Stato di fornirgli informazioni circa il funzionamento del *software*, il ricorrente ha richiesto alla Corte del New Jersey la *full disclosure* degli elementi probatori a proprio carico, lamentando l'omessa trasparenza della procedura e l'impossibilità di avere accesso al codice sorgente.

New Jersey c. Arteaga ha confermato l'orientamento già accolto dallo Stato dell'Illinois, nel caso *ACLU c. Clearview AI*[63], deciso dalla Circuit Court di Cook County che ha avuto protagonista il già citato *software Clearview AI*. La vicenda si è conclusa nel 2022 con un accordo transattivo tra le parti[64], con cui è stato fatto divieto all'azienda di rendere disponibile il proprio *database*, ritenendo le modalità di raccolta dei dati personali lesive del diritto alla *privacy* dei cittadini dello Stato dell'Illinois.

Accanto a questi, l'impiego dei sistemi di riconoscimento facciale da parte delle forze di polizia statunitensi continua ad attirare intorno a sé un acceso dibattito a motivo delle loro ricadute discriminatorie, soprattutto, ai danni della popolazione afro-americana[65], tanto da aver indotto diversi dipartimenti di alcune città ad introdurre *policies ad hoc* per regolamentarne l'impiego e scongiurarne gli effetti pregiudizievoli e distorsivi[66].

---

[60] Il riferimento è al *Décret* n. 2023-283 del 19 aprile 2023, su cui si veda il commento di S. BONOMI, *L'utilizzo di tecnologie di riconoscimento facciale da parte delle forze dell'ordine: la normativa europea e il caso francese*, consultabile al seguente link: https://www.cyberlaws.it/2023/utilizzo-tecnologie-riconoscimento-facciale/.

[61] Il testo integrale può essere consultato al seguente link: https://www.senat.fr/leg/pjl22-220.html.

[62] La pronuncia del 7 giugno 2023 può essere letta al seguente link: https://law.justia.com/cases/new-jersey/appellate-division-published/2023/a-3078-21.html.

[63] Circuit Court of Cook County, Illinois, County Department, Chancery Division, *ACLU c. Clearview AI*. Il ricorso è stato depositato in data 28 maggio 2020 e il primo *hearing* si è svolto in data 25 settembre 2020. Per un commento alla vicenda, si rinvia a I. AHMED, *ACLU v. Clearview Ai, Inc*., 33 *DePaul J. Art, Technology & Intellectual Property Law*, 2023, 66 ss.

[64] Il testo dell'accordo può essere consultato al seguente link: https://www.courthousenews.com/wp-content/uploads/2022/05/aclu-v-clearview-settlement.pdf.

[65] In questo senso, possono richiamarsi in questa sede i dati pubblicati nel 2019 dal *Report* del *Georgetown Center*, consultabile al seguente link: https://www.flawedfacedata.com/. In senso analogo, si veda, anche, il *Report* redatto dallo *United States Government Accountability Office* del giugno 2021, dal titolo *Facial recognition technology. Federal Law enforcement agencies should better assess privacy and other risks*, consultabile al seguente link: https://www.gao.gov/assets/gao-21-518.pdf.

[66] In tema, occorre sottolineare che non vi è alcun obbligo per le autorità di pubblica sicurezza di rendere edotta la popolazione in merito all'impiego o meno di sistemi di riconoscimento facciale quali strumenti di indagine, fatte salve, appunto, le iniziative di segno opposto adottate, a titolo di esempio, dalla città di New York nel 2020, e dagli Stati del Vermont e della Virginia nel 2021.

Degna di nota è, infine, anche la recente pronuncia della Corte d'Appello della città di Buenos Aires, Argentina, che si è espressa per la incostituzionalità del sistema di identificazione biometrica *Fugitive facial recognition system* (Srfp)[67], a motivo del difetto di una regolamentazione per legge del suo utilizzo dimostratosi lesivo dei diritti fondamentali dei cittadini argentini. In particolare, la Corte ha stabilito che la città di Buenos Aires potrà reintrodurre Srfp solo: previa istituzione di appositi meccanismi di *human oversight* e di controllo sul funzionamento del sistema; verifica delle sue potenzialità discriminatorie; pubblicità e *report* delle operazioni condotte.

La pronuncia presenta innumerevoli profili di interesse, che qui possono essere solo accennati. Tra tutti, la Corte si è soffermata sulla legittimità dell'interesse ad agire dei ricorrenti in relazione all'invocata violazione del diritto alla riservatezza, la cui violazione veniva denunciata con riferimento alla generalità dei cittadini. Su questo punto, la Corte ha occasione di precisare che il diritto alla *privacy* presenta una dimensione collettiva, in quanto diritto di titolarità collettiva avente ad oggetto un bene collettivo. Una simile e innovativa lettura del diritto alla riservatezza potrebbe supportare il deposito di ricorsi ulteriori, soprattutto da parte di chi non sia la vittima diretta dell'*agere* concreto dei sistemi di IA in discorso – si pensi al ruolo suppletivo delle ONG –, favorendo l'ampliamento dell'accesso alla giustizia e la soggezione dei *software* di identificazione biometrica, ma non solo, a controllo "umano", ancorché effettuabile *ex post*.

Nonostante la eterogeneità dei contesti ordinamentali e con la sola eccezione del caso francese, sembra rintracciabile una tendenza a guardare con sempre maggiore diffidenza ai sistemi di riconoscimento facciale. Tuttavia, l'aspetto più interessante dell'*excursus* qui proposto è costituito dal dato fattuale che ne emerge: la diffusione massiccia e quasi capillare delle tecnologie in esame a cui si accompagna l'altrettanto frequente assenza di consapevolezza da parte dei singoli di essere soggetti a controllo, con tutte le conseguenze che ne derivano sul piano del diritto al giudice, in termini cioè di accesso alla giustizia, e di tutela dei diritti[68].

5. Conclusioni: tempo di convergenze "continentali"?

Se posta a raffronto con le decisioni delle Corti nazionali e con le soluzioni normative che si stanno consolidando entro il contesto europeo, *Glukhin c. Russia* può apparire una pronuncia, forse, in parte deludente.

Condivisibili l'esito – la condanna –, e le argomentazioni della Corte – la sproporzione dello strumento di controllo e la sua inadeguatezza rispetto alle caratteristiche di uno Stato democratico –, restano invece sullo sfondo alcune questioni su cui il Giudice europeo avrebbe potuto soffermarsi maggior-

[67] Il testo della decisione in lingua spagnola è consultabile al seguente link: https://www.cels.org.ar/web/wp-content/uploads/2022/09/reconocimientofacialsentencia070922.pdf. Per una prima lettura della sentenza, si veda M. BADILLO, *Judge declares buenos aires' fugitive facial recognition system unconstitutional*, link: https://fpf.org/blog/judge-declares-buenos-aires-fugitive-facial-recognition-system-unconstitutional/.

[68] In proposito, valga richiamare, in questa sede, la presa di posizione del Parlamento europeo, *Use of artificial intelligence by the police: MEPs oppose mass surveillance*, 6 ottobre 2021, consultabile al seguente link: https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance.

mente per chiarire il proprio *iter* motivazionale, sì da rendere *Glukhin c. Russia* un precedente "pesante" per la propria giurisprudenza e per casi futuri da portare dinanzi a Corti nazionali e ad altri *Treaty Bodies* sovranazionali.

La pronuncia si raccorda poco con i principi "nuovi", che si stanno affermando sulla scena europea, tanto di diritto EU che a livello di Consiglio d'Europa, e che si accingono a tracciare i contorni della legittimità del ricorso anche a sistemi di identificazione biometrica[69], specie quando utilizzati per ragioni di pubblica sorveglianza e di sicurezza.

Non vi è, così, traccia nella sentenza della Corte europea dei principi di trasparenza e di conoscibilità, sui quali pure insiste il Consiglio d'Europa nel suo *Consolidated Working Draft*[70] e rispetto al quale ci si sarebbe potuti forse attendere una maggiore consonanza.

Analogamente, non si scorge alcun riferimento ad obblighi positivi da porre in capo allo Stato contraente, secondo una interpretazione del secondo paragrafo dell'articolo 8 CEDU, che voglia subordinato, anche entro il sistema convenzionale, l'impiego delle tecnologie di intelligenza artificiale in esame al rispetto dei c.d. *right to know*, per coloro che vi siano soggetti, e di *human oversight*, su cui fanno perno, ancora una volta, l'*Artificial Intelligence Act* così come la bozza di trattato il cui negoziato è ancora in corso in seno al Consiglio d'Europa.

È pure vero che la pronuncia potrebbe essere interpretata come implicitamente adesiva a tali principi. La sproporzione e la non "necessità in una società democratica" potrebbero, cioè, essere interpretate quali corollari o declinazioni ulteriori dei "nuovi" diritti alla trasparenza e alla spiegabilità dei sistemi di intelligenza artificiale; lo stesso per il diritto individuale alla consapevolezza della propria soggezione a sistemi di intelligenza artificiale, come nel caso del già citato *right to know*.

Ciò che si potrebbe rimproverare, o almeno, potuto attendere dalla Corte europea nella sua prima sentenza in materia di intelligenza artificiale è, l'eccessiva laconicità di alcuni passaggi della motivazione. La Corte non chiarisce come i criteri di cui si è avvalsa per accertare la violazione degli artt. 10 e 8 CEDU – quelli elencati al secondo paragrafo delle due norme – potrebbero essere interpretati sì da includere entro il rispettivo ambito applicativo anche i criteri o principi che il diritto "continentale europeo" sta facendo emergere quali criteri a cui assoggettare la legittimità dei sistemi di intelligenza artificiale.

In altre parole, la Corte aveva l'occasione di fare uso o di testare in concreto quei principi adattandoli al sistema della Convenzione, anche verificandone la conformità e l'adeguatezza, ma ha preferito un approccio minimale o, comunque, chiuso entro il recinto dei principi convenzionali. Ha lasciato, cioè, "fuori dalla porta" le novità che il fenomeno dell'intelligenza artificiale sta portando con sé sul versante

[69] In tema, valga ricordare che la versione dell'*AI Act* approvata il 9 dicembre 2023 escludeva il ricorso ai sistemi di identificazione biometrica in alcuni casi tipizzati, tra cui: il c.d. *social scoring*, il *predictive policing*, il *behavioural manipulation* cognitivo. Viceversa, il ricorso a sistemi di identificazione biometrica come tecniche "high risk" veniva consentito, subordinandolo al rispetto di specifiche garanzie, quale strumento di sorveglianza pubblica motivata da ragioni legate, ad esempio, alla prevenzione e al contrasto di attacchi terroristici oppure la ricerca di sospettati della commissione di crimini particolarmente gravi. Il c.d. "Pre-final text" del gennaio – febbraio 2024 parimenti vieta alcuni sistemi di riconoscimento facciale, come previsto a norma dell'art. 5 (1ba) e assoggetta a rigide limitazioni i sistemi di identificazione biometrica impiegati nello spazio pubblico secondo quanto dispone l'art. 5(1d).

[70] Si vedano, in particolare, gli artt. 7 e ss. del *Chapter* III.

della enucleazione di "nuovi" diritti o corollari nuovi di diritti fondamentali classici, tra tutti, il diritto alla vita privata e all'autodeterminazione.

Così facendo, e in conclusione, la Corte non svela il proprio orientamento nei confronti delle opzioni avallate dall'Unione Europea e, soprattutto, dal Consiglio d'Europa e lascia irrisolto l'interrogativo sul se e come deciderà di conciliare la propria giurisprudenza con i diritti di quella che è stata, efficacemente, definita la nuova frontiera dei diritti civili[71]. Una frontiera a cui nessuna Corte, nessun legislatore, nazionale o sovranazionale, può e potrà più sottrarsi nel prossimo futuro.

[71] Così C.A. BURROWS, *Chiar* della *Equal Employment Opportunity Commission* degli Stati Uniti d'America, che ha parificato il rapido sviluppo delle tecnologie di *AI* ad una «new civil rights frontier». La dichiarazione è stata rilasciata nell'aprile 2023. La notizia è stata resa nota dal Washington Post e può essere letta al seguente link: *https://www.washingtonpost.com/technology/2023/04/25/artificial-intelligence-bias-eeoc/*.