Freedom, Security & Justice: European Legal Studies

Rivista giuridica di classe A

2023, n. 1

EDITORIALE SCIENTIFICA
ES

Rivista quadrimestrale on line "Freedom, Security & Justice: European Legal Studies"
www.fsjeurostudies.eu
Editoriale Scientifica, Via San Biagio dei Librai, 39 - Napoli
CODICE ISSN 2532-2079 - Registrazione presso il Tribunale di Nocera Inferiore n° 3 del 3 marzo 2017

Indice-Sommario
2023, n. 1

Editoriale

Saggi e Articoli

Commenti e Note

LA RISERVATEZZA DEI DATI BIOMETRICI NELLO SPAZIO EUROPEO DEI DIRITTI FONDAMENTALI: SUI LIMITI ALL'UTILIZZO DELLE TECNOLOGIE DI RICONOSCIMENTO FACCIALE

Francesca Di Matteo*

SOMMARIO: 1. Introduzione: l'imporsi della tecnologia a base biometrica del riconoscimento facciale nel mercato globale e le ricadute nelle vite degli individui. − 2. La normativa regionale adottata nel quadro del Consiglio d'Europa. – 3. Il quadro normativo di riferimento a livello di diritto dell'Unione europea: il diritto vigente. − 4. La proposta di regolamento sull'intelligenza artificiale. – 5. Sulla dubbia legittimità dell'utilizzo della *facial recognition technology* in base ai contenuti degli articoli 7 e 8 della Carta dei diritti fondamentali. – 6. (segue)… e a quelli dell'articolo 8 della Convenzione europea dei diritti dell'uomo, quale diritto "corrispondente". – 7. Conclusioni.

1. Introduzione: l'imporsi della tecnologia a base biometrica del riconoscimento facciale nel mercato globale e le ricadute nelle vite degli individui

Dall'etimo greco «βίος» (vita) e «μέτρον» (misura), la biometria è quella disciplina che, per l'appunto, 'misura' grandezze biofisiche, a vari scopi. Ai fini del presente scritto sembra sufficiente evidenziare come i dati biometrici consentano di identificare gli individui attraverso le proprie caratteristiche: quelle fisiche, come le impronte digitali, la retina o il *pattern* venoso; quelle comportamentali, come la voce, il modo di camminare o di gesticolare[1]. Essi, pertanto, costituiscono una categoria particolare di dati personali,

Articolo sottoposto a doppio referaggio anonimo.
* Ricercatore t.d. di Diritto dell'Unione europea, Università LUMSA. Indirizzo e-mail: f.dimatteo3@lumsa.it.
[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*, in GUUE L 119 del 4 maggio 2016, pp. 1-88. Per la definizione di dati biometrici, v. in particolare l'art. 4, n. 14: "«dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici".

rientranti peraltro nel novero dei cd. dati sensibili di cui al primo paragrafo dell'art. 9 del Regolamento generale sulla protezione dei dati personali[2].

In virtù della loro potenzialità di identificare univocamente gli individui, i dati biometrici hanno attratto una particolare *species* dell'ampio *genus* costituito dalle tecnologie a base biometrica: le tecnologie di riconoscimento facciale (di seguito, anche, *facial recognition technology* o *FRT*), che allo stato ricoprono un ruolo di non scarso rilievo nel panorama della cd. *artificial intelligence*, vale a dire quella famiglia di tecnologie in rapida evoluzione dirette a realizzare sistemi informatici in grado di simulare la capacità del pensiero ed il comportamento umani, da cui ci si aspettano enormi benefici in termini economici e sociali[3]. Attraverso la *facial recognition technology* è possibile rilevare il volto di un determinato individuo all'interno di un'immagine, comparare quel volto con altre immagini presenti in un *database* di riferimento allo scopo di verificarne l'identità, ed infine 'categorizzare' quel viso, in base all'età, all'etnia, o persino in base alle espressioni facciali che denotano lo stato emotivo di una persona[4], operazioni che fino ad oggi richiedevano il diretto intervento umano e che, pertanto, mal si prestavano ad essere replicate sistematicamente e su vasta scala.

Non sfuggono le utilità che tale tecnologia può offrire. Dai benefici per il consumatore medio − la *FRT* può essere utilizzata come metodo di accesso ai dispositivi elettronici in luogo delle consuete *password*, come autorizzazione all'invio di bonifici bancari tramite *smartphone*, per aprire la portiera di una macchina o per rilevare i segnali di un guidatore in procinto di addormentarsi alla guida – ai vantaggi per il cittadino in

[2] Regolamento (UE) 2016/679, cit., art. 9: "È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

[3] Proposta di regolamento del Parlamento europeo e del Consiglio *che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, del 21 aprile 2021, COM (2021) 206 def.; Libro bianco *sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, del 19 febbraio 2020, COM (2020) 65 def.

[4] "Facial recognition refers to a multitude of technologies that can perform different tasks for different purposes. In this regard, a key distinction is whether facial recognition is used for verification, identification or categorisation. Verification and identification deal with matching unique characteristics of individuals to determine their individual identity. Categorisation deals with deducing whether an individual belongs to a specific group based on his or her biometric characteristics – for example, sex, age, or race", Agenzia dell'Unione europea per i diritti fondamentali (FRA), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, del 27 novembre 2019, p. 7, disponibile su www.fra.europa.eu.

ambito sanitario[5], lavorativo[6], nel campo della sicurezza e dell'ordine pubblico: così, ad esempio, nel caso dell'utilizzo della *FRT* ai fini del controllo delle frontiere o della repressione del crimine[7]. In quest'ultima ipotesi, peraltro, la presenza sul territorio nazionale di telecamere, asservite a *software* in grado di effettuare un riconoscimento facciale (anche in tempo reale), potrebbe risultare decisiva al fine di reprimere determinate tipologie di reati, si pensi, uno per tutti, al problema delle persone scomparse e, *in primis*, ai minori rapiti.

Non a caso l'uso della *facial recognition technology* ha avuto una diffusione esponenziale nell'ultimo decennio, nei settori più vari, sia da parte di attori pubblici che privati. Basti pensare che in Cina le tecnologie di riconoscimento facciale sono state impiegate nel controllo dei prestiti bibliotecari all'interno delle scuole o per compilare il piano nutrizionale annuo degli alunni[8], ma anche, all'occorrenza, per limitare i movimenti e le attività della minoranza Uyghur[9]. Parimenti è stato osservato come di recente, in

[5] "*FRT* is attractive for a variety of health care applications, such as diagnosing genetic disorders, monitoring patients, and providing health indicator information (related to behavior, aging, longevity, or pain experience, for example)", N. MARTINEZ-MARTIN, *What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?*, in *AMA journal of ethics*, 2019, n. 2, p. 180-187, p. 1, disponibile su https://journalofethics.ama-assn.org. Sull'uso della *FRT* in tempo di pandemia, M. VAN NATTA, P. CHEN, S. HERBEK, R. JAIN, N. KASTELIC, E. KATZ, M. STRUBLE, V. VANAM, N. VATTIKONDA, *The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic*, in *Journal of Law and the Biosciences*, 2020, n. 1, pp. 1-17, disponibile su https://doi.org/10.1093/jlb/lsaa038; D. PERPETUINI; C. FILIPPINI; D. CARDONE; A. MERLA, *An Overview of Thermal Infrared Imaging-Based Screenings during Pandemic Emergencies*, in *International Journal of Environmental Research and Public Health*, 2021, n. 6, pp. 1-12, disponibile su https://doi.org/10.3390/ijerph18063286.

[6] "Employers can use face identification to limit access of work spaces to employees. Others are using facial analysis on videos of job candidates to inform hiring decisions", J. BUOLAMWINI, V. ORDÓÑEZ, J. MORGENSTERN, E. LEARNED-MILLER, *Facial Recognition Technologies: a Primer*, 29 maggio 2020, p. 8, disponibile su https://www.ajl.org/federal-office-call.

[7] T. MADIEGA, H. MILDEBRATH, European Parliamentary Research Service (EPRS), *Regulating facial recognition in the EU*, 15 settembre 2021, p. 4, disponibile su https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2021)698021.

[8] "A central tension that schools will continue to face concerns whether emotion recognition will be used to measure academic performance, student behaviour, or both […]. For example, in acknowledging that Hangzhou No. 11's Smart Classroom Behaviour Management System may label students who rest their heads on their desks due to illness as 'inattentive', Vice Principal Zhang suggested the school nurse's office could establish 'white lists' of ill students to prevent them from being unfairly marked as unfocused in class. Similarly, Hangzhou No. 11 implemented facial recognition as a form of mobile payment authentication in its cafeteria in 2017. Not long after, the school used face recognition to monitor library loans and compile annual nutrition reports for each student, which shared information about students' cafeteria food consumption with their parents", Art. 19, *Emotional Entanglement: China's emotion recognition market and its implications for human rights*, 2021, A19/DIG/2021/001, p. 33, disponibile su https://www.article19.org/emotion-recognition-technology-report.

[9] "China has been the leader in the application of biometric surveillance, which is particularly ubiquitous in northwest China's Xinjiang Uyghur Autonomous Region. Chinese authorities use biometric identification to track and restrict the movements and activities of the Uyghur through the use of facial recognition technology and mandatory collection of sensitive data, such as DNA samples and iris scans. It has also been established that this surveillance technology is used to arbitrarily place large numbers of Uyghurs and members of other ethnic groups in so-called 're-education camps' under the pretext of countering religious extremism, without detainees being charged or tried", D. GŁOWACKA, R. YOUNGS, A. PINTEA, E. WOŁOSIK, Directorate General for External Policies of the Union − Policy Department, *Digital technologies as a means of repression and social control*, 18 maggio 2021, p. 15, disponibile su https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653636.

Russia, siano state installate più di centomila telecamere dotate di tecnologie di riconoscimento facciale al fine, si sostiene, di controllare il rispetto dell'obbligo di quarantena in tempo di pandemia[10]. Per non parlare di quando le tecnologie di riconoscimento facciale vengono dichiaratamente utilizzate a fini repressivi, come fatto dall'esercito israeliano nelle attività di sorveglianza del territorio palestinese occupato[11], nel cui ambito la *FRT* ha avuto un ruolo centrale, soprattutto con riferimento all'applicazione per *smartphone* nota come "Blue Wolf"[12]. Anche negli Stati membri dell'Unione europea si è fatto ampio ricorso all'uso delle tecnologie di riconoscimento facciale. A mero titolo esemplificativo: in Spagna, una catena di supermercati utilizzava telecamere dotate di meccanismi di riconoscimento facciale raccogliendo i dati biometrici di migliaia di clienti, minori compresi, nonché quelli degli stessi dipendenti, con lo scopo di impedire l'accesso a chi tra gli avventori fosse stato raggiunto da determinate tipologie di provvedimenti restrittivi da parte dell'autorità giudiziaria (ciò, prima di ricevere un'importante sanzione da parte della nazionale autorità garante della *privacy*); in Germania, la questura di Colonia ha installato ventisei telecamere (in grado di effettuare il riconoscimento facciale dei soggetti ripresi in tempo reale) intorno alla stazione e alla cattedrale principale della città, andando così a 'sorvegliare' centinaia di migliaia di metri

[10] Ivi, p.16: "The rise of biometric surveillance, in particular facial recognition technology, can be observed in different parts of the globe, despite evidence that it may exhibit bias and lead to or reinforce discrimination, alongside being intrusive in nature, lacking regard for privacy. The countries that have recently been expanding facial recognition cameras in public spaces, for example, include Kyrgyzstan, India, a number of Latin American countries, as well as some 'Global North countries' such as Israel (which has implemented the system on the West Bank), the United States, and Australia. The most prominent example of AI-assisted surveillance is Russia, where the pandemic has accelerated a process of installing a network of 100,000 facial recognition cameras to keep track of quarantined individuals. The expansion of this technology has contributed to the regime's already pervasive surveillance mechanisms".

[11] ROHAN TALBOT, *Automating occupation: International humanitarian and human rights law implications of the deployment of facial recognition technologies in the occupied Palestinian territory*, in *International Review of the Red Cross*, 2020, n. 914, pp. 823-849.

[12] "The Israeli military has been conducting a broad surveillance effort in the occupied West Bank to monitor Palestinians by integrating facial recognition with a growing network of cameras and smartphones [..] a smartphone technology called Blue Wolf that captures photos of Palestinians' faces and matches them to a database of images so extensive that one former soldier described it as the army's secret 'Facebook for Palestinians'. The phone app flashes in different colors to alert soldiers if a person is to be detained, arrested or left alone. To build the database used by Blue Wolf, soldiers competed last year in photographing Palestinians, including children and the elderly, with prizes for the most pictures collected by each unit. The total number of people photographed is unclear but, at a minimum, ran well into the thousands", The Washintgon Post, E. DWOSKIN, *Israel escalates surveillance of Palestinians with facial recognition program in West Bank*, 8 novembre 2021.

quadrati di territorio locale[13]; in Olanda, telecamere dotate di riconoscimento facciale sono state utilizzate durante i festeggiamenti del Carnevale ed altri eventi pubblici[14].

Senonché, oltre alle utilità ed ai benefici, a non sfuggire sono anche i rischi connessi all'utilizzo delle tecnologie di riconoscimento facciale: non solo in termini di sicurezza dei dati (intrusioni abusive nei *database* ed usi illeciti delle immagini ivi presenti), ma soprattutto con riferimento ai possibili errori che derivano dai processi di identificazione o di comparazione dei volti umani e alla potenziale lesione dei diritti fondamentali degli individui i cui volti sono sottoposti, spesso inconsapevolmente, a riconoscimento.

In punto di identificazione, la prassi ha dato ampia prova di cosiddetti falsi positivi (il sistema individua come 'faccia' qualcosa che faccia non è) e falsi negativi (al sistema sfugge la rilevazione di un volto all'interno di un'immagine)[15]. Peraltro, l'esito di una fase di comparazione tra 'facce' non si riassume sempre e comunque nell'alternativa *zero matches* o *true match*: oltre alla possibilità che si verifichino combinazioni di volti che in verità appartengono a persone diverse (cd. *false matches*), per i motivi più vari, come ad esempio la minore nitidezza di una delle due immagini, vi è anche la concreta possibilità che il sistema non riconosca la stessa persona (cd. *false mismatch*), magari per via della distanza di tempo intercorrente tra la rispettiva acquisizione delle immagini messe a confronto[16].

Quanto invece alla potenziale lesione dei diritti fondamentali, è noto come le tecnologie di riconoscimento facciale abbiano un più basso margine di accuratezza nel riconoscere i volti di persone di colore (soprattutto quelli delle donne) e il rischio di discriminazione può concretizzarsi già in fase di creazione degli algoritmi usati per il riconoscimento facciale, ovvero in un momento successivo, a seconda di come i risultati vengono gestiti da chi dirige il procedimento[17]: per bene intendere gli effetti deleteri che da siffatta tecnologia potrebbero derivare, si pensi al caso in cui la *FRT* venga utilizzata

[13] "This area, together with the Breslauer Platz behind the main station, presents itself as a high level surveillance network covering an area of approx. 300,000 to 360,000 square meters. Prior to the installation of the biometric ready video cameras, available statistical data evidenced that crime was declining in the area. However, notwithstanding the downward trend of crime, the use of video surveillance is increasing […]. For example, in addition to pedestrians, cyclists, cars (including license plates, which are not pixelated), GP practices, pharmacies, law firms, and places of worship are all in view of this surveillance. These areas include Rudolf Platz,14 which hosts a number of LGBT+ venues, and other areas, including Breslauer Platz, which host places of worship", L. MONTAG, R. MCLEOD, L. DE METS, M. GAULD, F. RODGER, M. PEŁKA, *The Rise and rise of biometrics mass surveillance in the EU, A legal analysis of biometrics mass surveillance practices in Germany, the Netherlands, and Poland*, EDRi – European Digital Rights, 7 luglio 2021, p. 20, disponibile su https://edri.org/our-work/new-edri-report-reveals-depths-of-biometric-mass-surveillance-in-germany-the-netherlands-and-poland.

[14] Ivi, pp. 37-38. Anche in Irlanda la FRT è stata utilizzata per prevenire frodi nel campo dei benefici previdenziali ed assistenziali; invece, in Francia, a Marsilia e a Nizza, alcune telecamere munite di *FRT* sono state utilizzate all'esterno di scuole secondarie di secondo grado, allo scopo di prevenire furti ed accessi abusivi, e ciò in virtù di provvedimenti municipali poi annullati dal giudice amministrativo francese.

[15] T. MADIEGA, H. MILDEBRATH, *Regulating facial recognition in the EU*, cit., p. 3.

[16] Ivi, pp. 13-14.

[17] Ivi, p. 7.

allo scopo di regolare l'accesso ad un *gate* aeroportuale[18]o con la finalità di identificare un criminale sulla base di milioni di foto segnaletiche[19].

Nondimeno l'uso esteso della *FRT* nei luoghi pubblici può produrre l'effetto di limitare il libero esercizio del diritto ad associarsi e riunirsi pacificamente da parte delle persone 'comuni', i cui comportamenti non potrebbero non risentire della consapevolezza di essere automaticamente identificati e tracciati dalle autorità statali. In altre parole, può contribuire ad alimentare un denegato stato di sorveglianza elettronica globale. Del resto, le informazioni fornite dall'ex analista della CIA, Edward Snowden, sul contenuto e l'estensione delle attività d'*intelligence* dei cosiddetti 'five eyes'[20], hanno ormai da anni rivelato all'opinione pubblica come sia oggi possibile, grazie all'evoluzione tecnologica, che taluni Stati attuino una vera e propria sorveglianza elettronica domestica (ed

[18] "Researchers have documented the racialized origins of biometric technologies, as well as their contemporary discriminatory operation on the basis of race, ethnicity and gender. A recent report on facial recognition technology deployed in border crossing contexts, such as airports, notes that despite the fact that even the best algorithms misrecognize black women twenty times more often than white men, the use of these technologies is increasing globally. As that report notes, 'where facial recognition is applied as a gate-keeping technology, travellers are excluded from border control mechanisms on the basis of race, gender and other demographic characteristics (e.g. country of origin)'. The frequent results of this differential treatment include perpetuation of negative stereotypes, and even prohibited discrimination which for asylum seekers might lead to refoulement", E. TENDAYI ACHIUME, *Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, 10 novembre 2020, A/75/590, p. 6. Nella stessa ottica anche, A. VALDIVIA, J. C. SERRAJÒRDIA, A. SWIANIEWICZ, *There is an elephant in the room: towards a critique on the use of fairness in biometrics*, in *AI Ethics*, 2022, disponibile su https://doi.org/10.1007/s43681-022-00249-2; M. S. CATALETA, *Humane Artificial Intelligence: The Fragility of Human Rights Facing AI*, East-West Center, 2020, p. 4.

[19] "Discriminatory law enforcement practices were highlighted following the murder of George Floyd by the Minneapolis PD. Black Americans are more likely to be arrested and incarcerated for minor crimes than White Americans. Consequently, Black people are overrepresented in mugshot data, which face recognition uses to make predictions. The Black presence in such systems creates a feed-forward loop whereby racist policing strategies lead to disproportionate arrests of Black people, who are then subject to future surveillance", A. NAJIBI, *Racial Discrimination in Face Recognition Technology*, 24 ottobre 2020, disponibile su https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/; "recent reports about the facial recognition start-up Clearview AI have exposed that the company has sold its capacity to rapidly identify individuals by sifting through a proprietary database of three billion face images—many of which it has unlawfully scraped from social media websites and applications—to hundreds of police forces […] with no transparency, no regulatory oversight […]. Examples like this seem to be multiplying, at present, as blinkered and reckless innovation practices like those of Clearview AI couple with the corresponding embrace by equally feckless government agencies and corporations of ethically and legally suspect facial analysis products and services", D. LESLIE, *Understanding bias in facial recognition technologies: an explainer*, 2020, disponibile su https://www.turing.ac.uk/research/publications/understanding-bias-facial-recognition-technologies, p. 22.

[20] Ci si riferisce alla serie di inchieste giornalistiche rese pubbliche a partire dal mese di giugno del 2013 e volte a rivelare dettagli sulle operazioni di sorveglianza di massa organizzate dall'Agenzia per la Sicurezza Nazionale statunitense (NSA) in complicità con servizi di *intelligence* di altri Paesi, sia nei confronti di cittadini e istituzioni statunitensi che di cittadini e istituzioni stranieri. È oggi noto che le prime attività di sorveglianza di massa negli Stati Uniti risalgano al tempo della seconda guerra mondiale, per poi essersi notevolmente estese nel corso degli anni '70, assumendo portata globale grazie al programma "Echelon". Nel 2013, le divulgazioni dell'ex analista della CIA, Edward Snowden, hanno svelato l'esistenza di nuovi programmi di sorveglianza di massa, quali "Prism", "XKeyscore" e "Tempora". Detti programmi di spionaggio sono stati posti in essere in collaborazione con varie agenzie straniere alleate, in particolare con quelle degli Stati parte del trattato "UkUsa", un'alleanza tra Australia, Canada, Nuova Zelanda, Regno Unito e Stati Uniti, i cd. "five-eyes".

extraterritoriale[21]) ricercando, raccogliendo ed analizzando in massa dati personali, non solo riferibili ad organi statali esteri, ma anche a comuni individui, ovunque essi si trovino nel mondo[22]: in quest'ottica, l'uso massimo ed indiscriminato di *FRT* andrebbe a collocarsi a pieno titolo in seno all'inviso fenomeno della sorveglianza di massa, *sub specie* di sorveglianza 'biometrica'.

Sicché i diritti che rischiano di essere violati o comunque limitati dall'utilizzo delle tecnologie di riconoscimento facciale sono plurimi[23]: come si è visto, di più immediata evidenza sembrano essere le potenziali violazioni del diritto al rispetto della vita privata e familiare, del diritto a non subire discriminazioni, nonché di talune libertà fondamentali, quali quella di espressione o di associazione.

Tuttavia, a ben guardare, gli utilizzi più rilevanti della *facial recognition technology* presuppongono la raccolta – talvolta anche in tempo reale – di una quantità considerevole ed indiscriminata di immagini che vengono conservate dal sistema di riferimento, al fine di poter effettuare le comparazioni cui si è fatto cenno, spesso senza ottenere il previo consenso da parte degli individui sottoposti a riconoscimento facciale o, addirittura, a loro insaputa. La 'pervasività' di siffatti sistemi costituisce un aspetto ontologico degli stessi e, soprattutto, un elemento indefettibile ove si voglia ottenere l'utilità che di volta in volta viene promessa dalla maggior parte delle loro applicazioni.

Da ciò sembra potersi desumere che il rapporto tra la tecnologia in esame e la tutela della *privacy* costituisca un *prius* logico-giuridico rispetto alle possibili violazioni di altri diritti o libertà: ove infatti l'identificazione mediante tecniche di riconoscimento facciale fosse ristretta a determinate categorie di individui, avvenisse per motivi legittimi, nel rispetto di condizioni procedurali legislativamente predeterminate, e fosse dunque rispettosa dei principi fondamentali in tema di *data protection*, non è affatto detto che dal suo utilizzo debbano discendere episodi di discriminazione o di limitazione delle libertà fondamentali. Che poi le medesime tecnologie possano essere utilizzate, o in alcuni casi

[21] "According to the leaked information, governmental agencies such as the US National Security Agency or Britain's Government Communications Headquarters, allegedly monitored millions of individuals and a variety of targets in more than 60 countries" T. CHRISTAKIS, K. BOUSLIMANI, *National Security, Surveillance and Human Rights*, in R. GEIß, N. MELZER (eds.), *The Oxford Handbook on the International Law of Global Security*, Oxford, 2020, pp. 699-717, p. 699; M. MILANOVIC, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, in *Harvard International Law Journal*, 2015, n. 1, pp. 81-146.

[22] "Examples of overt and covert digital surveillance in jurisdictions around the world have proliferated, with governmental mass surveillance emerging as a dangerous habit rather than an exceptional measure. Governments reportedly have threatened to ban the services of telecommunication and wireless equipment companies unless given direct access to communication traffic, tapped fibreoptic cables for surveillance purposes, and required companies systematically to disclose bulk information on customers and employees. Furthermore, some have reportedly made use of surveillance of telecommunications networks to target political opposition members and/or political dissidents […] Even non-State groups are now reportedly developing sophisticated digital surveillance capabilities", Assemblea generale, *The Right to privacy in the Digital Age. Report of the Office of the United Nations High Commissioner for Human Rights*, UN Doc. A/HRC/27/37 del 30 giugno 2014, p. 3.

[23] Per un elenco esaustivo delle norme contenute nei principali trattati internazionali sui diritti dell'uomo che potrebbero risultare violate dall'utilizzo delle nuove tecnologie, si legga D. GŁOWACKA, R. YOUNGS, A. PINTEA, E. WOŁOSIK, Directorate General for External Policies of the Union − Policy Department, *Digital technologies as a means of repression*, cit., pp. 34-35.

siano già utilizzate, da privati o da Stati per implementare politiche discriminatorie, e segnatamente per limitare libertà fondamentali di individui o categorie di individui, è questione certamente rilevante, che non attiene però alle particolari caratteristiche della *facial recognition technology*, ma alle politiche discriminatorie in sé. In detta prospettiva, infatti, la *facial recognition technology* è solo l'ultima di una lunga serie di tecnologie che, al pari di innumerevoli altre, può essere utilizzata per perseguire fini illeciti o, comunque, moralmente discutibili.

Quello dei rischi derivanti da un uso generalizzato della *facial recognition technology* pare pertanto costituire tema di non poco momento anche sotto un diverso ed ulteriore profilo, segnatamente in relazione ai già esposti margini di errore caratterizzanti i sistemi di riconoscimento facciale, nonché la loro potenziale eludibilità da parte dei consociati (al riguardo, sembrerebbe essere sufficiente che il soggetto indossi del semplice make-up sul volto per ingannare le tecnologie attualmente disponibili)[24]. Non è un caso che note società informatiche e commerciali abbiano abbandonato il mercato della *FRT* ovvero abbiano dichiarato pubblicamente di sospendere l'offerta di prodotti dotati di tecnologie di riconoscimento facciale[25], verosimilmente in attesa che la relativa tecnologia sia più matura ed affidabile nei risultati.

Senonché, da più parti è stata denunziata la grave assenza, a livello internazionale ed europeo, di un quadro giuridico chiaro ed uniforme sull'uso legittimo delle tecnologie di riconoscimento facciale[26]: lacuna che avrebbe consentito una grande diversità tra le normative statali sul tema *FRT*, a causa delle importanti differenze di vedute politiche al riguardo.

Il presente lavoro aspira a ponderare la veridicità di tale assunto. Si procederà alla verifica della compatibilità della raccolta massiva di immagini personali tipica dei sistemi di riconoscimento facciale con le disposizioni internazionali ed europee di riferimento; rispetto alle prime, e come premessa dell'indagine, l'attenzione sarà concentrata sulla

[24] N. GUETTA, A. SHABTAI, I. SINGH, S. MOMIYAMA, Y. ELOVICI, *Dodging Attack Using Carefully Crafted Natural Makeup*, 2021, disponibile su https://cris.bgu.ac.il/en/publications/dodging-attack-using-carefully-crafted-natural-makeup.

[25] "As recent waves of corporate back-pedalling, Big Tech moratoria, successful litigations and local facial recognition bans have shown […]. In June 2019, Axon, a major producer of police body cameras, responded to a review of its independent ethics board by banning the use of facial analysis algorithms in its systems. Similarly, following the killing of George Floyd and acknowledging the link between facial analysis technologies and legacies of racism and structural discrimination, Microsoft and Amazon announced moratoria on their production of facial recognition software and services, and IBM also announced that it is getting out of the business entirely. Even more recently, the Court of Appeal in South Wales ruled that the local police force could no longer use its automated facial recognition system, AFR Locate, on the grounds that it was not in compliance with significant aspects of the European Convention on Human Rights», D. LESLIE, *Understanding bias in facial recognition technologies*, cit., p. 22.

[26] Ritenendo la *FRT* una tecnologia in grado di condurre alla sorveglianza elettronica di massa, alla discriminazione e all'oppressione, *Amnesty International* ha lanciato la petizione "Ban the Scan" al fine di sollecitare i legislatori nazionali verso l'affermazione di un divieto assoluto di utilizzo della *facial recognition tecnology*; sulla stessa linea d'onda il movimento *ReclaimYourFace*.

Convenzione n. 108[27], trattandosi dell'unico strumento di diritto internazionale pattizio a carattere regionale specificamente dedicato alla materia della protezione dei dati personali, ratificato da tutti gli Stati membri dell'Unione europea e aperto all'adesione anche degli Stati non membri del Consiglio d'Europa. Si esamineranno poi i contenuti degli articoli 7 ed 8 della Carta dei diritti fondamentali alla luce dell'interpretazione che di essi è stata data dalla Corte di giustizia nei precedenti giurisprudenziali riguardanti le misure di sorveglianza elettronica, nonché quelli dell'art. 8 della Convenzione europea dei diritti dell'uomo, trattandosi del diritto corrispondente ai sensi dell'art. 52, paragrafo 3, della Carta. Ciò, al fine di comprendere se, ed eventualmente entro quali limiti, l'utilizzo della *facial recognition technology* possa ritenersi compatibile rispettivamente con il sistema della Convenzione europea dei diritti dell'uomo e con il diritto dell'Unione europea, che del resto ricomprende i principi generali *ex* art. art. 6, paragrafo 3, TUE; e se, conseguentemente, sia effettivamente necessaria o anche solo auspicabile una legislazione specifica diretta a sancirne la liceità o l'illiceità.

2. La normativa regionale adottata nel quadro del Consiglio d'Europa

A livello internazionale, si ritiene che le disposizioni a tutela del diritto alla *privacy* contenute nei principali trattati sui diritti dell'uomo – *in primis* il Patto internazionale sui diritti civili e politici[28], la Convenzione europea dei diritti dell'uomo (di seguito anche CEDU)[29]e la Carta dei diritti fondamentali[30] − siano astrattamente invocabili per far fronte (anche) alle conseguenze dell'utilizzo delle tecnologie di riconoscimento facciale; ciò, malgrado il fatto che, al tempo della loro formulazione, taluni problemi derivanti

[27] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Strasburgo, 28 gennaio 1981; ad oggi ne sono parte tutti gli Stati membri del Consiglio d'Europa, nonché nove Stati non membri (tra di essi, la Federazione Russa).

[28] Art. 17, Patto internazionale sui diritti civili e politici, New York, 16 dicembre 1966: "1. Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione. 2. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese".

[29] Art. 8, Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, Roma, 4 novembre 1950: "1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui".

[30] Art. 7 della Carta dei diritti fondamentali dell'Unione europea, Nizza, 7 dicembre 2000, rubricato "Rispetto della vita privata e della vita familiare": "Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni". Ivi, art. 8, rubricato "Protezione dei dati di carattere personale": "1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

dall'utilizzo di determinati strumenti di *artificial intelligence* non fossero ancora prospettabili.

Giova tuttavia rimarcare l'esistenza di uno strumento internazionale, a carattere regionale, specificamente dedicato alla disciplina della protezione dei dati personali, e le cui norme, di tipo inevitabilmente più dettagliato, possono senz'altro incidere sulla regolamentazione dell'utilizzo di tecnologie di riconoscimento facciale: la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale del 1981[31](di seguito: Convenzione n. 108).

È noto come la Convenzione n. 108 si applichi a tutti i trattamenti automatizzati di dati personali, nel settore pubblico e privato – in tale ambito, anche a quelli effettuati da autorità giudiziarie e di polizia – peraltro contemplando una disciplina dei flussi transfrontalieri di tali dati[32], che possono essere limitati laddove i Paesi di destinazione non garantiscano una protezione equivalente a quella assicurata dal Paese di provenienza[33]. Essa detta regole specifiche per il trattamento delle categorie 'speciali' di dati a carattere personale che "non possono essere elaborati automaticamente"[34] a meno che lo Stato interessato assicuri apposite garanzie. Si tratta dei cd. dati 'sensibili', tra i quali, per quanto non espressamente indicati, si ritiene di dover includere i dati biometrici, almeno nelle ipotesi in cui vengano impiegati ai fini del riconoscimento univoco degli individui. All'evidenza tali garanzie debbono ritenersi 'aggiuntive' rispetto alle salvaguardie già previste, in linea generale, dalla Convenzione per il trattamento di qualsiasi dato personale.

Ed invero, tutti i dati personali oggetto di elaborazione automatica – a più forte ragione se trattasi di dati biometrici – devono essere, *inter alia*: ottenuti ed elaborati in modo trasparente e nel rispetto della legge; risultare adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati, nonché conservati in una forma che consenta l'identificazione delle persone interessate per un periodo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti[35]. Principi, questi ultimi, che rappresentano dei veri e propri cardini in materia di *data protection* e che infatti hanno ispirato la successiva evoluzione normativa[36]. Nondimeno, agli interessati dal trattamento

[31] V. *supra* nota n. 27.
[32] Sul punto, si segnala anche lo specifico protocollo addizionale: Protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri (STE no. 181), Strasburgo, 8 novembre 2001.
[33] "The Convention was an important milestone in the development of data protection as a fundamental right. Unlike the European Convention on Human Rights, membership of Convention 108 does not give rise to jurisdiction of the European Court of Human Rights, so that there is no direct judicial enforcement of the Convention. However, in some cases the European Court of Human Rights has referred to Convention 108, and Article 8 of the European Convention on Human Rights probably includes the obligation to give effect to the provisions of Convention 108. The EU has also committed to ensure that its law is consistent with the relevant conventions of the Council of Europe (though EU law may provide more extensive protection)", C. KUNER, *Transborder Data Flows and Data Privacy Law*, Oxford, 2013, p. 37.
[34] Art. 6, Convenzione sulla protezione delle persone rispetto al trattamento automatizzato, cit.
[35] Ivi, art. 5.
[36] Un *punctum dolens* della Convenzione n. 108 sembra poter essere individuato nell'ambito di applicazione della stessa, confinato alla sola elaborazione automatica di dati personali. Invero, le ipotesi di trattamento non automatico di dati saranno oggetto, solo molti anni dopo, della Direttiva n. 95/46/CE, adottata in seno

automatizzato viene riconosciuto il diritto di essere a conoscenza dell'esistenza di una collezione automatizzata di dati a carattere personale e dei suoi fini, di chiedere la rettifica o la cancellazione dei propri dati ove essi siano stati elaborati "in violazione delle disposizioni di diritto interno che danno attuazione ai principi fondamentali enunciati negli articoli 5 e 6"[37]. Eccezioni o limitazioni ai diritti degli interessati dal trattamento – e, più in particolare, agli articoli 5, 6 ed 8 della Convenzione n. 108 – sono legittime solo se previste dalla legge, rispettose dell'essenza dei diritti e delle libertà fondamentali, nonchè costituenti misura necessaria e proporzionata in una società democratica per la protezione di interessi statali di carattere generale ovvero per la protezione della persona interessata o dei diritti e delle libertà fondamentali altrui.

Dell'appena ricordato trattato è stato peraltro di recente proposto un importante aggiornamento, il protocollo di emendamento del 2018[38], meglio noto come "Convenzione 108 +"[39]. Il processo di modernizzazione – che, tra l'altro, ha portato all'espunzione, sia dal titolo che dall'articolato[40], del riferimento specifico al "trattamento automatizzato" dei dati personali in favore di un più lato "trattamento" − si è svolto in parallelo rispetto alla complessiva riforma delle regole dell'Unione europea sulla *data protection* ed è possibile riscontrare molti punti di contatto, in termini contenutistici, con la disciplina prevista dal Regolamento generale sulla protezione dei dati personali 2016/679.

La convenzione aggiornata prevede nuovi diritti degli interessati: *in primis*, quello a non essere sottoposti a una decisione che li riguardi in modo significativo ove fondata esclusivamente su un trattamento automatizzato di dati, salvo che tale decisione sia stata autorizzata da una legge e questa stabilisca anche misure idonee a salvaguardare i diritti degli interessati[41]; la possibilità di opporsi al trattamento dei propri dati personali[42]; il

all'Unione europea proprio al fine di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati in generale, assicurando al contempo la libera circolazione dei dati personali tra gli Stati membri. Per lungo tempo i due citati strumenti hanno ricoperto un ruolo chiave nello sviluppo di comuni *qualitative principles* in materia, si veda sul punto F. FABBRINI, *Human Rights in the Digital Age: the European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States*, in *Harvard Human Rights Journal*, 2015, pp. 65-95, pp. 71-72. Come si vedrà, almeno a livello di diritto dell'Unione europea, il citato panorama normativo è stato stravolto dal Regolamento generale per la protezione dei dati personali e dalla Direttiva Polizia; detti strumenti hanno infatti abrogato la Direttiva 95/46/CE e la Decisione quadro 2008/977/GAI del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale.

[37] Art. 8, Convenzione sulla protezione delle persone rispetto al trattamento automatizzato, cit.

[38] Protocollo di emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Strasburgo, 10 ottobre 2018. Di seguito, anche "Convenzione n. 108+".

[39] Per raggiungere l'obiettivo dell'entrata in vigore del protocollo di emendamento occorre la ratifica da parte di tutti gli Stati membri della Convenzione n. 108, ovvero, entro la data dell'11 ottobre 2023, la ratifica da parte di almeno trentotto di essi; ciò, consentirebbe di avere uno strumento giuridicamente vincolante a livello internazionale che sia anche aggiornato, nel contesto della protezione dei dati personali.

[40] Si noti che la locuzione "trattamento automatizzato", è stata espunta, *inter alia*, dal dettato dell'articolo 1 dedicato all'oggetto e ai fini della Convenzione n. 108+, nonché da quello dell'articolo 3 relativo al suo campo di applicazione.

[41] Art. 9, parr. 1, lett. a, e 2, Convenzione n. 108+.

[42] Ivi, art. 9, par. 1, lett. d.

diritto a disporre di un ricorso in caso di violazione dei diritti della persona[43]cui corrisponde il dovere degli Stati Parte di stabilire al loro interno rimedi per le violazioni delle disposizioni della Convenzione, oltre che appropriate sanzioni[44].

Ai fini del presente lavoro rileva evidenziare come il protocollo del 2018 abbia emendato il precedente testo dell'articolo 6 della Convenzione, introducendo espressamente i dati biometrici "che identificano univocamente una persona" nell'elenco di categorie speciali di dati il cui trattamento "dovrà" essere consentito "soltanto" ove sussistano "apposite garanzie sancite nella legislazione dello Stato membro a complemento di quelle previste dalla Convenzione" [45]; al secondo paragrafo, la norma stabilisce come siffatte salvaguardie debbano essere idonee a prevenire i rischi che il trattamento di dati sensibili possa comportare per gli interessi, i diritti e le libertà fondamentali dell'interessato, con particolare riferimento al rischio discriminatorio.

A distanza di quarant'anni dall'apertura alla firma della Convenzione n. 108, il Comitato dalla stessa istituito *ex* art. 18, ha pubblicato delle linee guida[46] specificamente dedicate al riconoscimento facciale, il cui campo di applicazione investe sia il settore privato che quello pubblico. Le linee guida, che si fondano sui principi della Convenzione n. 108 modernizzata, forniscono una serie di misure di riferimento tanto per i legislatori nazionali e i governanti, che per gli stessi produttori (e venditori) di sistemi di riconoscimento facciale. Ed il loro filo conduttore è costituito dall'idea che l'uso della *FRT* debba sempre presupporre il superamento di 'un vaglio di necessità'.

Per alcuni utilizzi della *FRT*, le linee guida auspicano l'adozione di una normativa interna molto restrittiva, che in alcune occasioni consiste nell'imposizione di un vero e proprio divieto legislativo: così, ad esempio, per l'uso della *FRT* in tempo reale negli *uncontrolled environments* (luoghi pubblici, come le piazze, o aperti al pubblico, come le scuole, i centri commerciali, gli ospedali), ovvero per la cd. *affect recognition*, cioè l'applicazione della *FRT* finalizzata alla identificazione e classificazione delle emozioni umane[47]. Viene poi condivisibilmente raccomandata la necessità di condizionare la liceità del trattamento di dati biometrici tramite *FRT* a requisiti di volta in volta diversi, a seconda del contesto in cui la *FRT* venga utilizzata, della fase in cui la stessa verta – in fase di sviluppo della tecnologia (formazione della *watchlist*), piuttosto che in fase di concreta applicazione − o ancora dell'intrusività della specifica *FRT* in considerazione. In particolare, nel settore pubblico, considerando lo squilibrio di poteri tra individui interessati dal trattamento e autorità pubbliche, il tradizionale e diffuso requisito del consenso potrebbe rivelarsi insufficiente: "legislators and decision makers have to lay down specific rules for biometric processing using facial recognition technologies for law enforcement purposes. These rules will ensure that such uses must be strictly necessary

[43] Ivi, art. 9, par. 1, lett. f.
[44] Ivi, art. 12.
[45] Ivi, art. 6.
[46] Consiglio d'Europa, Comitato Consultivo della Convenzione n. 108, *Linee Guida sul riconoscimento facciale*, 28 gennaio 2021, reperibili su https://www.coe.int/it/web/portal/-/facial-recognition-strict-regulation-is-needed-to-prevent-human-rights-violations.
[47] Ivi, p. 8.

and proportionate to these purposes and prescribe the necessary safeguards to be provided" [48]. Ed anche nel settore privato, dove ad avviso del Comitato consultivo della Convenzione n. 108 il consenso dell'individuo sottoposto a trattamento potrebbe invece costituire un valido fondamento per la raccolta dei dati biometrici, si ricorda come detto consenso, per potersi ritenere valido, debba essere informato, libero, specifico ed esplicito; per inciso, affinché un consenso possa definirsi effettivamente libero, al soggetto dovrebbe essere stata (quantomeno) offerta una soluzione alternativa rispetto alla *FRT* (per esempio, la possibilità di ricorrere ad una *password* o a un *badge* identificativo per ottenere la medesima utilità)[49].

Ciò premesso, a titolo di completezza va detto che il panorama normativo internazionale è parimenti ricco di risoluzioni e atti programmatici riferibili al tema dell'*artificial intelligence*, in seno ai quali è talvolta possibile riscontrare riferimenti espressi o mediati alla *FRT*. Invero, facendo leva sulla ritenuta 'natura generica' dell'art. 17 del Patto sui diritti civili e politici e dell'art. 8 della CEDU, varie istituzioni a tutela dei diritti umani hanno incentivato il ricorso alla predisposizione di strumenti di *soft law*, sull'assunto che gli stessi, sebbene non dotati di efficacia vincolante, possano pur sempre giocare un ruolo significativo nell'interpretazione e nell'applicazione delle norme internazionali di riferimento[50], inducendo gli Stati e gli attori non statali a dotarsi di regole il più possibile compatibili con gli *standards* di tutela dei diritti umani.

Sul punto, sembra possibile rinvenire una sostanziale coerenza tra i contenuti degli strumenti regionali di diritto internazionale pattizio sopracitati e la normativa internazionale universale. Invero, anche solo limitandosi al contesto delle Nazioni Unite, è stato evidenziato[51]come già da tempo il Segretario Generale abbia annunciato un piano d'azione[52]finalizzato ad individuare le modalità con cui il sistema delle Nazioni Unite avrebbe potuto sostenere l'uso delle nuove tecnologie garantendone al contempo la compatibilità con il diritto internazionale dei diritti umani, anche al fine di accelerare il raggiungimento degli obiettivi previsti dall'Agenda 2030 per lo sviluppo sostenibile[53]; a tale ultimo proposito è stato peraltro istituito un comitato per la cooperazione digitale, avente il precipuo scopo di pianificare le azioni idonee a mitigare l'impatto sociale, etico, legale ed economico delle tecnologie digitali, massimizzandone i benefici e minimizzandone i danni[54]. Sulla base delle relazioni redatte dall'*High-level Panel on Digital Cooperation*, il Segretario Generale ha lanciato la cd. *Roadmap for digital*

[48] Ivi, pp. 9-10. Le linee guida ricomprendono nell'ambito del settore pubblico anche l'utilizzo della *FRT* da parte di entità di natura privata che siano state a ciò autorizzate dall'autorità pubblica.
[49] Ivi, p. 11.
[50] Ivi, p. 33.
[51] Ivi, p. 36.
[52] A. GUTERRES, Segretario Generale delle Nazioni Unite, *Strategy on new technologies*, New York, 2018, disponibile su https://www.un.org/en/newtechnologies.
[53] Risoluzione dell'Assemblea Generale, *Transforming our world: the 2030 Agenda for Sustainable Development*, 25 settembre 2015, A/RES/70/1.
[54] Report dell'High-level Panel on Digital Cooperation, *The age of digital interdependence: report of the UN Secretary-General's High-Level Panel on Digital Cooperation*, New York, 2019, disponibile su https://digitallibrary.un.org/record/3865925.

cooperation[55]: un piano d'azione per la cooperazione digitale che, prendendo atto dei rischi derivanti (anche) dalle tecniche di riconoscimento facciale[56], contiene raccomandazioni sulle azioni concrete da intraprendere a livello statale e prevede l'istituzione di un organo consultivo per la cooperazione globale verso un'intelligenza artificiale *human-rights based*[57].

In un *report*[58] è stato esaminato l'impatto della *artificial intelligence* sulla libertà di espressione, sul diritto alla *privacy* e alla non discriminazione; il Relatore Speciale, nel tentativo di definire i termini essenziali della relazione 'diritti umani-intelligenza artificiale' e sul presupposto che quest'ultima metta in discussione i pilastri della disciplina internazionale della protezione dei dati personali (precipuamente la tradizionale nozione di consenso), ha tentato di delineare un quadro giuridico di riferimento, nonché di elaborare alcune conseguenti raccomandazioni: la necessità di una valutazione di impatto sul godimento dei diritti fondamentali della tecnologia di turno già in fase di *design* della stessa, e comunque *prima* che venga immessa sul mercato; l'opportunità dell'espletamento di *audit* periodici, condotti da periti terzi ed imparziali; l'urgenza di stabilire rimedi agevoli ed effettivi esperibili dai soggetti i cui diritti sono potenzialmente affetti da tale tecnologia.

Sempre in seno alle Nazioni Unite, il Consiglio per i diritti umani ha evidenziato i rischi derivanti dalle attività di profilazione – con riferimento alle quali la *FRT* occupa un posto di primo piano – riconoscendo espressamente il rischio che l'elaborazione automatica di dati personali possa condurre a discriminazione o, comunque, a decisioni

[55] A. GUTERRES, Segretario Generale delle Nazioni Unite, *Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation. Report of the Secretary-General*, 29 maggio 2020, A/74/821.

[56] Ivi, parr. 49-50: «there are reports of targeted communications surveillance and facial recognition software that could result in human rights violations and lead to arbitrary arrests or detentions and violation of the right to peaceful protest. These technologies may also misidentify certain minority groups and cement existing social biases […]. It is critical that legislation and safeguards are in place to protect people from unlawful or unnecessary surveillance, including any arbitrary surveillance that may be carried out by State actors in cyberspace, as well as in the physical world».

[57] Ivi, parr. 88-89: «I intend to establish a multi-stakeholder advisory body on global artificial intelligence cooperation to provide guidance to myself and the international community on artificial intelligence that is trustworthy, human-rights based, safe and sustainable and promotes peace. The advisory body will comprise Member States, relevant United Nations entities, interested companies, academic institutions and civil society groups. Such a body could also serve as a diverse forum to share and promote best practices, as well as exchange views on artificial intelligence standardization and compliance efforts, while taking into account existing mandates and institutions».

[58] DAVID KAYE, Relatore Speciale delle Nazioni Unite sulla libertà di opinione ed espressione, *Promotion and protection of the right to freedom of opinion and expression*, 29 agosto 2018, A/73/348, par. 1: "Artificial intelligence recommends people to friend or follow, news articles to read and places to visit or eat, shop or sleep. It offers speed, efficiency and scale, operating to help the largest companies in the information and communications technology sector manage the huge amounts of content uploaded to their platforms every day. Artificial intelligence technologies may enable broader and quicker sharing of information and ideas globally, a tremendous opportunity for freedom of expression and access to information. At the same time, the opacity of artificial intelligence also risks interfering with individual self-determination […]: how can States, companies and civil society ensure that artificial intelligence technologies reinforce and respect, rather than undermine and imperil, human rights?".

aventi il potenziale effetto di limitare il godimento di determinati diritti umani[59]. Nel contesto del diritto a manifestare pacificamente, il Consiglio ha peraltro adottato una risoluzione in cui si condanna *expressis verbis* l'uso delle tecnologie di riconoscimento facciale[60], potendo lo stesso tradursi nella riluttanza e nella refrattarietà dei soggetti 'riconosciuti' rispetto all'esercizio di una libertà fondamentale: ciò che è stato peraltro ribadito nel *General Comment* n. 37, di recente adottato[61].

3. Il quadro normativo di riferimento a livello di diritto dell'Unione europea: il diritto vigente

Quali emanazioni settoriali degli artt. 7 e 8 della Carta dei diritti fondamentali, anche il Regolamento Generale sulla protezione dei dati personali[62] e la direttiva 2016/680 sulla protezione dei dati personali nelle attività di polizia e giudiziarie[63] (d'ora innanzi, "Direttiva Polizia"), risultano parimenti applicabili al fenomeno della *FRT*, occupandosi, entrambi gli strumenti citati, del trattamento automatizzato e manuale di dati personali contenuti in un archivio o destinati a figurarvi[64]. Mentre la Direttiva Polizia costituisce un regime normativo specifico per le ipotesi in cui la pubblica autorità (o il privato incaricato di esercitare poteri pubblici) utilizzi dati personali allo scopo di prevenzione, indagine, accertamento, perseguimento di reati o di esecuzione di sanzioni penali, il Regolamento generale sulla protezione dei dati personali offre il quadro normativo *de residuo*, essendo applicabile a tutte le ipotesi in cui i dati personali vengano raccolti per finalità diverse da quelle della Direttiva Polizia[65].

---

[59] "Automatic processing of personal data for individual profiling may lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights, and recognizing the need to further discuss and analyse these practices on the basis of international human rights law», Risoluzione del Consiglio per i diritti umani, *The right to privacy in the digital age*, 23 marzo 2017, A/HRC/RES/34/7; v. anche Risoluzione del Consiglio per i diritti umani, *New and emerging digital technologies and human rights*, 11 luglio 2019, A/HRC/RES/41/11.

[60] "Expressing its concern also at the unlawful or arbitrary surveillance, both in physical spaces and online, of individuals engaged in peaceful protests, including through the use of new and emerging digital tracking tools such as facial recognition, international mobile subscriber identity-catchers ("stingrays") and closed-circuit television", Risoluzione del Consiglio per i diritti umani, *The promotion and protection of human rights in the context of peaceful protests*, 13 luglio 2020, A/HRC/44/L.1, p. 3.

[61] Comitato per i diritti umani, *General comment No. 37 (2020) on the right of peaceful assembly (article 21)*, 17 settembre 2020, CCPR/C/GC/37, par. 62: "The mere fact that a particular assembly takes place in public does not mean that participants' privacy cannot be violated. The right to privacy may be infringed, for example, by facial recognition and other technologies that can identify individual participants in a crowd".

[62] V. *supra* nota n. 1.

[63] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, in GUUE L 119 del 4 maggio 2016, pp. 89-131.

[64] Art. 2, Direttiva Polizia; art. 2, par. 1, Regolamento generale sulla protezione dei dati personali.

[65] Sui rispettivi ambiti di applicazione, v. Corte di giustizia, Quinta Sezione, sentenza del 26 gennaio 2023, causa C-205/21, *V.S. c. Ministerstvo na vatreshnite raboti e altri*, par. 63: "l'articolo 10 della direttiva

È stato pertanto evidenziato come[66], alla luce dei principi basilari sulla protezione dei dati personali contenuti nei menzionati atti di diritto derivato[67], il trattamento di immagini finalizzato al riconoscimento di un volto debba quantomeno: i. risultare lecito, corretto e trasparente; ii. perseguire finalità determinate, esplicite e legittime; iii. rispettare i requisiti di minimizzazione e accuratezza dei dati, limitazione della loro conservazione nel tempo, sicurezza e responsabilizzazione.

Sotto il primo profilo, affinché un trattamento di dati personali possa dirsi lecito è anzitutto necessario che i dati siano stati raccolti sulla base di un fondamento valido ai sensi dell'art. 6 del Regolamento generale sulla protezione dei dati personali o dell'art. 8 della Direttiva Polizia. Ma nel contesto della *facial recognition technology* i dati personali elaborati sono dati biometrici "intesi a identificare in modo univoco una persona fisica" e, quindi, dati sensibili *ex* art. 9 del Regolamento, sicché il loro trattamento è considerato in linea di principio vietato[68], salvo che ricorra una delle rigide condizioni specificate nei paragrafi successivi della disposizione medesima[69]; così pure nel campo di applicazione della Direttiva Polizia, ove se ne prescrive l'autorizzabilità "solo se strettamente

2016/680 prevede che il trattamento di tali dati sensibili è autorizzato «solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato» e soltanto in tre ipotesi, in particolare, ai sensi di tale articolo, lettera a), se tale trattamento è autorizzato dal diritto dell'Unione o dello Stato membro. Per contro, il paragrafo 1 dell'articolo 9 del RGPD enuncia un divieto di principio del trattamento di detti dati sensibili, corredato di un elenco di situazioni, elencate al paragrafo 2 di tale articolo, nelle quali si può derogare a tale divieto, elenco che non menziona situazioni corrispondenti a quella di un trattamento di dati per finalità come quelle di cui all'articolo 1, paragrafo 1, di detta direttiva e che soddisferebbe il requisito di cui all'articolo 10, lettera a), di quest'ultima. Ne consegue che, mentre un trattamento di dati biometrici e genetici da parte delle autorità competenti a fini rientranti nell'ambito di applicazione della direttiva 2016/680 può essere autorizzato purché, conformemente ai requisiti enunciati all'articolo 10 di quest'ultima, sia strettamente necessario, soggetto a garanzie adeguate e previsto dal diritto dell'Unione o dello Stato membro, ciò non avviene necessariamente nel caso di un trattamento di questi stessi dati rientrante nell'ambito di applicazione del RGPD".

[66] T. MADIEGA, H. MILDEBRATH, *Regulating facial recognition in the EU*, cit., pp. 10-17.

[67] Art. 5, Regolamento generale sulla protezione dei dati personali; art. 4, Direttiva Polizia.

[68] Art. 9, par. 1, Regolamento generale sulla protezione dei dati personali: "*È vietato* trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, *dati biometrici intesi a identificare in modo univoco una persona fisica*, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" (corsivo aggiunto).

[69] Art. 9, par. 2, Regolamento generale sulla protezione dei dati personali: "Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; […] g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato […]".

necessario"[70]. A più forte ragione sono vietate le decisioni basate unicamente sul trattamento automatizzato di dati sensibili, salvo che gli stessi siano stati acquisiti dietro esplicito consenso (art. 9, paragrafo 2, lett. a) o per motivi di interesse pubblico (art. 9, paragrafo 2, lett. g) e siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato[71]. Sempre in punto di liceità, le norme del diritto dell'Unione europea richiedono poi che il trattamento avvenga in modo corretto[72]e trasparente nei confronti della persona fisica interessata[73]; ciò, tuttavia, non impedisce di per sé alle autorità incaricate dell'applicazione della legge di svolgere attività quali operazioni di infiltrazione o videosorveglianza, purché siano previste dalla legge e costituiscano una misura necessaria e proporzionata in una società democratica[74].

Quanto invece al perseguimento di uno scopo determinato, esplicito e legittimo, non va dimenticato che la *FRT* presenta un altissimo rischio di 'function creep'[75], cioè un

[70] Art. 10 Direttiva Polizia: "Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di *dati biometrici intesi a identificare in modo univoco una persona fisica* o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale *è autorizzato solo se strettamente necessario*, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto: a) se autorizzato dal diritto dell'Unione o dello Stato membro; b) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; o c) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato".

[71] Art. 22, par. 4, Regolamento generale sulla protezione dei dati personali; art. 11, par. 2, Direttiva Polizia.

[72] È stato sottolineato come il principio di correttezza del trattamento non debba essere considerato un *minus* rispetto ai principi di trasparenza o di liceità, avendo al contrario un proprio specifico significato: "fairness refers to a substantial balancing of interests among data controllers and data subjects. The GDPR approach of fairness is, thus, effect-based: what is relevant is not the formal respect of procedures (in terms of transparency, lawfulness or accountability), but the substantial mitigation of unfair imbalances that create situations of "vulnerability"", G. MALGIERI, *The concept of Fairness in the GDPR: a linguistic and contextual interpretation*, in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 27-30 gennaio 2020, Barcellona, pp. 154-166, p. 162.

[73] Sull'utilizzo della *FRT* al di fuori delle attività di polizia, il Comitato europeo per la protezione dei dati ha raccomandato un approccio a due livelli ai fini del rispetto del principio di trasparenza: l'informazione più importante sull'attività di *FRT* dovrebbe essere fornita all'interessato attraverso dei cartelli di segnalazione posti prima dell'ingresso dell'area monitorata; poi, ulteriori dettagli potrebbero essere comunicati attraverso altri mezzi (ad esempio siti web o codici QR). Per approfondimenti, Comitato europeo per la protezione dei dati (EDPB), *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, 29 gennaio 2020.

[74] Art. 13, par. 3, della Direttiva Polizia: "Gli Stati membri possono adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato ai sensi del paragrafo 2 nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di: a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari; b) non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; c) proteggere la sicurezza pubblica; d) proteggere la sicurezza nazionale; e) proteggere i diritti e le libertà altrui.".

[75] "Such 'function creep' may also happen if fingerprints – taken for whatever purpose – are included in searches done for criminal investigation purposes. This was the case in Ireland, when an audit by the Data Protection Commissioner revealed that fingerprints taken in the context of asylum or visa applications were included in all fingerprint searches carried out during police investigations, irrespective of whether there was any reason to believe that the immigrant or asylum seeker was involved in a crime", Agenzia dell'Unione europea per i diritti fondamentali (FRA), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, 2018, p. 61, su https://fra.europa.eu/en/publication/2018/under-watchful-eyes-biometrics-eu-it-systems-and-fundamental-rights; L. HOUWING, *Stop the Creep of Biometric Surveillance*

pericolo di deviazione dallo scopo inizialmente dichiarato della raccolta di dati personali. Pertanto, un sistema che ne preveda l'utilizzo dovrebbe includere salvaguardie atte a prevenire utilizzi per finalità non autorizzate dagli interessati. Difatti, il principio della limitazione delle finalità − cristallizzato nell'articolo 8, paragrafo 2, della Carta, nonché nell'articolo 5, paragrafo 1, lettera b, del Regolamento generale sulla protezione dei dati personali e l'articolo 4, paragrafo 1, lett. b, della Direttiva Polizia − richiede che i dati personali siano trattati solo per finalità specifiche, esplicitamente definite, e che, una volta raccolti, essi non vengano trattati in modo incompatibile con tali finalità (o addirittura per altri scopi).

Circa il rispetto del principio di minimizzazione[76], di accuratezza[77], limitazione della loro conservazione nel tempo[78], sicurezza[79]e responsabilizzazione[80], in premessa sono stati evidenziati i pericoli legati all'utilizzo della *FRT*, i cui più rilevanti utilizzi presuppongono la raccolta – talvolta anche in tempo reale – di una quantità considerevole ed indiscriminata di immagini[81]che vengono conservate dal sistema di riferimento, spesso rendendone quasi impossibile l'aggiornamento o la rettifica, in virtù della ingente mole delle banche dati; si è fatto altresì cenno agli errori che possono (e che sono) derivati dai processi di identificazione o di comparazione dei volti umani, nonché della potenziale lesione su larga scala dei diritti fondamentali degli individui e dei rischi legati alle intrusioni abusive nei *database* e agli usi illeciti delle immagini ivi presenti (si pensi, uno per tutti, al caso *Clearview*[82]).

Technology, in *European Data Protection Law Review*, 2020, pp. 174-177, p. 176: "A concern we have about calling for new regulation addressing biometric surveillance in the public space, is that we will not be able to contain the use. The call for regulation is a call for a limited legal basis for the deployment of this extremely invasive technology. History has taught us never to underestimate a good function creep".

[76] Secondo tale principio i dati dovrebbero essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati, art. 5, par. 1, lett. c, Regolamento generale sulla protezione dei dati personali. Si veda anche l'art. 4, par. 1, lett. c, Direttiva Polizia.

[77] Secondo tale principio i dati dovrebbero essere esatti e, se necessario, aggiornati, art. 5, par. 1, lett. d, Regolamento generale sulla protezione dei dati personali. Si veda anche l'art. 4, par. 1, lett. d, Direttiva Polizia.

[78] Secondo tale principio i dati dovrebbero essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati, art. 5, par. 1, lett. e, Regolamento generale sulla protezione dei dati personali. Si veda anche l'art. 4, par. 1, lett. e, Direttiva Polizia.

[79] Secondo tale principio il titolare del trattamento deve attuare misure tecniche ed organizzative tali da mettere al riparo i dati personali raccolti, tanto da trattamenti non autorizzati (o illeciti), quanto dalla perdita, dalla distruzione e dal danno accidentali, art. 5, par. 1, lett. f, Regolamento generale sulla protezione dei dati personali. Si veda anche l'art. 4, par. 1, lett. f, Direttiva Polizia.

[80] Secondo tale principio è il titolare del trattamento a dover assicurare il rispetto di tutti i suesposti principi e, soprattutto, egli è tenuto a "comprovare" di aver adottato tutti i comportamenti o le misure necessarie in tal senso, art. 5, par. 2, Regolamento generale sulla protezione dei dati personali.

[81] In base all'art. 25 del Regolamento generale sulla protezione dei dati personali, i titolari del trattamento sono tenuti a programmare *ab initio* le loro attività di elaborazione dati nel rispetto dei principi di *privacy by design* e *privacy by default* (si veda anche l'art. 20 della Direttiva Polizia). Ciò, non può non avere un effetto, quantomeno indiretto, sugli stessi produttori e venditori di sistemi dotati di *FRT*. Per approfondimenti, Comitato europeo per la protezione dei dati (EDPB), *Linee guida 4/2019 sull'articolo 25. Protezione dei dati fin dalla progettazione e per impostazione predefinita*, 20 ottobre 2020.

[82] Con ordinanza ingiunzione del 10 febbraio 2022, il garante per la protezione dei dati personali italiano ha comminato una sanzione di 20 milioni di euro alla società statunitense Clearview AI Inc., dichiarando

4. La proposta di regolamento sull'intelligenza artificiale

Il quadro normativo sinora descritto deve oggi aggiungersi la proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (anche nota come "legge sull'intelligenza artificiale")[83]. La bozza di regolamento − che tiene fede all'impegno politico della Presidente von der Leyen sulla presentazione di una proposta legislativa per un approccio europeo coordinato alle implicazioni umane ed etiche dell'intelligenza artificiale[84] − intende promuovere lo sviluppo e l'utilizzo dell'intelligenza artificiale nella prospettiva di una auspicata *leadership* tecnologica dell'Unione europea, senza che possa ritenersi in alcuna misura derogata la disciplina di cui al Regolamento generale sulla protezione dei dati e alla Direttiva Polizia, rispetto ai quali la stessa si pone, dichiaratamente, in un rapporto di integrazione[85].

Senonché, nell'ottica di non creare restrizioni eccessive al commercio e di predisporre dei meccanismi flessibili in grado di adeguarsi dinamicamente all'evoluzione della tecnologia[86], viene proposto un approccio normativo basato sul rischio: la regolamentazione dell'utilizzo dei sistemi di intelligenza artificiale è differenziata in base alle caratteristiche del sistema specificamente utilizzato, se "ad alto rischio" o "a basso rischio" rispetto alla possibilità di pregiudicare i diritti e le libertà fondamentali della persona. Per i sistemi ad alto rischio la bozza di regolamento propone l'imposizione del rispetto di una serie di requisiti obbligatori[87], nonché l'ottenimento di una valutazione della conformità *ex ante*, prima che il prodotto di turno venga immesso sul mercato[88]; di converso, per i sistemi a basso rischio, viene sostanzialmente suggerita l'imposizione di obblighi minimi di trasparenza[89].

Le pratiche di intelligenza artificiale di cui si propone il divieto sono ben poche e concernono esclusivamente quei sistemi di intelligenza artificiale che, attraverso tecniche subliminali, appaiono in grado di agire su una persona inconsapevole, distorcendone il

---

l'illiceità del trattamento di dati personali effettuato dalla Società, in violazione degli artt. 5, par. 1, lett. a), b) ed e), 6, 9, 12, 13, 14, 15 e 27 del Regolamento. Clearview Ai Inc. è nota per aver creato un motore di ricerca finalizzato al riconoscimento facciale (*facial recognition search engine*) che mette a disposizione di forze di polizia e agenzie governative interessate, dietro corrispettivo. La Società ha formato un database di oltre 30 miliardi di immagini attraverso tecniche di *web scraping*, cioè estraendo immagini da *social network*, blog e, in generale, da siti web che mettano a disposizione del pubblico video o fotografie (es. YouTube).

[83] Proposta di Regolamento del Parlamento europeo e del Consiglio *che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, 21 aprile 2021, COM/2021/206 def., pp. 1-108, disponibile su https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52021PC0206.

[84] Commissione europea, Direzione generale della Comunicazione, U. LEYEN, *Un'Unione più ambiziosa: il mio programma per l'Europa: orientamenti politici per la prossima Commissione europea 2019-2024*, Ufficio delle pubblicazioni, 2019, https://data.europa.eu/doi/10.2775/523340, p. 14. Si veda anche: Commissione europea, *Libro bianco sull'intelligenza artificiale − Un approccio europeo all'eccellenza e alla fiducia*, 19 febbraio 2020, COM(2020) 65 def.

[85] Proposta di regolamento, cit., pp. 1 e 4.

[86] Proposta di regolamento, cit., pp. 1 e 3.

[87] Ivi, artt. 8-15.

[88] Ivi, artt. 40-51.

[89] Ivi, art. 52.

comportamento, con conseguente danno, fisico o psicologico, alla stessa o agli altri[90](come potrebbe accadere con alcune applicazioni della *FRT*, quali quelle finalizzate alla identificazione e classificazione delle emozioni umane) ovvero i sistemi di intelligenza artificiale che consentano la valutazione o la classificazione dell'affidabilità di persone fisiche mediante l'attribuzione di un punteggio sociale da cui possano dipendere trattamenti pregiudizievoli o sfavorevole da parte della pubblica autorità[91].

All'elenco di pratiche di intelligenza artificiale da vietare, la Commissione ha poi aggiunto l'uso dei sistemi di identificazione biometrica remota a fini di attività di contrasto in spazi accessibili al pubblico e "in tempo reale"[92]: dunque, l'ipotesi applicativa di *FRT* più temuta dagli attivisti per i diritti umani alla luce del pericolo di deriva in uno stato di sorveglianza elettronica di massa[93]. Ma tale divieto non presenta il carattere di assolutezza comune alle ipotesi che lo precedono. Infatti, a ben guardare, sulla base della proposta, la *facial recognition technology* per attività di contrasto *può* essere utilizzata, anche in spazi aperti e nella sua più temuta modalità *live*, se e nella misura in cui il suo utilizzo venga ritenuto strettamente necessario per il raggiungimento di tre precisi obiettivi: la ricerca mirata di potenziali vittime specifiche di un reato, compresi i minori scomparsi; la prevenzione di una minaccia specifica e imminente per l'incolumità delle persone o di un attacco terroristico; l'individuazione, la localizzazione, l'identificazione o il perseguimento del responsabile (o presunto tale) di un reato *ex* art. 2, paragrafo 2, della decisione quadro sul mandato di arresto europeo[94]. Ciò subordinatamente al rilascio, da parte di un'autorità amministrativa indipendente o giudiziaria dello Stato membro in cui deve avvenire l'uso, di un'autorizzazione preventiva che, in situazioni di motivata urgenza, può anche intervenire in un tempo successivo alla raccolta dei dati mediante FRT[95]. Ne consegue che, in ultima analisi,

[90] Ivi, art. 5, par. 1, lett. a; ciò vale anche per il caso in cui non vengano applicate tecniche subliminali ma i soggetti interessati appartengano ad un gruppo di persone vulnerabili (per età, per disabilità fisica o mentale), v. art. 5, par. 1, lett. b.

[91] Ivi, art. 5, par. 1, lett. c. In altre e più chiare parole la Commissione ritiene che debba essere vietata ogni pratica di intelligenza artificiale che possa risultare nel fenomeno del *social scoring*, particolarmente noto a seguito dell'iniziativa della Repubblica Popolare Cinese di creare un sistema nazionale volto a classificare la reputazione dei propri cittadini, cd. sistema di credito sociale. Per quanto l'esperienza cinese detenga senz'altro il primato in termini di estensione ed intrusività, non bisogna per ciò solo ritenere che il *social scoring* sia estraneo alla mentalità europea, tantomeno a quella nazionale. Alcuni enti locali sono finiti sotto la lente del Garante per la *privacy* italiano in virtù di iniziative basate su soluzioni di tipo premiale che fanno ricorso a meccanismi di *scoring* associati a comportamenti "virtuosi" del cittadino, in diversi settori. Sul punto, si veda Garante per la protezione dei dati personali, Comunicato stampa, *"Cittadinanza a punti": Garante privacy ha avviato tre istruttorie. Preoccupanti i meccanismi di scoring che premiano i cittadini "virtuosi"*, 8 giugno 2022, su www.garanteprivacy.it.

[92] Art. 5, par. 1, lett. d, Proposta di regolamento, cit.

[93] V. *supra* nota n. 26.

[94] Decisione-quadro 2002/584/GAI del 12 giugno 2002 *relativa al mandato di arresto europeo e alle procedure di consegna tra Stati membri*, in GUCE L 190 del 18 luglio 2002.

[95] Art. 5, par. 3, Proposta di regolamento, cit.: "ogni singolo uso di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità alle regole dettagliate del diritto nazionale di cui al paragrafo 4. Tuttavia, in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione e richiedere

secondo il testo della Proposta, un'ampia gamma di tecnologie di riconoscimento facciale, in tempo reale o in differita, utilizzate dalle autorità pubbliche per scopi diversi dalla prevenzione dei reati (ad esempio, controllo delle frontiere, trasporti pubblici e persino scuole) potrà ritenersi consentita[96]; e lo stesso deve dirsi per l'utilizzo in tempo reale della *FRT* in spazi accessibili al pubblico da parte di soggetti privati (così, ad esempio, la scansione degli acquirenti che entrano nei supermercati, il controllo dell'ingresso negli stadi, nelle scuole e nei trasporti), per quanto a condizione che essa venga effettuata previa valutazione di conformità e nel rispetto degli ulteriori requisiti richiesti ai sistemi di intelligenza artificiale "ad alto rischio". Difatti, tali sistemi di intelligenza artificiale, nonostante siano classificati come "ad alto rischio", non sono vietati di *default*, bensì sono soggetti ad alcuni obblighi di conformità: i fornitori di sistemi di riconoscimento facciale saranno tenuti, tra l'altro, ad effettuare un'adeguata valutazione del rischio − per inciso, già dovuta in virtù del Regolamento generale sulla protezione dei dati personali, cd. *impact assessment*[97] − e ad implementare misure di mitigazione del rischio, utilizzare dati di alta qualità, garantire trasparenza, attuare adeguate misure di supervisione umana e, in generale, garantire che tali sistemi siano progettati con un livello adeguato di accuratezza, robustezza e sicurezza informatica.

Resta fermo che qualsiasi utilizzo di *facial recognition technology* in tempo reale o in differita, in spazi pubblici, aperti al pubblico o in privato, rimane sempre soggetto al rispetto delle norme sancite nel Regolamento generale sulla protezione dei dati personali (e nella Direttiva Polizia, con riferimento alle ipotesi rientranti nel suo campo di applicazione), rispetto alle quali gli anzidetti requisiti richiesti dalla Proposta di Regolamento sull'intelligenza artificiale sembrano sovente rappresentare mere specificazioni, se non vere e proprie ripetizioni.

---

l'autorizzazione solo durante o dopo l'uso. L'autorità giudiziaria o amministrativa competente rilascia l'autorizzazione solo se ha accertato, sulla base di prove oggettive o indicazioni chiare che le sono state presentate, che l'uso del sistema di identificazione biometrica remota "in tempo reale" in questione è necessario e proporzionato al conseguimento di uno degli obiettivi di cui al paragrafo 1, lettera d), come indicato nella richiesta. Nel decidere in merito alla richiesta, l'autorità giudiziaria o amministrativa competente tiene conto degli elementi di cui al paragrafo 2".

[96] Per una efficace critica alla Proposta di Regolamento sull'intelligenza artificiale si veda V.L. RAPOSO, *Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence*, in *International Journal of Law and Information Technology*, 2022, pp. 88-109; F. DONATI, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, in *Diritto dell'Unione europea*, 2021, nn. 3-4, pp. 453-466. Sull'opportunità di escludere da taluni contesti delicati, come quello migratorio, la tecnica delle decisioni automatizzate fondate su sistemi di intelligenza artificiale, v. in particolare L. JASMONTAITE-ZANIEWICZ, J. ZOMIGNANI BARBOZA, *Disproportionate Surveillance: Technology-Assisted and Automated Decisions in Asylum Applications in the EU?*, in *International Journal of Refugee Law*, 2021, pp. 89-110.

[97] Art. 35, Regolamento generale sulla protezione dei dati personali.

5. Sulla dubbia legittimità dell'utilizzo della *facial recognition technology* in base ai contenuti degli articoli 7 e 8 della Carta dei diritti fondamentali

In seno alla Carta dei diritti fondamentali il diritto al rispetto della vita privata e familiare (art. 7) e quello alla protezione dei dati di carattere personale (art. 8) vengono scissi: ad ognuno di essi è stata dedicata un'apposita disposizione. Tale scelta riflette il dibattito, mai sopito, sul rapporto intercorrente tra i due macro-contenuti del diritto alla *privacy*: se per parte della dottrina la relazione intercorrente tra *privacy* e *data protection* sarebbe configurabile in termini di genere a specie, per altra parte le stesse dovrebbero considerarsi due fattispecie del tutto autonome[98]; vi è poi un orientamento che media tra le due menzionate posizioni, proponendo la tesi secondo cui il diritto al rispetto della vita privata e quello alla protezione dei dati personali sarebbero "*twins but not identical*", ammettendo, quindi, parziali sovrapposizioni fra i due[99]. E del resto, la scissione normativa operata in seno alla Carta sembra confermare il fatto che, nonostante le possibili coincidenze di contenuti, la disciplina della *data protection* presenti limitazioni e scopi parzialmente diversi, o comunque ulteriori, rispetto al diritto alla vita privata e familiare *tout court*, tanto da aver fatto ritenere la scelta di formulare due distinte disposizioni "non meramente simbolica"[100].

Poiché la *facial recognition technology* implica l'acquisizione e la conservazione di dati biometrici allo scopo di effettuare un riconoscimento facciale, in tempo reale o in differita, il suo utilizzo da parte delle autorità pubbliche costituisce una limitazione all'esercizio dei diritti fondamentali sanciti agli articoli 7 e 8 della Carta dei diritti fondamentali. Conformemente al dettato dell'art. 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà fondamentali ivi riconosciuti possono essere apportate, nel rispetto del principio di proporzionalità, solo laddove risultino necessarie, siano previste dalla legge e rispettino il contenuto essenziale di detti diritti e libertà; condizioni, queste ultime, i cui contenuti sono stati specificati a più riprese nel corso degli anni dalla Corte di giustizia.

Guardando alla giurisprudenza della Corte nell'ottica delle questioni qui affrontate, sembra pertanto opportuno esaminare i precedenti giurisprudenziali concernenti le varie forme di sorveglianza elettronica statale, dal momento che, la *FRT*, nelle sue più temute applicazioni, presuppone una raccolta generalizzata ed indiscriminata di dati, ed in tale ottica ricopre un posto di primo piano nel contesto delle misure di sorveglianza elettronica statale e non. Sul punto un *landmark case* è senz'altro costituito dal noto caso *Digital*

[98] S. NIGER, *Le nuove dimensioni della privacy dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, p. 75.
[99] DE HERT, E. SCHREUDERS, *The Relevance of Convention 108*, in *Proceedings of the Council of Europe Conference on Data Protection*, Varsavia, 19-20 novembre 2001, p. 42.
[100] J. KOKOTT, C. SOBOTTA, *The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law*, 2013, pp. 222-228. Per ulteriori approfondimenti si legga anche, M. TZANOU, *Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a Not So New Right*, in *International Data Privacy Law*, 2013, pp. 88-99.

Rights[101], in cui la Corte ha dichiarato l'invalidità con effetti *ex tunc* della direttiva 2006/24/CE (anche nota come direttiva sulla *data retention*[102]), strumento di diritto derivato che si poneva, da un lato, lo scopo di armonizzare le disposizioni degli Stati membri sulla conservazione di determinati dati relativi al traffico telefonico e, dall'altro, quello di garantire la disponibilità di particolari informazioni a fini di indagine, accertamento e perseguimento di reati gravi, in particolare i reati legati alla criminalità organizzata e al terrorismo; i Giudici, nel seguire l'*iter* logico tipico della Corte EDU, hanno dapprima ravvisato nella direttiva sulla *data retention* un'interferenza con gli articoli 7 e 8 della Carta dei diritti fondamentali[103]e, in secondo luogo, hanno escluso la giustificabilità della stessa. Il complessivo *reasoning* caratterizzante le motivazioni della sentenza è incardinato sui contenuti degli articoli 7 e 8 della Carta e la dichiarazione di invalidità risulta fondata esclusivamente sulla non conformità della direttiva a tali disposizioni[104], per violazione del principio di proporzionalità nel bilanciamento tra diritto alla *privacy* ed esigenze di pubblica sicurezza alla luce del combinato disposto degli articoli 7, 8 e 52, paragrafo 1, della Carta dei diritti fondamentali. Invero, come si è già avuto modo di sottolineare[105], pur riconoscendo che la lotta contro gravi forme di criminalità possa considerarsi indubbiamente un obiettivo d'interesse generale e pur confermando il rispetto, da parte della normativa in scrutinio, dell'essenza del diritto alla *privacy* e di quello alla protezione dei dati personali[106], i giudici hanno concluso per la mancanza di proporzionalità tra le attività poste in essere in virtù della direttiva sulla *data retention* e la necessità e/o appropriatezza delle stesse al fine di raggiungere gli obiettivi ivi prefissati[107]: per dirla con le parole dell'Avvocato generale Cruz Villalòn, richiamate

[101] Corte di giustizia, Grande Sezione, sentenza dell'8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung e altri*, cause riunite C-293/12 e C-594/12.

[102] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, del 15 marzo 2006 in GUUE L 105 del 13 aprile 2006, pp. 54-63.

[103] La conservazione di meri dati di traffico, sebbene non possa rappresentare di per sé un'intrusione consistente nella *privacy* degli individui al pari della conservazione del contenuto delle comunicazioni, comporta in ogni caso dei rischi evidenti. Corte di giustizia, *Digital Rights*, cit., par. 27: "those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships".

[104] "[I]t is the first time an entire Directive was invalidated solely on the basis of its incompatibility with the EU Charter of Fundamental Rights", Garante europeo per la protezione dei dati, *Court of Justice Judges EU Data Retention Directive Invalid*, in *Newsletter* n. 42, 2014, p. 5, disponibile su www.edps.europa.eu.

[105] F. DI MATTEO, *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella direttiva PNR?*, in *Diritti umani e diritto internazionale*, 2017, pp. 213-236, p. 226.

[106] Corte di giustizia, *Digital Rights*, cit., par. 40.

[107] "[T]he ECJ underlined that the Data Retention Directive set up a regime that failed to limit interference with privacy rights 'to what is strictly necessary', suggesting emphatically that, on the contrary, the Data Retention Directive 'entail[ed] an interference with the fundamental rights of practically the entire European population'", F. FABBRINI, *Human Rights in the Digital Age*, cit., p. 80; sulla sentenza, vedi E. GUILD, S. CARRERA, *The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive*, in *CEPS Paper in Liberty and Security in Europe*, 2014, n. 65, pp. 1-15, disponibile su www.ceps.eu; T. KONSTADINIDES, *Mass Surveillance and Data Protection in EU Law: The*

dalla Corte, tale direttiva consentiva interferenze nel diritto alla *privacy* tali da ingenerare negli individui ad esse sottoposti la sensazione che le proprie vite private fossero oggetto di sorveglianza costante[108].

Siffatta conclusione è la medesima cui la Corte è pervenuta nel caso *Tele2 Sverige*[109], in cui i Giudici hanno richiamato costantemente il precedente *Digital Rights*, confermando l'idea di base per la quale le misure di sorveglianza nazionali non possano essere generalizzate ed indiscriminate[110]e che debbano essere sempre accompagnate da una serie di garanzie[111]; nel caso di specie, involgente l'interpretazione di un altro strumento di diritto derivato – segnatamente, dell'art. 15 della direttiva 2002/58/CE[112] – viene statuito che una normativa nazionale di recepimento che consenta l'accesso alle autorità nazionali competenti ai dati conservati nell'ambito della lotta contro la criminalità, senza limitare tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporlo ad un controllo preventivo da parte di un giudice o di un'autorità

Data Retention Directive Saga, in *European Police and Criminal Law Co-Operation. Swedish Studies in European Law*, Oxford, 2014, pp. 69-84; T. OJANEN, *Privacy Is More Than Just a Seven-Letter Word. The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance - Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others*, in *European Constitutional Law Review*, 2014, pp. 528-541.

[108] Corte di giustizia, *Digital Rights*, cit., par. 37.

[109] Corte di giustizia, Grande Sezione, sentenza del 21 dicembre 2016, *Tele2 Sverige AB c. Post-och telestyrelsen e Secretary of State for the Home Department c. Tom Watson e altri*, cause riunite C-203/15 e C-698/15. Per un inquadramento generale del caso, v. L. WOODS, *Data Retention and National Law: the ECJ Ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)*, in *EU Law Analysis*, 21 dicembre 2016, disponibile su www.eulawanalysis.blogspot.it; v. anche, G. NADDEO, *Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella "data retention saga" dinanzi alla Corte di giustizia*, in questa *Rivista*, 2022, n. 2, pp. 188-217, p. 198.

[110] "[A]nche se l'efficacia della lotta contro la criminalità grave, e in particolare contro la criminalità organizzata e il terrorismo, può dipendere in larga misura dall'utilizzo delle moderne tecniche di indagine, un siffatto obiettivo di interesse generale, per quanto fondamentale esso sia, non vale di per sé solo a giustificare che una normativa nazionale che prevede la conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione venga considerata necessaria ai fini della lotta suddetta (v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza Digital Rights, punto 51)", Corte di giustizia, *Tele 2 e Watson*, cit., par. 103.

[111] "Per contro, l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, non osta a che uno Stato membro adotti una normativa la quale consenta, a titolo preventivo, la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione, per finalità di lotta contro la criminalità grave, a condizione che la conservazione dei dati sia, per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista, limitata allo stretto necessario[…]. la suddetta normativa nazionale deve, in primo luogo, prevedere norme chiare e precise che disciplinino la portata e l'applicazione di una siffatta misura di conservazione dei dati e fissino un minimo di requisiti, […] deve in particolare indicare in quali circostanze e a quali condizioni una misura di conservazione dei dati può, a titolo preventivo, essere adottata, garantendo così che una misura siffatta sia limitata allo stretto necessario […] se certo tali condizioni possono variare in funzione delle misure adottate ai fini della prevenzione, della ricerca, dell'accertamento e del perseguimento della criminalità grave, la conservazione dei dati deve comunque rispondere sempre a criteri oggettivi, istituendo un rapporto tra i dati da conservare e l'obiettivo perseguito. In particolare, tali condizioni devono risultare, in pratica, idonee a delimitare effettivamente la portata della misura e, di conseguenza, il pubblico interessato", Corte di giustizia, *Tele 2 e Watson*, cit., parr. 108-110.

[112] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, del 12 luglio 2002, in GUUE L 201 del 31 luglio 2002, pp. 37-47;

amministrativa indipendente, e senza esigere che i dati personali raccolti vengano conservati nel territorio dell'Unione, viola gli articoli 7 e 8 della Carta dei diritti fondamentali, in combinato disposto con l'art. 52, paragrafo 1. Peraltro, in punto di controllo demandato alle autorità garanti nazionali *ex* art. 8 della Carta, già a seguito della prima sentenza *Schrems*[113], la Corte ha chiarito che ogni normativa che contempli, *inter alia*, il trasferimento di dati personali a Stati terzi, deve garantire l'effettività di tale controllo senza limiti territoriali. I giudici, pur riconoscendo che la formulazione letterale dell'articolo 28, paragrafi 1 e 6, della direttiva 95/46/CE, potesse condurre l'interprete a considerare i poteri delle autorità garanti limitati al confine dei rispettivi Stati membri[114], hanno voluto sottolineare come, tanto l'articolo 8 della Carta, quanto l'articolo 28 della direttiva 95/46/CE − strumento oggi superato, come si è visto, dal nuovo regolamento n. 679/2916 − non escludano dalla sfera di competenza delle autorità indipendenti il controllo del trasferimento di dati personali a Paesi terzi, neanche se questi ultimi siano stati oggetto di una decisione della Commissione ai sensi dell'articolo 25, paragrafo 6, della direttiva 95/46/CE[115].

Senonché, è stato evidenziato[116] come, questo orientamento garantista, inaugurato da *Digital Rights*, confermato in *Tele2 Sverige*, e a cui vanno ricondotte anche le note pronunce *Schrems I* e *Schrems II*[117], abbia subito un'inversione di rotta verso

[113] Corte di giustizia, Grande Sezione, sentenza del 6 ottobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, causa C-362/14. Si tratta del noto caso in cui un cittadino austriaco, Maximiliam Schrems, ha presentato una denuncia presso l'autorità irlandese per la protezione dei dati, ritenendo che i suoi dati personali − così come quelli di tutti gli altri cittadini dell'Unione iscritti a *Facebook* − una volta trasferiti dalla filiale irlandese di *Facebook* a *server* statunitensi del noto *social network*, non fossero adeguatamente protetti; ciò, alla luce delle rilevazioni fatte nel 2013 dall'ex analista della CIA, Edward Snowden, relativamente alle attività di *intelligence* negli Stati Uniti. L'autorità garante irlandese ha respinto detta denuncia sulla base dell'esistenza di una decisione del 26 luglio 2000 della Commissione che − nel contesto del regime *Safe Harbour* − aveva stabilito l'adeguatezza del livello di protezione dei dati personali negli Stati Uniti. Per approfondimenti, vedasi F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal Safe Harbour al Privacy Shield)*, in *Rivista di Diritto internazionale*, 2016, p. 690-724; A. GIATTINI, *La tutela dei dati personali davanti alla Corte di giustizia dell'UE: il caso Schrems e l'invalidità del sistema di 'approdo sicuro'*, in *Diritti umani e diritto internazionale*, 2016, n. 1, pp. 247-254; C. KUNER, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, in *German Law Journal*, 2017, pp. 881-918 ss.; M. NINO, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, in *Il Diritto dell'Unione Europea*, 2021, n. 1, pp. 93-124.

[114] Corte di giustizia, *Maximillian Schrems*, cit., par. 44.

[115] "On the contrary, Article 28 of Directive 95/46 applies, by its very nature, to any processing of personal data. Thus, even if the Commission has adopted a decision pursuant to Article 25(6) of that directive […] if that were not so, persons whose personal data has been or could be transferred to the third country concerned would be denied the right, guaranteed by Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim for the purpose of protecting their fundamental rights", Corte di giustizia, *Maximillian Schrems*, cit., parr. 57-58.

[116] M. NINO, *La normalizzazione della sorveglianza di massa nella prassi giurisprudenziale delle Corti di Strasburgo e Lussemburgo: verso il cambio di paradigma del rapporto privacy v. security*, in questa *Rivista*, 2022, n. 3, pp. 105-133, pp. 125-129; M. NINO, *La disciplina internazionale ed europea della data retention*, cit., p. 94 ss.

[117] Della prima pronuncia, che ha invalidato il regime del cd. *Safe Harbour*, si è detto *supra*. Con la seconda sentenza è stato invalidato il regime del cd. *Privacy Shield*: Corte di giustizia, Grande Sezione, sentenza del 16 luglio 2020, *Data Protection Commissioner c. Facebook Ireland Limited e Maximillian Schrems*, causa C-311/18. Entrambi i regimi − che costituivano le basi giuridiche per la trasmissione di dati tra

l'affermazione della compatibilità della raccolta generalizzata ed indiscriminata di dati personali con il diritto dell'Unione europea: il riferimento è ai casi *Privacy International*[118] e *La Quadrature du Net*[119], sorti da questioni pregiudiziali relative, ancora una volta, all'interpretazione dell'art. 15 della direttiva 2002/58/CE.

Guardando al primo dei precedenti sopra menzionati, in cui la Corte di giustizia ha ampiamente ribadito i *dicta* contenuti in *Digital Rights*, sembra in effetti già possibile intravedere una mutata percezione della tecnica di raccolta di dati personali in massa. Secondo il Giudice di Lussemburgo, una normativa, quale quella in contestazione, che consenta all'autorità nazionale competente di imporre ai fornitori di servizi di comunicazione elettronica la trasmissione, ai servizi di sicurezza e di *intelligence*, di tutti i dati relativi al traffico e all'ubicazione raccolti in via generalizzata e indifferenziata, costituisce una sicura ingerenza nel diritto alla riservatezza, peraltro di grave entità, perché "può ingenerare nelle persone interessate la sensazione che la loro vita privata costituisca l'oggetto di una sorveglianza continua"[120] e perché "ha l'effetto di trasformare in regola la deroga all'obbligo del principio di garantire la riservatezza dei dati, mentre il sistema istituito dalla direttiva 2002/58 richiede che tale deroga resti l'eccezione"[121]. Tuttavia, all'atto di valutare la giustificabilità dell'ingerenza, effettivamente la Corte sembra dare per acquisita la possibilità che il diritto interno di uno Stato membro possa consentire la raccolta indiscriminata e generalizzata di dati personali a fini di sicurezza nazionale, materia di esclusiva competenza di ciascuno Stato membro, anche a mente dell'articolo 4, paragrafo 2, TUE[122]. Nel caso di specie, la normativa nazionale,

---

Unione europea e Stati Uniti, e consentivano una raccolta in blocco di dati personali – sono stati ritenuti dalla Corte non conformi alla normativa europea di riferimento. M. MASTRACCI, *Evoluzione del diritto alla privacy tra Europa e Stati Uniti: dal Safe Harbor al Privacy Shield*, in *La Comunità internazionale*, 2016, pp. 555-579; M. NINO, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 2020, n. 3, pp. 733-759; G. CAGGIANO, *Sul trasferimento internazionale dei dati personali degli utenti del Mercato unico digitale all'indomani della sentenza "Schrems II" della Corte di giustizia*, in *Studi sull'integrazione europea*, 2020, n. 3, pp. 563-585.

[118] Corte di giustizia, Grande Sezione, sentenza del 6 ottobre 2020, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e altri*, causa C-623/17. La domanda è stata proposta nell'ambito di una controversia che vede la *Privacy International* contrapposta al governo britannico in ordine alla legittimità della normativa statale che autorizza l'acquisizione e l'utilizzo da parte dei servizi di *intelligence* di dati di comunicazione in massa. La Corte conclude, per quanto qui interessa, che "l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce dell'articolo 4, paragrafo 2, TUE nonché degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, dev'essere interpretato nel senso che osta ad una normativa nazionale che consente a un'autorità statale di imporre ai fornitori di servizi di comunicazione elettronica, ai fini della salvaguardia della sicurezza nazionale, la trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence", Corte di giustizia, Grande Sezione, *Privacy International*, cit., par. 82.

[119] Corte di giustizia, Grande Sezione, sentenza del 6 ottobre 2020, *La Quadrature du Net e altri c. Premier ministre e altri*, cause riunite C-511/18, C-512/18 e C520/18. Si tratta di una serie di cause instaurate da alcune organizzazioni di categoria francesi e belghe contro i rispettivi governi nazionali, giunte alla Corte sotto forma di domande di pronuncia pregiudiziale concernenti, *inter alia*, la compatibilità delle normative statali sulla raccolta e conservazione in blocco dei dati personali degli utenti di servizi di comunicazione, con l'articolo 15, paragrafo 1, della direttiva 2002/58/CE.

[120] Corte di giustizia, Grande Sezione, *Privacy International*, cit., par. 71.

[121] Ivi, par. 69.

[122] Ivi, par. 74.

nell'imporre ai fornitori di servizi di comunicazione elettronica di procedere alla trasmissione generalizzata e indifferenziata di dati relativi al traffico e all'ubicazione ai servizi di sicurezza e di *intelligence*, istituiva una facoltà di "accesso generale" da parte di questi ultimi a tali dati, ed è sulla base di tale specifico aspetto che la stessa è stata censurata come eccedente i limiti dello stretto necessario (e non per la presupposta raccolta di dati personali in massa)[123].

In *La Quadrature du Net* viene statuito in modo espresso quanto tra le righe era già emerso dalle motivazioni della sentenza relativa al caso *Privacy International*. Dapprima viene chiarito che l'articolo 15, paragrafo 1, della direttiva 2002/58, se correttamente interpretato alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, osta a misure legislative che prevedono la conservazione generalizzata e indifferenziata di dati relativi al traffico e all'ubicazione *a titolo preventivo*[124], anche laddove tale raccolta avvenga nel perseguimento dei fini di cui al medesimo art. 15, paragrafo 1[125]. Tuttavia, subito dopo viene affermata – questa volta senza mezzi termini – la compatibilità con la Carta di una misura legislativa che preveda la possibilità di ingiungere *hic et nunc* ai fornitori di servizi di comunicazione elettronica la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, ove lo Stato membro interessato stia affrontando una minaccia per la sicurezza nazionale "reale e attuale o prevedibile"[126]; tale ingiunzione dovrà essere oggetto di un controllo effettivo da parte di un giudice o di un organo amministrativo indipendente, diretto ad

[123] "[P]er quanto riguarda l'accesso di un'autorità a dati personali, una normativa non può limitarsi ad esigere che l'accesso ai dati da parte delle autorità risponda alla finalità perseguita da tale normativa, ma essa deve altresì prevedere le condizioni sostanziali e procedurali che disciplinano tale utilizzo […]. Tali requisiti si applicano, a fortiori, ad una misura legislativa, come quella controversa nel procedimento principale, sul fondamento della quale l'autorità nazionale competente può imporre ai fornitori di servizi di comunicazione elettronica di procedere alla comunicazione mediante trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence […]. Tenuto conto del fatto che la trasmissione di tali dati alle autorità pubbliche equivale, conformemente a quanto è stato constatato al punto 79 della presente sentenza, ad un accesso, si deve ritenere che una normativa che consente una trasmissione generalizzata e indifferenziata dei dati alle autorità pubbliche implichi un accesso generale. Ne consegue che una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica di procedere alla comunicazione mediante trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence eccede i limiti dello stretto necessario e non può essere considerata giustificata in una società democratica", ivi, parr. 77 e 79-81.

[124] Corte di giustizia, Grande Sezione, *La Quadrature du Net*, cit., par. 168.

[125] Art. 15, Direttiva 2002/58/CE, cit.: "Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva [95/46], una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica, e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto [dell'Unione], compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea.

[126] *Ibidem*.

accertare l'esistenza della minaccia attuale o prevedibile, e dovranno essere previste le necessarie salvaguardie[127].

Eccezion fatta per l'ipotesi della minaccia grave ed imminente alla sicurezza nazionale, *de residuo* la conservazione dei dati relativi al traffico e all'ubicazione, per i fini di cui all'art. 15, par. 1, della Direttiva, sarebbe consentita solo se *mirata*: deve essere "delimitata" sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, eventualmente rinnovabile[128]. Seguono, poi, considerazioni ulteriori per talune tipologie di dati, ritenute evidentemente meno delicate rispetto alla categoria di quelli relativi al traffico e all'ubicazione, quali gli indirizzi IP attribuiti all'origine di una connessione e le informazioni sull'identità civile degli utenti di mezzi di comunicazione elettronica, per i quali la Corte ritiene consentita la conservazione generalizzata e indifferenziata nel perseguimento dei fini di cui all'art. 15, paragrafo 1 della Direttiva; ciò, purché tale conservazione risulti, in base a disposizioni legislative chiare, subordinata al rispetto di condizioni sostanziali e procedurali – locuzione di cui è stata criticata la vaghezza[129], ma che si ritiene debba rappresentare un rinvio ai requisiti della misura di sorveglianza 'giustificabile' annosamente ribaditi dalla Corte nei propri precedenti sul tema (condizioni che, comunque, sono rinvenibili nel Regolamento generale sulla protezione dei dati personali[130]), comprese le necessarie ed effettive garanzie contro il rischio di abusi.

L'idea che possa concedersi una maggiore o minore apertura alla raccolta sistematica di dati personali quale strumento di contrasto alla criminalità 'a seconda della specifica tipologia di dato raccolto' sembra emergere anche nel recentissimo rinvio pregiudiziale *V.S. c. Ministerstvo na vatreshnite raboti e altri*[131], dove la Corte ha chiarito come le norme della Direttiva Polizia ostino a una normativa nazionale che preveda la raccolta sistematica di dati biometrici e genetici – persino di chi è formalmente accusato di aver commesso un reato doloso, perseguibile d'ufficio nello Stato Membro – ai fini della loro registrazione, senza prevedere l'obbligo, per l'autorità competente, di verificare e di dimostrare, da un lato, che tale raccolta è strettamente necessaria per il raggiungimento dei concreti obiettivi perseguiti e, dall'altro, che tali obiettivi non possano essere raggiunti mediante misure meno invasive in punto di ingerenza nei diritti fondamentali della persona interessata.

Ciò posto, si ritiene che le riepilogate statuizioni circa la giustificabilità, *ex* art. 52, paragrafo 1, della Carta, delle limitazioni del diritto fondamentale alla *privacy*, nei casi

[127] *Ibidem*. A detta della Corte, tale ingiunzione deve essere emessa per un periodo temporalmente limitato allo stretto necessario, ma essa è rinnovabile in caso di persistenza della minaccia.
[128] Corte di giustizia, Grande Sezione, *La Quadrature du Net*, cit., par. 168.
[129] M. NINO, *La normalizzazione della sorveglianza di massa nella prassi giurisprudenziale delle Corti*, cit., p. 127.
[130] Per le condizioni che devono ricorrere, e i principi che devono essere rispettati, affinché qualsiasi trattamento di dati personali possa ritenersi lecito, a più forte ragione se di tipo 'sensibile' come nel caso dei dati biometrici, v. *infra* pp. 15-17. Per inciso, anche la Convenzione n. 108, che obbliga tutti gli Stati membri dell'Unione europea, impone una serie di requisiti da rispettare, si veda ancora *infra* p. 9-10,
[131] Corte di giustizia, *V.S. c. Ministerstvo na vatreshnite raboti e altri*, cit.

riguardanti le misure di sorveglianza statale, risulteranno preziose per la nuova generazione di procedimenti, di cui si prevede l'instaurazione innanzi la Corte di Giustizia (e la Corte EDU), concernenti l'uso di tecnologie ancora più sofisticate a fini di sorveglianza: mentre sinora i casi di sorveglianza "tradizionali" hanno riguardato principalmente l'intercettazione e l'analisi delle comunicazioni e dei metadati, questa nuova generazione non mancherà di riguardare l'uso, da parte degli Stati, delle tecnologie di riconoscimento facciale al fine di monitorare la propria popolazione e individuare più facilmente terroristi e altri criminali[132]. In tale prospettiva i suesposti *dicta* consentono di cogliere in anticipo le potenziali criticità di qualsiasi normativa che aspiri ad autorizzare e regolare l'utilizzo della *facial recognition technology*; limitando il diritto fondamentale alla *privacy*, essa sarà soggetta al test di necessità e proporzionalità della Corte di giustizia alla luce del diritto primario, ed in particolare alla luce della Carta dei diritti fondamentali, come dimostrato dalla giurisprudenza appena esaminata: difatti, ove tale normativa rivestisse la natura di diritto interno, vi soggiacerà per ovvie ragioni di primato; ove invece si trattasse di diritto secondario, la Carta dei diritti fondamentali ne costituirebbe comunque parametro di validità ed interpretazione.

6. (segue)… e a quelli dell'articolo 8 della Convenzione europea dei diritti dell'uomo, quale diritto "corrispondente"

Dopo aver esaminato i contenuti degli articoli 7 e 8 della Carta dei diritti fondamentali alla luce dell'interpretazione che di essi è stata data dalla Corte di giustizia nei precedenti giurisprudenziali riguardanti le misure di sorveglianza elettronica, sembra pertinente far cenno, nella medesima ottica, ai contenuti dell'art. 8 della Convenzione europea dei diritti dell'uomo, quale diritto corrispondente ai sensi dell'art. 52, paragrafo 3, della Carta.

Come anticipato il diritto alla *privacy* non è un diritto assoluto, esso può essere limitato, a determinate condizioni; nel secondo paragrafo dell'art. 8 CEDU vengono introdotte le condizioni in presenza delle quali la pretesa illegittimità di una data ingerenza da parte dell'autorità pubblica[133] nella *privacy* dell'individuo (*rectius*, dell'individuo e/o della persona giuridica[134]) potrebbe essere esclusa: sicurezza nazionale,

[132] T. CHRISTAKIS, K. BOUSLIMANI, *National Security, Surveillance and Human Rights*, cit., p. 715.

[133] A differenza del dettato dell'art. 17 del Patto sui diritti civili e politici del 1966, il secondo paragrafo dell'art. 8 CEDU si riferisce esclusivamente all'autorità pubblica. Ciò ha sollevato dubbi circa l'interpretazione di detta disposizione. Ci si è chiesti se essa tuteli le sole ingerenze nella *privacy* riconducibili ad autorità pubbliche, o se invece la norma attribuisca alle sole autorità pubbliche la possibilità di interferire 'legittimamente' nella *privacy*, e mai a soggetti non qualificabili come tali. Vedasi J. DE MEYER, *The Right to Respect for Private and Family Life, Home and Communications between Individuals and the Resulting Obligations for States parties to the Convention*, in A.H. ROBERTSON (ed.), *Privacy and Human Rights. Papers by Experts on an Issue of Growing Importance Given Under the Auspices of the European Convention on Human Rights*, Manchester, 1973, pp. 263-275.

[134] "If juridical persons are entitled to a name or reputation and honour why should they not be able to rely on certain aspects of the right to respect for private life? [...] It has also been doubted whether the right to respect for the home can be relied on by judicial persons. […] a building in which a trading company has its registered office, its management and its offices is considered its home […] similarly, in my opinion

pubblica sicurezza, benessere economico del Paese, difesa dell'ordine e prevenzione dei reati, protezione della salute o della morale, protezione dei diritti e delle libertà altrui. La pronuncia su di una domanda ai sensi dell'art. 8 CEDU impone pertanto una verifica su due livelli: il primo attiene all'applicabilità dell'art. 8, para. 1 CEDU, dovendosi stabilire se il diritto di cui il ricorrente postula una lesione sia tutelato dalla Convenzione; il secondo livello attiene all'accertamento, in concreto, della violazione del diritto individuale da parte dello Stato, secondo i parametri di cui all'art. 8, para. 2 della stessa. Alla luce della consolidata giurisprudenza europea sul tema, a prescindere dall'obbligo negativo o positivo violato e dal margine di apprezzamento riconosciuto allo Stato parte nel caso specifico, esso risulterà in ogni caso responsabile di una violazione dell'art. 8 CEDU laddove l'ingerenza, una volta riconosciuta come afferente alla nozione di vita privata e familiare, non fosse prevista dalla legge ("*in accordance with the law")*, o fosse prevista ma non perseguisse alcuno scopo lecito ("*legitimate aim")*, oppure ancora fosse prevista da una legge, sorretta da uno scopo lecito, ma non fosse necessaria rispetto all'obbiettivo che si prefiggeva di raggiungere ("*necessary in a democratic society"*).

Fatta questa premessa, ai nostri fini occorre precisare come la Corte EDU si sia occupata a più riprese di casi riguardanti la raccolta o la conservazione di dati biometrici:

judicial persons may rely on the right to respect for their correspondence", J. VELU, *The European Convention on Human Rights and the Right to Respect for Private Life, the Home and Communications*, in A. H. ROBERTSON (ed.), *Privacy and Human Rights*, cit., pp. 19-20. Per quanto concerne i titolari del diritto riconosciuto dall'art. 8 CEDU, va detto che, oltre agli individui, si è per anni dibattuto in dottrina se potessero rientrarvi o meno anche le persone giuridiche. Potendosi forse, da un lato, escludere queste ultime dalla titolarità del diritto alla vita familiare − la cui natura sembrerebbe strettamente individuale − dall'altro lato non poteva aversi il medesimo grado di certezza rispetto ad altre sfumature ricomprese nel più generale diritto alla *privacy*, ad esempio la tutela della riservatezza del domicilio o della corrispondenza. A tutt'oggi, non è stata data chiara risposta. Tuttavia, pare condivisibile sostenere l'esistenza di "un approccio di tipo 'relativista' riguardo alla titolarità del diritto alla *privacy* da parte delle persone giuridiche, un approccio che faccia riferimento, cioè, alla nozione di *privacy* di volta in volta rilevante (vita privata, familiare, domicilio o corrispondenza) e che tenga in considerazione le circostanze del caso concreto", M.E. BONFANTI, *Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti*, in *Diritti umani e diritto internazionale*, 2011, n. 3, pp. 437-481, p. 439.

dai campioni cellulari[135] ai profili di DNA[136], dalle impronte digitali[137]a quelle palmari[138], dai campioni vocali[139]. Le pronunce maggiormente pregnanti per il tema che ci occupa sono però quelle relative alla sorveglianza elettronica statale. Infatti, la preoccupazione maggiormente esternata con riferimento alla *facial recognition technology* concerne non tanto le sue applicazioni commerciali più banali, ed ormai capillarmente diffuse − come l'utilizzo della stessa per accedere ai propri dispositivi elettronici o ai servizi della banca multicanale, per le quali resta comunque valida la verifica della legittimità dell'ingerenza nei termini suesposti – quanto piuttosto la possibilità di un suo utilizzo indiscriminato da parte delle forze dell'ordine nazionali (anche alla luce del rischio di *function creep* di cui si è detto[140]); non sfugge ai più che la *FRT* costituirà una modalità, tecnologicamente più avanzata, di contrasto alle attività criminose, aggiuntiva rispetto alle tecniche tradizionali, quali le intercettazioni telefoniche o postali, di cui la Corte EDU si è già ampiamente occupata, costruendo, nel corso degli anni, un apparato di principi che può (e sarà) esteso alle nuove fattispecie involgenti l'utilizzo delle tecniche di riconoscimento facciale.

Già nello storico precedente *Klass e altri c. Germania*[141] il difficile bilanciamento da operare rispetto alle caratteristiche dell'ingerenza 'giusta' − quelle del *prescribed by law*,

[135] Corte europea dei diritti dell'uomo, decisione del 7 dicembre 2006, ricorso n. 29514/05, *Van der Velden c. Paesi Bassi*; decisione del 5 gennaio 2006, ricorso n. 32352/02, *Schmidt c. Germania*; Grande Camera, sentenza del 4 dicembre 2008, ricorsi nn. 30562/04 e 30566/04, *S. e Marper c. Regno Unito*; sentenza del 2 giugno 2015, ricorso n. 22037/13, *Canonne c. Francia*; sentenza del 15 maggio 2018, ricorso n. 41079/16, *Caruana c. Malta*; sentenza del 13 febbraio 2020, ricorsi nn. 53205/13 e 63320/13, *Trajkovski e Chipovski c. Macedonia del Nord*; sentenza del 16 giugno 2020, ricorso n. 47443/14, *Boljević c. Serbia*.

[136] Corte europea dei diritti dell'uomo, *Van der Velden c. Paesi Bassi*, cit.; *Schmidt c. Germania*, cit.; Grande Camera, S. *e Marper c. Regno Unito*, cit.; decisione del 20 gennaio 2009, ricorso n. 20689/08, *W. c. Paesi Bassi*; sentenza del 4 giugno 2013, ricorsi nn. 7841/08 e 57900/12, *Peruzzo e Martens c. Germania*; Quinta Sezione, *Canonne c. Francia*, cit.; sentenza del 22 giugno 2017, ricorso n. 8806/12, *Aycaguer c. Francia*; sentenza del 29 gennaio 2019, ricorso n. 62257/15, *Mifsud c. Malta*; sentenza del 13 giugno 2020, ricorso n. 45245/15, *Gaughran c. Regno Unito*; *Trajkovski e Chipovski c. Macedonia del Nord*, cit.; sentenza del 14 aprile 2020, ricorso n. 75229/10, *Dragan Petrović c. Serbia*.

[137] Corte europea dei diritti dell'uomo, Grande Camera, *S. e Marper c. Regno Unito*, cit.; sentenza del 10 febbraio 2011, ricorso n. 11379/03, *Dimitrov-Kazakov c. Bulgaria*; sentenza del 18 aprile 2013, ricorso n. 19522/09, *M.K. c. Francia*; sentenza del 19 giugno 2018, ricorso n. 8630/11, *Suprunenko c. Russia*; *Gaughran c. Regno Unito*, cit.; sentenza dell'11 giugno 2020, ricorso n. 74440/17, *P.N. c. Germania*; sentenza del 9 novembre 2021, ricorso n. 57294/16, *Willems c. Paesi Bassi*.

[138] Corte europea dei diritti dell'uomo, *P.N. c. Germania*, cit.

[139] Corte europea dei diritti dell'uomo, sentenza del 25 settembre 2001, ricorso n. 44787/98, *P.G. e J.H. c. Regno Unito*; sentenza del 5 novembre 2002, ricorso n. 48539/99, *Allan c. Regno Unito*; sentenza del 27 aprile 2004, ricorso n. 50210/99, *Doerga c. Paesi Bassi*; sentenza del 31 maggio 2005, ricorso n. 59842/00, *Vetter c. Francia*; sentenza del 20 dicembre 2005, ricorso n. 71611/01, *Wisse c. Francia*.

[140] V. *infra* nota n. 75.

[141] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 6 settembre 1978, ricorso n. 5029/71, *Klass e altri c. Germania*. È il caso di cinque ricorrenti di nazionalità tedesca − un ministro della giustizia, tre avvocati ed un giudice – i quali hanno sostenuto che l'art. 2 della legge fondamentale tedesca (*Grundgesetz*), nonché uno statuto adottato ai sensi di detta legge, vale a dire l'atto del 13 agosto 1968 sulle restrizioni alla segretezza della posta e delle telecomunicazioni (*Gesetz zur Beschränkung des Brief-Post- under Fernmeldegeheimnisses*, in appresso denominato "il G10"), erano contrarie agli articoli 8, 13 e 6 della Convenzione. In particolare, gli *applicants* non contestavano che la Germania avesse diritto a ricorrere alle misure di sorveglianza contemplate dalle menzionate disposizioni, bensì avversavano questa normativa in quanto consentiva che tali misure potessero essere adottate dalle autorità senza obbligo di informare le persone interessate dopo l'evento, evitando inoltre di predisporre un rimedio contro l'ordine e l'esecuzione di tali misure innanzi all'autorità giudiziaria.

del *legitimate aim* e del *necessery in a democratic society* – si era palesato in tutta la sua intrinseca delicatezza. In quella sede la Corte fu chiamata a valutare se una serie di misure di sorveglianza, previste dalla legge e finalizzate ad intensificare la tutela della sicurezza collettiva e dell'ordine pubblico in Germania, potessero ritenersi necessarie in una società democratica. Nel precedente in discorso, la Corte ha rilevato, *inter alia*, che la normativa attenzionata imponeva una serie di condizioni al cui ricorrere era subordinata la possibilità di adottare le misure di sorveglianza, escludendo il rischio di una sorveglianza generalizzata o comunque 'esplorativa'. Ad esempio, le stesse dovevano essere confinate alle ipotesi di individui per i quali vi erano indicazioni chiare circa l'aver pianificato la commissione, l'aver commesso o lo stare commettendo, determinati gravi reati e, soprattutto, dovevano costituire l'*extrema ratio*, lo strumento cui ricorrere quando non vi era altro metodo investigativo sufficiente ad ottenere l'accertamento dei fatti. Non solo, pur non prevedendo la presenza di un controllo giudiziale – che pure la Corte sottolinea essere sempre il più auspicabile – la legislazione in esame prevedeva dei controlli ad opera di soggetti indipendenti rispetto a chi effettuava la sorveglianza, in grado di poterne assicurare un sufficiente grado di imparzialità[142]. A ciò si aggiungevano altri positivi aspetti, che ad oggi possono senz'altro considerarsi principi fondamentali in materia di *data protection*, come la conservazione dei dati personali per un periodo limitato, e comunque non oltre quanto necessario al perseguimento degli scopi prefissati[143].

Klass e altri c. Germania rappresenta una vera e propria pietra miliare nel panorama giurisprudenziale relativo alle misure che possono condurre ad uno stato di sorveglianza, perché oltre a fungere da ragguardevole esempio della dialettica logico-giuridica sopra descritta – *id est*, la valutazione delle caratteristiche del caso concreto, quali la natura, la portata e la durata delle misure di sorveglianza previste, i motivi necessari all'adozione di tali misure, le autorità competenti a consentirle, eseguirle e a sorvegliarne l'esecuzione e il tipo di rimedio previsto dalla legge nazionale – esso si conclude con il rigetto delle doglianze dei ricorrenti e, quindi, ai nostri fini, con una attenta disquisizione sui requisiti che una misura di sorveglianza statale deve possedere per non incorrere nella violazione dell'art. 8 CEDU.

Diversamente in *Malone c. Regno Unito*[144] la Corte ha accolto le doglianze del ricorrente, riscontrando una violazione dell'art. 8 sulla base della carenza del requisito del *prescribed by law*, almeno per quanto concerne una delle due misure di sorveglianza denunziate da James Malone, quella delle intercettazioni postali e telefoniche cui era stato sottoposto. Nel caso di specie, infatti, pur essendo presente nell'ordinamento giuridico di

[142] Ivi, parr. 54 e 56.
[143] Ivi, par. 52.
[144] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 2 agosto 1984, ricorso n. 8691/79, *Malone c. Regno Unito*. James Malone, antiquario di nazionalità inglese, era sospettato di ricettazione e, conformemente alla legislazione in vigore sul punto in Inghilterra e nel Galles, era stato sottoposto ad intercettazione (telefonica e postale) dalle autorità di polizia inglesi. Egli fu altresì sottoposto alla pratica del 'metering', *id est* i numeri chiamati dal ricorrente, la durata delle sue telefonate ed il momento in cui le stesse erano state effettuate, venivano registrate da un apposito macchinario in grado di raccogliere e stampare i predetti dati.

Galles e Inghilterra una apposita ed articolata regolamentazione relativa alle intercettazioni delle comunicazioni, predisposta ai fini generali della prevenzione dei reati, la medesima, secondo la Corte, si caratterizzava per essere «*somewhat obscure and open to differing interpretations*»[145]. Il giudice di Strasburgo ha colto allora l'occasione per definire i contorni del requisito *in accordance with law* dell'ingerenza legittima con il diritto alla *privacy*, che non implica la mera esistenza di una previsione legislativa nell'ordinamento interno dello Stato parte, necessitando altresì di una positiva valutazione circa la 'qualità' della stessa; ed infatti, nonostante vi fosse consenso sul fatto che la finalità perseguita dall'interferenza in esame − la prevenzione e/o la scoperta di un reato − fosse legittima, oltre che necessaria in una società democratica, il Giudice europeo ritenne di poter in ogni caso ravvisare una violazione dell'art. 8 CEDU[146]. Detto precedente rappresenta un'ulteriore dimostrazione del difficile bilanciamento da operare rispetto alle caratteristiche dell'ingerenza 'giusta' cui si è fatto cenno, posto che anche quando sembrano astrattamente presenti tutti gli elementi necessari a configurare la scriminante *ex* art. 8, para. 2, CEDU, un'attenta disamina del caso concreto potrebbe comunque condurre la Corte a riscontrare l'avvenuta violazione dell'art. 8, magari a causa della scarsa chiarezza della legge, o per la mancata predisposizione di procedure garantiste tramite le quali l'individuo sottoposto alle misure di sorveglianza è posto in condizione di chiedere conto delle stesse allo Stato autore. Considerazioni, quest'ultime,

[145] Ivi, par. 79.

[146] Ciò in quanto, stando alle prove acquisite, non si era riuscito a distinguere "with any reasonable certainty what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive[…].To that extent, the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking", *ibidem*.

che sono state ribadite in *Huvig*[147]e in *Kruslin*[148], e poi perfezionate in *AEIH e Ekimdzhien c. Bulgaria*[149], *Weber e Saravia c. Germania*[150]e *Liberty e altri c. Regno Unito*[151].

A seguito del caso *datagate*[152], mentre l'opinione pubblica iniziava ad avere sempre maggiore consapevolezza circa l'attività di sorveglianza elettronica attuata dagli Stati, sia di tipo domestico che transfrontaliero, i giudici di Strasburgo hanno iniziato a porre maggior rilievo sulle procedure garantiste[153]che ogni misura di sorveglianza – anche segreta − deve rispettare, affinché possano scongiurarsi eventuali abusi da parte dei governi: la fase dell'autorizzazione della misura di controllo, la supervisione imparziale della sua applicazione, nonché l'effettività dei rimedi offerti al cittadino per contestarla (se in una fase iniziale dell'attività investigativa la misura deve giocoforza essere disposta all'insaputa dell'individuo attenzionato, una volta cessata è altresì necessario che lo stesso venga informato di essere stato attinto da una misura di controllo affinché possa

[147] Corte europea dei diritti dell'uomo, sentenza del 24 aprile 1990, ricorso n. 11105/84, *Huvig c. Francia*, parr 34-35: "Above all, the system does not for the time being afford adequate safeguards against various possible abuses. For example, the categories of people liable to have their telephones tapped by judicial order and the nature of the offences which may give rise to such an order are nowhere defined. Nothing obliges a judge to set a limit on the duration of telephone tapping. Similarly unspecified are the procedure for drawing up the summary reports containing intercepted conversations […]; the circumstances in which recordings may or must be erased or the tapes be destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court[…]. In short, French law, written and unwritten, does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities".

[148] Corte europea dei diritti dell'uomo, sentenza del 24 aprile 1990, ricorso n. 11801/85, K*ruslin c. Francia*, parr. 35-36.

[149] Corte europea dei diritti dell'uomo, sentenza del 28 giugno 2007, ricorso n. 62540/00, *AEIH e Ekimdzhien c. Bulgaria*, parr. 75 e 77: "[i]n the context of covert measures of surveillance, the law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence […]. In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated […]. The Court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case".

[150] Corte europea dei diritti dell'uomo, Terza Sezione, decisione del 29 giugno 2006, ricorso n. 54934/00, *Weber e Saravia c. Germania*, par. 95. Si tratta del noto precedente in cui la Corte, nell'esaminare la legislazione tedesca in materia di *strategic monitoring*, ha definito i cd. sei criteri minimi di salvaguardia per determinare la legittimità o meno di una misura di sorveglianza: 1) l'indicazione della natura dei reati che possono dar luogo all'ordine di intercettazione; 2) la definizione delle categorie di persone che possono essere sottoposte ad intercettazione; 3) l'indicazione di un limite massimo di durata della misura; 4) la procedura da seguire per l'elaborazione e la conservazione dei dati ottenuti; 5) le precauzioni da adottare nel trasferimento dei dati; 6) le circostanze in cui le registrazioni possono – o devono – essere cancellate.

[151] Corte europea dei diritti dell'uomo, Quarta Sezione, sentenza del 1° luglio 2008, ricorso n. 58243/00, *Liberty e altri c. Regno Unito*.

[152] Si veda *supra* nota 20.

[153] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 4 dicembre 2015, ricorso n. 47143/06, *Zakharov c. Russia*, par. 232. Si tratta del ricorso presentato da un cittadino russo, caporedattore di una rivista di aviazione, il quale lamentava una violazione dell'articolo 8 CEDU per via del fatto che il diritto interno russo richiedesse agli operatori di rete mobile di installare apparecchiature che permettevano ai servizi di sicurezza nazionale di intercettare la totalità delle comunicazioni telefoniche senza preventiva autorizzazione giudiziaria e senza peraltro che gli individui avessero alcuna forma di rimedio successivo.

effettivamente beneficiare del rimedio giurisdizionale che lo Stato è tenuto a predisporre[154]).

Dell'appena esposta tendenza a quello che è stato definito "feticismo procedurale"[155] si trova conferma nella nota pronuncia *Big Brother Watch & Altri c. Regno Unito*[156], aspramente criticata da larga parte della dottrina sull'assunto che essa abbia costituito l'avvio di un denegato processo di normalizzazione della sorveglianza di massa[157], rispetto al quale non sembra essere ancora intervenuta una inversione di rotta[158]. Nonostante vi siano state critiche sulla recente apertura della Corte ai sistemi di intercettazione in blocco, va sottolineato che la stessa ha ravvisato una violazione dell'art.

---

[154] "The authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when "necessary in a democratic society". The supervision of interceptions, as it is currently organised, does not comply with the requirements of independence, powers and competence which are sufficient to exercise an effective and continuous control, public scrutiny and effectiveness in practice. The effectiveness of the remedies is undermined by the absence of notification at any point of interceptions, or adequate access to documents relating to interceptions", Corte europea dei diritti dell'uomo, Grande Camera, *Zakharov c. Russia*, cit., par. 302; sulla stessa linea, v. anche Corte europea dei diritti dell'uomo, sentenza del 12 gennaio 2016, ricorso n. 7138/14, *Szabó e Vissy c. Ungheria*, parr. 85-88.

[155] M. ZALNIERIUTE, *Procedural Fetishism and Mass Surveillance Under the ECHR. Big Brother Watch v. UK*, in *Verfassungsblog*, 2 giugno 2021, disponibile su verfassungsblog.de/big-b-v-uk.

[156] La Corte distingue tra quattro diverse fasi del processo di intercettazione di massa e statuisce che gli Stati debbano fornire garanzie "end-to-end" in ogni fase di questo processo. Nel valutare se lo Stato convenuto abbia agito nell'ambito del proprio margine di apprezzamento, occorrerà poi tenere conto di una serie di requisiti ulteriori rispetto ai cd. sei criteri minimi di salvaguardia stabiliti in *Weber e Saravia c. Germania* (cfr. *supra* nota n. 150): all'uopo il Giudice europeo indica un test ad otto fasi cui la legislazione nazionale deve essere rispondente. Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 25 maggio 2021, ricorsi nn. 58170/13, 62322/14 e 24960/15, *Big Brother Watch e altri c. Regno Unito*, rispettivamente parr. 325, 350 e 361.

[157] Sul punto *funditus* M. NINO, *La normalizzazione della sorveglianza di massa nella prassi giurisprudenziale delle Corti*, cit., p. 120. Per posizioni assonanti v. anche M. MILANOVIC, *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa*, in *EJIL:Talk! Blog of the European Journal of International Law*, 26 maggio 2021, disponibile su https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa; e, prima ancora della pubblicazione della sentenza della Grande Camera, A. STIANO, *Il diritto alla privacy alla prova della sorveglianza di massa e dell'intelligence sharing: la prospettiva della Corte europea dei diritti dell'uomo*, in *Rivista di diritto internazionale*, 2020, n. 2, pp. 511-537; 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 *Cronache dal cyberspazio*, maggio-agosto 2021, disponibile su www.nomosleattualitaneldiritto.it, pp.1-5.

[158] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 25 maggio 2021, ricorso n. 35252/08, *Centrum för Rättvisa c. Svezia*. I *dicta* contenuti nella pronuncia *Big Brother Watch* sono stati pienamente confermati. Nel caso di specie la Corte ha accertato che la normativa svedese di intercettazione di massa non prevedeva una norma chiara sulla distruzione del materiale intercettato non contenente dati personali; non includeva una disposizione garantista che tenesse conto della protezione della privacy individuale, in caso di trasmissione di materiale di intelligence ad entità straniere; non contemplava un effettivo riesame ex post della sorveglianza delle comunicazioni. Non contenendo, quindi, adeguate garanzie "end-to-end" idonee a salvaguardare il diritto alla vita privata, tale regime è stato ritenuto in contrasto con l'articolo 8 della CEDU. M. NINO, *La normalizzazione della sorveglianza di massa nella prassi giurisprudenziale delle Corti*, cit., p. 122; M. ROJSZCZAK, *The ECTHR's Judgment in Case of Centrum för Rättvisa v. Sweden as a Leading Case for the Review of Domestic Regulations on Signals Surveillance*, in *Review of International, European and Comparative Law*, 2019, n. 17, pp. 84-103; J. SAJFERT, *The Big Brother Watch and Centrum för Rättvisa Judgments of the Grand Chamber of the European Court of Human Rights – The Altamont of Privacy?*, in *European Law Blog*, 8 giugno 2021, in europeanlawblog.eu.

8 CEDU in entrambe le sentenze in ultimo citate, *mutatis mutandis*. Ciò che peraltro si è verificato anche nel caso *Gaughran c. Regno Unito*, particolarmente pertinente ai nostri fini avendo trattato, oltre che della conservazione a tempo indeterminato delle impronte digitali e del DNA, anche delle fotografie di un individuo condannato per guida in stato di ebrezza; in base al diritto interno del Paese convenuto tali fotografie, una volta acquisite in fase di arresto, sarebbero state conservate in un database e alle stesse sarebbe stato applicato il sistema di riconoscimento facciale in uso alle forze di polizia nazionali[159]. La Corte, nel ravvisare una violazione dell'art. 8 CEDU, ha evidenziato come la durata indefinita del periodo di conservazione di dati biometrici non sia *ex se* determinante al fine di valutare se uno Stato abbia o meno oltrepassato il proprio margine di apprezzamento; occorre, piuttosto, ponderare di volta in volta se la normativa nazionale di turno tenga conto della gravità del reato, della necessità di conservare i dati, e preveda idonee garanzie per l'individuo: "[w]here a State has put itself at the limit of the margin of appreciation in allocating to itself the most extensive power of indefinite retention, the existence and functioning of certain safeguards becomes decisive"[160].

7. Conclusioni

La *facial recognition technology* è una tecnologia a base biometrica che elabora dati personali sensibili, per l'appunto i dati biometrici, sicché essa costituisce una limitazione del diritto alla *privacy*. Peraltro, con riferimento alle sue più temute applicazioni, tale tecnica opera sulla base di una raccolta generalizzata ed indiscriminata di dati biometrici, ed in tal guisa ricopre un posto di primo piano nel contesto delle misure di sorveglianza elettronica statale e non.

Nell'introduzione al presente scritto si è detto come da più parti sia stata denunziata la grave assenza, a livello internazionale ed europeo, di un quadro giuridico chiaro ed uniforme sull'uso legittimo delle tecnologie di riconoscimento facciale[161]: con l'analisi condotta si pensa di aver dimostrato che tale assunto è privo di fondamento.

Al contrario, siccome qualsiasi applicazione di *FRT* costituisce un trattamento di dati personali sensibili, ad essa può ritenersi estendibile tutto l'*acquis* normativo, internazionale ed europeo, relativo alla tutela dei dati personali che, com'è noto, soprattutto nel quadro del diritto dell'Unione europea, è particolarmente robusto oltre che aggiornato. In tale prospettiva si è premessa l'importanza, a livello di cooperazione internazionale, della Convenzione n. 108, strumento di diritto internazionale pattizio a carattere regionale specificamente dedicato alla materia della protezione dei dati personali ratificato da tutti gli Stati membri dell'Unione europea ed aperto all'adesione di Stati che non sono parte del Consiglio d'Europa, per poi, sul piano dell'integrazione europea,

[159] Corte europea dei diritti dell'uomo, Prima Sezione, sentenza del 13 giugno 2020, ricorso n. 45245/15, *Gaughran c. Regno Unito*, par. 70.
[160] Ivi, par. 88.
[161] V. *supra* nota n. 26.

dedicare spazio all'analisi alle norme di diritto derivato in rilievo, tra le quali spicca senz'altro il Regolamento europeo sulla protezione dei dati personali, che costituisce un indubbio passo in avanti in termini di tutela del diritto fondamentale alla *privacy*, sia per lo strumento normativo in sé che da un punto di vista contenutistico.

Dovrebbe ora risultare chiaro come una normativa specificamente dedicata alle tecnologie di riconoscimento facciale, tanto reclamata dagli attivisti dei diritti umani nella speranza di vederne affermato il divieto di utilizzo, non solo non sia necessaria, ma al contrario potrebbe risultare funzionale proprio a chi si prefigge l'obiettivo di sfruttare economicamente i benefici che tale tecnologia, rientrante nella famiglia dell'*artificial intelligence*, può comportare: non a caso, questa è la dichiarata impostazione della Proposta di regolamento sull'intelligenza artificiale, in seno alla quale l'uso delle tecniche di riconoscimento facciale viene di fatto legittimato, proponendone il divieto assoluto solo in due ipotesi estreme[162].

Non vi è dubbio, pertanto, che *iure condito* le *facial recognition technologies* trovino già una precisa, e stringente, regolamentazione; e che, a ben vedere, ogni ulteriore disciplina di cui si auspica l'adozione correrebbe il rischio di creare un diritto particolare per tali tecniche rispetto ad altre tecnologie già sperimentate, parimenti idonee a ledere la vita privata dei consociati.

Si prenda l'esempio del legislatore italiano, che nel regolare in via interinale la materia con il disposto dell'art. 9, comma 9°, d.l. 8 ottobre 2021, n. 139 ha previsto la sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2023[163]. In buona sostanza, mentre sarà possibile anche nei luoghi pubblici o aperti al pubblico, al ricorrere delle condizioni di legge, registrare conversazioni tra presenti, utilizzare altre tecnologie biometriche (riconoscimento delle impronte digitali, dello sfondo dell'iride, ecc.), identificare le persone presenti attraverso il riconoscimento dei loro apparecchi telefonici e telematici, non si potrà, salve le limitate ipotesi non limpidamente descritte nei successivi commi 10 e 11, istallare impianti per il riconoscimento facciale, né utilizzare gli stessi ove previamente installati.

In quest'ottica, proprio il "feticismo procedurale" da taluni contestato alla più recente giurisprudenza delle due Corti appare maggiormente consapevole della realtà del

[162] Si veda *infra* pp. 18-19.

[163] Art. 9, comma 9, d.l. n. 139 dell'8 ottobre 2021: "in considerazione di quanto disposto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, nonché dalla direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dell'esigenza di disciplinare conformemente i requisiti di ammissibilità, le condizioni e le garanzie relativi all'impiego di sistemi di riconoscimento facciale, nel rispetto del principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea, l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici di cui all'articolo 4, numero 14), del citato regolamento (UE) 2016/679 in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, sono sospese fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2023".

fenomeno rispetto all'apparente rigidità di un legislatore, come quello italiano, che ha stabilito un donchisciottesco divieto di utilizzo della tecnologia "fino all'entrata in vigore di una disciplina legislativa della materia", ossia fino a che il legislatore medesimo non comprenda cosa sia giusto fare, o non venga sollevato in tale incombenza dal legislatore europeo.

Invero, dal panorama giurisprudenziale suesposto, l'ultimo orientamento di entrambe le Corti sembra volgere verso un ripensamento in positivo circa la validità e l'efficacia delle misure di sorveglianza, soprattutto quale strumento di lotta al terrorismo o, comunque, di contrasto a reati suscettibili di mettere in crisi la sicurezza nazionale; in effetti, negli ultimi anni, sul piatto della bilancia del test di stretta necessità che ogni interferenza con il diritto alla *privacy* deve superare, sembra aver assunto maggior peso il margine di apprezzamento statale, almeno con riferimento al fine della salvaguardia della sicurezza nazionale. Tale ripensamento sull'utilità di una raccolta di dati personali massiva ed indiscriminata nell'ottica appena descritta non sembra tuttavia equivalere ad una cieca accettazione delle attività statali di sorveglianza elettronica, ciò cui invece il concetto di 'normalizzazione', utilizzato da autorevole dottrina[164], sembra rimandare.

Come si è visto, l'approccio scelto da entrambe le Corti è quello di tentare di regolare il più possibile le attività che implicano misure di sorveglianza elettronica, con l'evidente obiettivo di impedirne le degenerazioni attraverso l'esame severo delle normative nazionali che le autorizzano e la verifica delle loro applicazioni in concreto: tant'è che l'attuale panorama giurisprudenziale, sia con riferimento alla Corte di giustizia che alla Corte europea dei diritti dell'uomo, è costellato dalla costante censura delle misure di sorveglianza nazionale di turno, all'esito del test di stretta necessità, ciò che sembra in palese contrasto con un'idea di normalizzazione del fenomeno, almeno da un punto di vista sostanziale.

ABSTRACT: La *facial recognition technology* è una tecnologia a base biometrica che elabora dati personali sensibili, per l'appunto i dati biometrici, sicché essa costituisce una limitazione del diritto alla *privacy*. Peraltro, con riferimento alle sue più temute applicazioni, tale tecnica opera sulla base di una raccolta generalizzata ed indiscriminata di dati biometrici, ed in tal guisa ricopre un posto di primo piano nel contesto delle misure di sorveglianza elettronica statale e non. Da più parti è stata denunziata la grave assenza, a livello internazionale ed europeo, di un quadro giuridico chiaro ed uniforme sull'uso legittimo delle tecnologie di riconoscimento facciale. Il presente lavoro aspira a ponderare la veridicità di tale assunto. Ciò, all'auspicato fine di comprendere se, ed eventualmente entro quali limiti, l'utilizzo della *facial recognition technology* possa ritenersi compatibile rispettivamente con il sistema della Convenzione europea dei diritti dell'uomo e con il diritto dell'Unione

[164] V. *supra* nota n. 157.

europea; e se, conseguentemente, sia effettivamente necessaria o anche solo auspicabile una legislazione specifica diretta a sancirne la liceità o l'illiceità.

KEYWORDS: tecnologie di riconoscimento facciale – diritto alla privacy – limiti – Corte di giustizia dell'Unione europea – Corte europea dei diritti dell'uomo.

THE PROTECTION OF BIOMETRIC DATA IN THE EUROPEAN AREA OF FUNDAMENTAL RIGHTS: ON THE LIMITS TO THE USE OF FACIAL RECOGNITION TECHNOLOGIES

ABSTRACT: Facial recognition technology is a biometric-based technology that processes sensitive personal data, namely biometric data, and thus constitutes a limitation of the right to privacy. Moreover, with reference to its most alarming applications, this technique operates on the basis of a generalised and indiscriminate collection of biometric data, and thus holds a prominent place in the context of state and non-state electronic surveillance measures. The serious absence, at international and European level, of a clear and uniform legal framework on the legitimate use of facial recognition technologies has been denounced in many contexts. This paper aspires to assess the validity of this assumption, in order to understand whether, and if so within what limits, the use of facial recognition technology can be considered compatible with the system of the European Convention on Human Rights and with European Union law; and whether, consequently, specific legislation aimed at sanctioning its lawfulness or unlawfulness is actually necessary or even desirable.

KEYWORDS: facial recognition technologies – right to privacy – limits – Court of Justice of the European Union – European Court of Human Rights.