Ricerche giuridiche

224
nuovissima serie

Ricerche giuridiche
Collana diretta da

A. CELOTTO, F. LIGUORI, L. ZOPPOLI

Comitato Scientifico

I. Caracciolo, M. Delfino, M. D'Onghia
L. Fernandez Del Moral Dominguez, F. Galgano, L. Gatt
A. Guardiano, M. Iovane, V. Luciani, R. Mastroianni, G. Montedoro
A. Patroni Griffi, S. Prisco, R. Spagnuolo Vigorita, A. Zito

GIUSEPPE MOBILIO

TECNOLOGIE DI RICONOSCIMENTO FACCIALE

Rischi per i diritti fondamentali e sfide regolative

EDITORIALE SCIENTIFICA

Il presente Volume è stato realizzato e finanziato nell'ambito delle attività del PRIN 2017 "Self- and Co-regulation for Emerging Technologies: Towards a Technological Rule of Law (SE.CO.R.E TECH)", responsabile Prof. Andrea Simoncini.

Proprietà letteraria riservata

© Copyright 2021 Editoriale Scientifica s.r.l.
via San Biagio dei Librai, 39 - 80138 Napoli
www.editorialescientifica.com info@editorialescientifica.com
ISBN 979-12-5976-053-1

A Lucia, Agnese e Marta,
che mi ricordano il significato autentico
del "vegliare-sopra"

INDICE

INTRODUZIONE

CAPITOLO I

RICONOSCIMENTO FACCIALE: TECNOLOGIE E PROBLEMATICHE INNOVATIVE

CAPITOLO II

DIRITTI FONDAMENTALI A RISCHIO

CAPITOLO III

IL TENTATIVO DEL DIRITTO POSITIVO DI REGOLARE LE TRF

CAPITOLO IV

TRF E NUOVE FRONTIERE DI SVILUPPO: I SISTEMI DI INFORMAZIONE EUROPEI

CAPITOLO V

LA REGOLAZIONE GIURIDICA DELLE TRF: NUOVE FORME E APPROCCI

INTRODUZIONE

SOMMARIO: 1. La sorveglianza biometrica tramite riconoscimento facciale: peculiarità e pericolosità. – 2. Percorso di analisi.

1. *La sorveglianza biometrica tramite riconoscimento facciale: peculiarità e pericolosità*

Le tecnologie di riconoscimento facciale (d'ora in avanti TRF) si basano su complessi procedimenti algoritmici che consentono di identificare una persona a partire dall'immagine del suo volto. In via generale, mediante la fotografia o il video che riprendono una persona, è possibile risalire alla sua identità grazie al confronto automatizzato dell'immagine estrapolata con altra immagine appartenente alla stessa persona nella quale era stata previamente identificata.

Ci troviamo nel campo delle tecnologie biometriche, tramite le quali è possibile distinguere un soggetto in forza di caratteristiche fisiche uniche, come le impronte digitali, il DNA, la forma dell'iride, la struttura vascolare della retina, la struttura venosa della mano, oppure attraverso i tratti differenziali del suo comportamento, come il modo di camminare o il timbro della voce[1].

Fra tutte queste tecnologie, quelle che sfruttano le immagini facciali possono considerarsi uniche. Una persona difficilmente potrà nascondere il proprio volto senza destare allarme. Allo stesso tempo, catturare l'immagine di un volto risulterà relativamente più facile rispetto ad acquisire le impronte digitali, un campione di DNA o le scansioni delle iridi[2].

Il riconoscimento facciale avviene tramite strumenti di rilevazione

[1] E. LEARNED-MILLER, V. ORDÓÑEZ, J. MORGENSTERN, J. BUOLAMWINI, *Facial Recognition Technologies in the Wild: A Primer*, 29 maggio 2020, 8. Più approfonditamente, v. *infra* Cap. III, par. 3.

[2] S.Z. LI, A.K. JAIN, *Introduction*, in S.Z. LI, A.K. JAIN (a cura di), *The Handbook of Face Recognition*, Springer, New York, 1.

meno invasivi, in quanto possono carpire immagini a distanza, in movimento e senza alcuna volontà cooperativa dell'interessato[3].

Le TRF, inoltre, possono essere integrate con molti altri strumenti e dispositivi, come sistemi di telecamere a circuito chiuso o i comuni *smartphone*, i quali rendono più facile raccogliere le immagini e trasmetterle poi a un server remoto ai fini della loro elaborazione[4].

L'interessato potrà quindi essere sottoposto ad un procedimento di riconoscimento facciale con la forza, con la persuasione, per mera accondiscendenza, o semplicemente senza che se ne renda conto e ne abbia consapevolezza[5].

Il ricorso a queste tecnologie risulta sempre meno costoso, più rapido, più diffuso; esso tuttavia manifesta criticità tecniche che altri sistemi biometrici non condividono nei medesimi termini. L'accuratezza del riconoscimento facciale dipende fortemente dalle condizioni e dalle modalità con le quali queste tecnologie vengono utilizzate. In aggiunta, occorre disporre di immagini di buona qualità, sia con riferimento alla rappresentazione del volto della persona da identificare, sia con riguardo alle immagini con cui viene operato il confronto. Altre parti del corpo, come ad esempio le impronte digitali o il DNA, si rivelano inoltre più affidabili per identificare una persona, soggette a minore rischio di confusione e suscettibili di minori mutamenti con il passare del tempo[6].

Più in generale, le TRF aprono a forme inedite e molto pervasive di sorveglianza rispetto ad ogni altra tecnologia attualmente disponibile. Con sorveglianza si può intendere la «raccolta ed elaborazione di dati personali, identificabili o meno, allo scopo di influenzare o controllare coloro ai quali essi appartengono»[7]; una pratica concepita sia

[3] GARVIE ET AL., *The Perpetual Line-Up. Unregulated Police Face Recognition in America*, *Georgetown Center on Privacy & Technology*, 18 ottobre 2016, 16 ss.

[4] Cfr. GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile*, WP 192, 22 marzo 2012.

[5] I. BERLE, *Face Recognition Technology. Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images*, Springer, Cham, 2020, 2.

[6] K.A. GATES, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance,* New York, NYU Press, 2011, 17.

[7] D. LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002, 2.

nella sua accezione positiva di "vegliare-sopra", allo scopo ad esempio di proteggere o garantire il benessere di una o più persone, come avviene nell'ipotesi della responsabilità genitoriale, negli ambiti lavorativi, o ad opera dei governi; sia nei suoi aspetti più pericolosi e lesivi dei diritti fondamentali, attraverso la capacità di imporre limiti e controlli[8].

Per contestualizzare questo assunto e inquadrare la portata di queste tecnologie può essere utile attingere alla riflessione sociologica che da tempo si interroga sulle evoluzioni – e involuzioni – delle molteplici forme di sorveglianza[9]. Si comprende come oramai non sia più adeguata l'immagine di un controllo potenzialmente costante, visibile e inverificabile incarnato dal modello di carcere panottico di Jeremy Bentham, ove una sola guardia, collocata al centro di una struttura circolare, potrebbe sorvegliare assiduamente i carcerati pur senza essere vista[10]. Nuove tecnologie come quelle di riconoscimento facciale, che sfruttano – sul punto si ritornerà – algoritmi, internet e *big data*, consentono di praticare una sorveglianza che va ben oltre le aspirazioni di questo modello[11].

Alla ineffettività del controllo esercitato da una sola persona posta

[8] *Ivi*, 3 ss. e 71 ss.

[9] P. PERRI, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, GFL, Milano, 2020, 3 ss.; M. GALIČ, T. TIMAN, B.-J. KOOPS, *Bentham, Deleuze and Beyond: an Overview of Surveillance Theories from the Panopticon to Participation*, in *Philosophy & Technology*, 30, 1, 2017, 10 ss.

[10] J. BENTHAM, *Panopticon ovvero la casa d'ispezione*, Marsilio, Venezia, 1983, 1997, 37 ss. Come noto, si tratta di un modello di carcere ideato con una architettura circolare, in cui i detenuti sono collocati alla periferia, tutti visibili da un unico "ispettore" collocato in una torre di controllo al centro, senza che essi possano sapere se l'ispettore sia davvero presente o li stia guardando, perché nascosto dietro a persiane che permettono di vedere ma non di essere visto. Come messo in luce da M. FOUCAULT, *Sorvegliare e punire. Nascita della prigione*, Einaudi, Torino, 1993, 218 ss., l'asimmetria cognitiva tra sorvegliante e sorvegliato è cruciale, poiché il primo è in grado di garantire la perfetta disciplina e il «funzionamento automatico del potere», senza che la sorveglianza venga continuamente esercitata, mentre il secondo «è visto ma non vede; oggetto di informazioni, mai soggetto di una comunicazione».

[11] Sulle rielaborazioni della concezione benthamiana della sorveglianza nella sociologia contemporanea, a partire dell'avvento delle tecnologie informatiche, v. più ampiamente D. LYON, *La società sorvegliata*, cit., 149 ss.

staticamente al centro della ipotetica prigione, si sostituisce oggi la capacità di raccogliere enormi quantità di informazioni su larga scala e la disponibilità di tecniche di analisi e rielaborazione dei dati raccolti[12]. Le vicende dell'ultimo ventennio legate al caso "ECHELON" e al controllo dei c.d. Cinque Occhi[13], alla diffusione di documenti riservati da parte di WikiLeaks[14], al c.d. scandalo "Datagate" originato dalle misure adoperate dopo gli attentati dell'11 settembre[15], hanno gettato luce sulle pratiche di sorveglianza digitale di massa condotte dai governi democratici.

Queste nuove forme di sorveglianza, inoltre, vengono perpetrate non soltanto da uno o più soggetti pubblici, alla stregua di un "Grande Fratello che ti osserva"[16], ma vengono praticate soprattutto da parte

[12] P. TINCANI, *Sorveglianza e potere. Disavventure dell'asimmetria cognitiva*, in *Ragion pratica*, 1, 2018, 61 ss.

[13] Con il caso "ECHELON" ci si riferisce al programma di sorveglianza condotto tramite intercettazioni di telecomunicazioni che è stato praticato, anche in Europa, su accordo di USA, Canada, Australia, Nuova Zelanda, Regno Unito (c.d. *Five Eyes*), accertato dalle istituzioni dell'UE a cavallo tra fine anni '90 e inizio anni 2000; più ampiamente, cfr. P. PERRI, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, cit., 96 ss.

[14] WikiLeaks è il sito fondato da Julian Assange allo scopo di pubblicare, tramite una interfaccia c.d. *wiki* (con una modalità aperta e collaborativa), documenti riservati su governi e aziende messi a disposizione anonimamente a seguito fughe di notizie (c.d. *leaks*) non rintracciabili: ne è derivato un forte dibattito, tra l'altro, sulla giustificabilità della pubblicazione di documenti riservati ma di interesse pubblico, sulla portata del potere di informazione e democratizzazione di internet, sul ruolo dei media tradizionali; più diffusamente cfr. G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, Milano, 2015, 166 ss.

[15] Lo scandalo *Datagate* nasce dalle rivelazioni di Edward Snowden, ex analista della *National Security Agency* degli Stati Uniti, che ha svelato come, a seguito degli attentati terroristici dell'11 settembre 2001, l'Agenzia abbia praticato un regime di sorveglianza indiscriminato e continuativo, avendo accesso, tra l'altro, ai metadati riguardanti il traffico telefonico all'interno degli USA e tra questi e l'estero; anche qui, più ampiamente, v. P. PERRI, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, cit., 100 ss.; S. SICA, G. GIANNONE CODIGLIONE, *La libertà fragile. Pubblico e privato al tempo della rete*, ESI, Napoli, 2014, 25 ss.; G. GREENWALD, *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, Rizzoli, Milano, 2014.

[16] Il riferimento va ovviamente a G. ORWELL, *1984*, Mondadori, Milano, 1950.

di soggetti e imprese private, cosicché nella società dell'informazione ognuno è soggetto ad una pluralità di sorveglianti[17].

Grazie alle nuove tecnologie disponibili, la sorveglianza è divenuta oramai pervasiva, ubiquitaria, ma soprattutto rispondente a finalità disparate, non tanto per imporre la disciplina, quanto piuttosto per ragioni economiche e lucrative. La grande novità che – è stato detto – ha elevato la sorveglianza a fattore "culturale"[18], è data poi dalla partecipazione attiva degli stessi sorvegliati, nell'essere ad un tempo "oggetti" che forniscono contenuti e "soggetti" che generano nuove forme di sorveglianza. Grazie ai dati e ai contenuti prodotti tramite i click sul web, i messaggi inviati o gli scambi di foto. i gesti quotidiani di chiunque vengono monitorati da parte di chiunque, siano essi governi, imprese o altri utenti dei *social network*. Tali dati divengono oggetto di desiderio per ragioni commerciali e di controllo soprattutto dei c.d. *Big Tech*[19], colossi del web che detengono oggi il vero potere di sorveglianza, protagonisti di una nuova forma di "capitalismo"[20].

[17] Questi elementi erano già presenti nel concetto di "società della sorveglianza" elaborato nei primi anni 2000, per indicare una sorveglianza portata avanti non solo dai governi, ma anche dalle imprese capitalistiche, che pervade ogni aspetto della vita sociale, compresi i luoghi di lavoro o di consumo, consentita da una infrastruttura informativa integrata che permette di scambiare informazioni tra diversi settori, con la collaborazione delle stesse persone sorvegliate; cfr. D. LYON, *La società sorvegliata*, cit.

[18] Cfr. ID., *La cultura della sorveglianza. Come la società del controllo ci ha reso tutti controllori*, Luiss University Press, Roma, 2020, ove il temine "cultura della sorveglianza" viene impiegato per indicare una sorveglianza che non agisce più semplicemente all'esterno delle persone per essere subìta, ma per dare la cifra di un fenomeno che oramai è stato interiorizzato e di cui tutti sono partecipi e fanno esperienza, in termini non indiscriminati ma fluidi, complicati e imprevedibili.

[19] Individuate nelle americane "GAFA", ovvero Google (e la collegata Alphabet), Amazon, Facebook ed Apple (cui si può aggiungere Microsoft e IBM), e le cinesi "BAT" (Baidu, Alibaba e Tencent, cui si può aggiungere Xiaomi).

[20] Il riferimento va alla già notissima elaborazione in S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma, 2019. Tale nuova forma di capitalismo «si appropria dell'esperienza umana usandola come materia prima da trasformare in dati sui comportamenti» ed impone il proprio potere tramite «l'automazione e una architettura computazionale sempre più presente, fatta di dispositivi, oggetti e spazi *smart* interconnessi» (*ivi*, 17 s.). I dati vengono carpiti per essere trasformati in «prodotti predittivi», in grado di stabilire cosa

Questi cenni sui mutamenti nelle forme e nelle accezioni della sorveglianza, oscillanti tra istanze di protezione e di sfruttamento, consentono di inquadrare più consapevolmente il rilievo assunto dalle TRF, la diffusione e la versatilità dei loro impieghi nelle società contemporanee.

In ambito pubblico[21], come si avrà modo di vedere più approfonditamente, queste tecnologie vengono sfruttate dalle forze dell'ordine per identificare e perseguire i sospettati di un crimine, o ricercare persone scomparse[22]; per esercitare controlli alle frontiere, come accade soprattutto negli aeroporti[23]; come strumento di gestione delle politiche migratorie e di rimpatrio[24].

Le TRF vengono altresì utilizzate per garantire la sicurezza e tracciare le persone in luoghi pubblici come stadi[25], durante concerti[26], in

sentiremo, penseremo e faremo, per influenzare il comportamento umano e trasformare i dati stessi in una fonte di guadagno, da cedere in quello che viene definito il «mercato dei comportamenti futuri», comprensivo della pubblicità online, assicurazioni, banche, finanza, vendita al dettaglio, ecc. (*ivi*, 18). Il potere che ne deriva induce queste compagnie ad acquisire sempre più dati per essere competitive e ad un tempo renderci dipendenti, generando una vera e propria «sorveglianza commerciale» (*ivi*, 21).

[21] Per una ampia ricognizione distinta per diverse finalità, v. già T. HUANG, Z. XIONG Z. ZHANGE, *Face Recognition Applications*, in S.Z. LI, A.K. JAIN (a cura di), *The Handbook of Face Recognition*, cit., 617 ss.

[22] Una pratica che si è diffusa massicciamente negli Stati Uniti, ma che sta prendendo piede in altri ordinamenti; cfr. J. SCHUPPE, *How Facial Recognition Became a Routine Policing Tool in America*, in *NBC NEWS*, 11 maggio 2019 [nbcnews.to/3cNNCQh].

[23] N. BERNAL, *AI lie detectors to be tested by the EU at border points*, in *The Telegraph*, 1 novembre 2018 [bit.ly/3fISCaJ].

[24] Grande scalpore ha suscitato negli USA l'utilizzo da parte delle agenzie federali responsabili per i rimpatri forzati di immagini tratte dai *database* degli uffici adibiti al rilascio delle patenti di guida, documenti che possono essere richiesti anche da coloro che sono sprovvisti di un regolare permesso di soggiorno; cfr. D. HARWELL, *FBI, ICE Find State Driver's License Photos are a Gold Mine for Facial-Recognition Searches*, in *The Washington Post*, 7 luglio 2019 [wapo.st/3rNyjeB].

[25] R. RODENBERG, *Sports Betting and Big Brother: Rise of Facial Recognition Cameras*, in *ESPN*, 3 ottobre 2018 [es.pn/3dDusfi].

[26] See G. CANON, *How Taylor Swift Showed us the Scary Future of Facial Recognition*, in *The Guardian*, 15 febbraio 2019 [bit.ly/3fPKXaQ].

occasione di manifestazioni pubbliche[27], persino all'interno di luoghi di culto[28], e più in generale all'interno delle *smart cities*[29].

Particolari impieghi del riconoscimento facciale cominciano ad essere sfruttati nel settore dell'istruzione – su cui si ritornerà[30] – per effettuare controlli di sicurezza all'interno degli istituti scolastici, monitorare la frequenza degli studenti e valutare il loro grado effettivo di partecipazione alle lezioni; oppure in ambito medico, per rilevare il dolore dei pazienti[31], indagare le caratteristiche genetiche attraverso i tratti fenotipici[32], per compiere indagini sulla salute mentale delle persone[33], o per monitorare i pazienti ad alto rischio[34]. Più di recente, durante l'emergenza pandemica da Covid-19, i sistemi di riconoscimento facciale sono stati adoperati in questi settori per monitorare gli studenti durante gli esami a distanza[35], oppure per misurare la temperatura delle persone tra la folla, identificare (a scopi sollecitatori) coloro che non indossano la mascherina e tracciare coloro che risultano potenzialmente infetti[36].

Ci sono Paesi in cui le TRF sono impiegate sistematicamente allo

[27] Come accaduto in occasione del carnevale a Rio de Janeiro; cfr. *Rio Carnival turns to biometrics*, in *Biometric Technology Today*, 2, 2019, 3.

[28] Cfr. S. PULLIAM BALLEY, *Skipping Church? Facial Recognition Software Could Be Tracking You*, in *The Washington Post*, 24 luglio 2015 [wapo.st/3cSCGRG].

[29] Cfr. P.K. MEDAPATI, P.H.S.T. MURTHY, K.P. SRIDHAR, *LAMSTAR: For IoT-based face recognition system to manage the safety factor in smart cities*, in *Transaction on Emerging Telecommunications Technologies*, 31, 12, 8 dicembre 2019.

[30] Cfr. *infra* Cap. II, par. 8 e Cap. III, par. 4.1.

[31] C. SMITH, *Facial Recognition Enters into Healthcare*, in *Journal of AHIMA*, 4 settembre 2018 [bit.ly/3dArb03].

[32] Y. GUROVICH ET AL., *Identifying facial phenotypes of genetic disorders using deep learning*, in *Nature Medicine*, 25, 2019, 60 ss.

[33] R. WANG, A.T. CAMPBELL, X. ZHOU, *Using Opportunistic Face Logging from Smartphone to Infer Mental Health: Challenges and Future Directions*, in *UbiComp/ISWC'15 Adjunct*, settembre 2015, 683 ss. [bit.ly/3rSafYa].

[34] J. LOUGHRAN, *Facial recognition used to monitor high-risk hospital patients*, in *Engeneering & Technology*, 3 giugno 2019 [bit.ly/3mo8np6].

[35] Cfr. A. DINI, *La tecnologia per combattere imbrogli e distrazioni negli esami online*, in *La Stampa*, 12 maggio 2020 [bit.ly/3cRsfgX].

[36] Cfr. M. VAN NATTA ET AL., *The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic*, in *Journal of Law and the Biosciences*, 7, 1, gennaio-giugno 2020.

scopo di perseguire determinate politiche, come in India con il controverso *Aadhaar project*, finalizzato a stabilire in maniera univoca l'identità dei cittadini e preordinato alla allocazione più efficace di sussidi, benefici, sovvenzioni e servizi pubblici ai soggetti più bisognosi e alle fasce più povere della società[37]; oppure in Cina, nell'ambito del "Sistema di credito sociale", attraverso cui – sul punto si tornerà[38] – il governo riesce a profilare le persone, assegnare loro un punteggio (c.d. *scoring*) e influenzare il comportamento di massa; o addirittura per identificare oppositori politici, minoranze etniche e religiose[39].

Le TRF stanno andando incontro ad una diffusione crescente anche in ambiti privati o per scopi commerciali[40].

Questi sistemi possono essere sfruttati, anche qui, per scopi di sicurezza all'interno di esercizi commerciali[41], da parte degli istituti bancari[42], o delle compagnie assicurative[43]. Tramite riconoscimento facciale è

[37] Il controverso *Aadhaar project* è un sistema nazionale sviluppato in India e finalizzato ad individuare in maniera univoca l'identità dei cittadini mediante l'attribuzione del c.d. *Aadhaar number*, ottenuto tramite il rilascio di una serie di informazioni, tra cui i dati biometrici e le fotografie del volto, funzionale anche alle attività di controllo. I dati vengono conservati in un *database* centrale, sotto la gestione della *Unique Identification Authority of India* (UIDAI). Progressivamente l'utilizzo dell'*Aadhaar number* è stato esteso anche ad ulteriori ambiti, come quello bancario o i servizi di telefonia. La disciplina recata dall'*Aadhaar Act* n. 18/2016 è stata impugnata innanzi alla Corte Suprema indiana, che con una pronuncia del 26 settembre 2018 ha fatto salvo il sistema, a condizione, fra l'altro, che tali forme di rilevamento e controllo fossero limitate alla loro finalità originaria; cfr. G. FORMICI, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in *DPCE online*, 2, 2019, 1113 ss.

[38] Cfr. *infra* Cap. III, par. 6.4.

[39] È quanto sta avvenendo con la minoranza mussulmana degli Uiguri in Cina; cfr. P. MOZUR, *One month, 500,000 face scans: how China is using A.I. to profile a minority*, in *The New York Times*, 14 aprile 2019 [nyti.ms/2PFHxMZ]; HUMAN RIGHTS COUNCIL, *Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, A/HRC/41/35, 28 maggio 2019.

[40] Per una ricognizione distinta per diverse finalità, v. U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522, 11 agosto 2020, 11 ss.

[41] Cfr. *infra* Cap. II, par. 7.

[42] FINDFACE, *Face recognition for financial institutions* [bit.ly/2PD9vcb].

possibile effettuare pagamenti[44], ovvero personalizzare in tempo reale l'esperienza di acquisto dei clienti tramite offerte e pubblicità mirate[45].

Le TRF vengono utilizzate per realizzare ambienti c.d. *smart*, come avviene nella domotica, non solo per aprire le proprie abitazioni, ma anche per identificare le persone al loro interno, interpretare le azioni e interagire con i dispositivi in base alle espressioni del volto[46].

Sistemi di riconoscimento facciale vengono integrati negli *smartphone* di ultima generazione come modalità di sbloccamento[47]; da parte dei *social media* per ottenere maggior visibilità e allargare il proprio *network* di conoscenti[48]; dalle *console* di gioco per creare esperienze più immersive[49].

Si tratta di tecnologie sempre più alla portata di chiunque, soggetti pubblici o privati.

Quanto ai primi, si consideri che in questo settore della tecnologia, nel corso del tempo, il legame con le imprese private sia andato progressivamente stringendosi, in una comunanza di interessi verso queste forme di sorveglianza[50]. Le forze dell'ordine, in particolare, si rivolgo-

[43] *How facial recognition could save insurance companies billions*, in *Information Age*, 11 maggio 2018 [bit.ly/3utOdNd].

[44] *Smile-to-pay: Chinese shoppers turn to facial payment technology*, in *The Guardian*, 4 settembre 2019 [bit.ly/3dHGlku].

[45] K. KULIGOWSKI, *Facial Recognition Advertising: The New Way to Target Ads at Consumers*, in *Business News Daily*, 19 luglio 2019 [bit.ly/3cRAVEf].

[46] A. PENTLAND, T. CHOUDHURY, *Personalizing Smart Environments: Face Recognition for Human Interaction*, in *Computer*, 33, 2000, 50 ss.; F. ZUO, P.H.N. DE WITH. *Real-time embedded face recognition for smart home*, in *IEEE Transactions on Consumer Electronics*, 51, 1, febbraio 2005, 183 ss.

[47] *Face unlock degli smartphone: tecnologia sempre più avanzata per il 2020*, in *Adnkronos*, 9 gennaio 2020 [bit.ly/2OmiQVd].

[48] Sul sistema di suggerimento di Facebook per aggiungere i c.d. "tags", cfr. *infra* Cap. III, par. 4.1.

[49] D. GANTENBEIN, *Helping Kinect Recognize Faces*, in *Microsoft.com*, 31 ottobre 2011 [bit.ly/3sRZTJf].

[50] Cfr. K.A. GATES, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*, cit., 28 ss., per una più ampia ricostruzione della diffusione di TRF incentrata prevalentemente sugli Stati Uniti, ove i primi progetti negli anni '60 vennero finanziati dalla Defense Advanced Research Projects Agency (DARPA) a scopo militare, ma a partire dagli anni '60 emerse prepotentemente l'interesse tanto delle banche al contrasto dei "furti di identità", quanto delle imprese a conoscere meglio le

no oggi ad intermediari privati, o direttamente alle grandi piattaforme del web, per ottenere la disponibilità di tecnologie, immagini e dati personali[51]. Basti considerare il successo e le polemiche riscosse da Clearview AI, una piccola start-up newyorkese che ha sviluppato un sistema di riconoscimento facciale, venduto ad oltre seicento agenzie negli Stati Uniti, in grado di identificare una persona attraverso il confronto non soltanto limitato alle foto segnaletiche disponibili alle forze di polizia o alle fotografie presenti negli archivi delle motorizzazioni civili, ma rastrellando miliardi di immagini presenti su internet, compresi i *social network*[52].

Analoghi strumenti sono a disposizione anche di soggetti privati, come grandi industrie o piccoli commercianti, e chiunque può scaricare numerosi software di riconoscimento facciale in *open-source*[53].

Ovviamente, però, nella corsa alla ricerca e sviluppo delle TRF i *Big Tech* occupano i primi posti, in ragione del *know-how*, delle risorse e della quantità di dati a loro disposizione: si pensi al sistema "Rekognition" di Amazon; "Deepface" di Facebook; "FaceNet" di Google; e così via[54].

abitudini dei consumatori per adattare la produzione e controllare i propri lavoratori. A partire dagli anni '90, si è assistito ad un impennare della domanda di questi strumenti per finalità di controllo della popolazione carceraria, contrasto al crimine nelle città, controlli alle frontiere e lotta al narcotraffico, sino alla fatidica data dell'11 settembre 2001 e all'avvio di politiche su scala globale di contrasto al terrorismo, di *intelligence* e di sorveglianza massiva, citate *retro*.

[51] K. BRENNAN-MARQUEZ, *The Constitutional Limits of Private Surveillance*, in *Kansas Law Review*, 66, 2018, 485 ss.

[52] Cfr. K. HILL, *The Secretive Company That Might End Privacy as We Know It*, in *The New York Times*, 18 gennaio 2020 [nyti.ms/3dFyCDs]; I. NERONI REZENDE, *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, in *New Journal of European Criminal Law*, 11, 3, 2020, 375 ss.

[53] Si pensi, tra gli esempi più conosciuti, a Facefirst, azienda statunitense che vende un prodotto che può integrare TRF con "qualsiasi software di terze parti", comprese le telecamere a circuito chiuso (cfr. *Sentinel-IQ Face Recognition Surveillance* [bit.ly/3uoW1Q5]); oppure al "Dragonfly Eye System" messo a disposizione dalla cinese YITU Technology (cfr. A. LENTINO, *This Chinese facial recognition start-up can identify a person in seconds*, in *CNBC*, 16 maggio 2019 [cnb.cx/3fK65iI]). Per altri esempi di software di riconoscimento facciale *open-source* e reperibili da chiunque, cfr. O. KHARKOVYNA, *Facial recognition: 8 Open-source tools to detect faces*, in *Medium*, 1 marzo 2021 [bit.ly/3cTckPg].

[54] Cfr. *Facial recognition: top 7 trends (tech, vendors, markets, use cases & latest news)*, in *Thales*, 20 febbraio 2021 [bit.ly/3sS2zq1].

Le criticità che sorgono da questi innovativi strumenti di sorveglianza non riguardano solamente la difesa della nostra intimità da occhi (elettronici) indiscreti, ma anche l'incapacità di sapere cosa ne venga fatto dei dati e delle informazioni così acquisite[55]. Adoperando un parallelo letterario[56], si potrebbe sostenere che il problema non nasca soltanto – richiamando la già citata metafora orwelliana del Grande Fratello[57] – dalla sorveglianza in sé, il controllo sociale e la capacità inibitoria che ne deriva; quanto piuttosto – prendendo in prestito la metafora kafkiana de "Il processo"[58] – la sottoposizione ad un potere invisibile e incomprensibile che può raccogliere informazioni su ciascuno, compilare profili e dossier, assumere decisioni senza fornire spiegazioni o garantire alcuna partecipazione. Le TRF possono contribuire ad incutere uno stato di soggezione che deriva dalla raccolta di informazioni sui luoghi frequentati, le persone incontrate, le preferenze espresse, le reazioni esercitate, aprendo così ad enormi criticità sulle modalità con cui avviene la raccolta delle immagini, la loro conservazione, i soggetti che possono averne accesso, la cessione e la circolazione dei dati che da esse possono ricavarsi, l'impiego che potrà esserne fatto.

Alcuni governi e decisori politici stanno prendendo posizione innanzi ai rischi legati a questi sviluppi tecnologici. Negli Stati Uniti, ove questi sistemi di sorveglianza sono particolarmente diffusi[59], alcuni Stati, come il New Hampshire[60], e molte città, come San Francisco[61], Boston[62], Somerville[63] o Portland[64], stanno discutendo l'opportunità o

[55] D. LYON, *La società sorvegliata*, cit., 28.

[56] Riprendendo le considerazioni in D.J. SOLOVE, *Nothing to hide: the false trade off between privacy and security*, New Haven-London, Yale University Press, 2011, 25 s.

[57] G. ORWELL, *1984*, cit.

[58] Cfr. F. KAFKA, *Il processo*, Garzanti, Milano, 1984.

[59] Più ampiamente, cfr. J. SPIVACK, C. GARVIE, *A Taxonomy of Legislative Approaches to Face Recognition in the United States*, in A. KAK (a cura di), *Regulating Biometrics: Global Approaches and Urgent Questions*, AI Now Institute, settembre 2020, 89 ss.

[60] Sulla proposta di vietare la raccolta e l'uso di dati biometrici, cfr. [bit.ly/3s3RAZl].

[61] La prima città che, dal maggio 2019, ha approvato tale divieto per le forze dell'ordine; cfr. [bit.ly/39ZKkaT].

[62] Divieto riferito alle forze di polizia ed alter pubbliche autorità: cfr. [bit.ly/2PSnlaL].

hanno già proibito l'impiego delle TRF da parte delle forze di polizia e altre autorità pubbliche, mentre altri Stati ne hanno sospeso il ricorso per un certo periodo di tempo, come la California[65] e New York[66]. A livello federale, invece, da tempo le TRF sono all'attenzione della *Federal Trade Commission*[67] e del *National Institute of Standards and Technology*[68], ma di recente si registrano iniziative volte ad approfondire l'impatto di queste tecnologie a livello socio-economico e giuridico, come dimostrano il report pubblicato nel luglio 2020 dal *Government Accountability Office* (GAO)[69] e le "*hearings*" svolte dal Congresso statunitense nel biennio 2019-2020[70].

Anche alcune imprese private stanno decidendo di non sviluppare più, o non mettere a disposizione delle autorità pubbliche, tecnologie legate al riconoscimento facciale. Così la statunitense *Axon*, ovvero la più grande produttrice al mondo di videocamere indossabili (c.d. *bo-*

[63] Divieto rivolto alle forze dell'ordine: cfr. [bit.ly/3dUHpBx].

[64] Divieto rivolto alle pubbliche amministrazioni e, a certe condizioni, anche ai privati: cfr. [bit.ly/3d3wvtN]. https://bit.ly/2PSnlaL.

[65] Con riguardo alle forze dell'ordine: Cfr. [bit.ly/3wL8Oyb].

[66] Con riguardo all'impiego negli istituti scolastici: cfr. *Governor Cuomo Signs Legislation Suspending Use and Directing Study of Facial Recognition Technology in Schools*, 22 dicembre 2020 [on.ny.gov/3wsCekL].

[67] La *Federal Trade Commission* (FTC) ha avviato nel 2011 una inchiesta sull'uso delle tecnologie di riconoscimento facciale dopo un reclamo proposto nei confronti dell'uso di queste tecnologie da parte di Facebook promosso da alcune organizzazioni a tutela dei consumatori. In esito ad un seminario intitolato "*Face Facts*" che ha coinvolto numerosi stakeholders, la FRC ha adottato nell'ottobre 2012 il documento "*Facing Facts: Best practices for common uses of facial recognition technologies*".

[68] Il NIST è un'agenzia facente parte dell'*U.S. Department of Commerce*, che sta conducendo, a partire dall'inizio degli anni 2000, un test degli algoritmi di riconoscimento facciale che vengono ad essa sottoposti volontariamente dalle aziende private; maggior informazioni, anche per reperire i documenti citati di seguito, su: [bit.ly/3rM68Ni].

[69] U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, cit.

[70] Si ha riguardo al ciclo di audizioni avviate tra il maggio 2019 e il gennaio 2020 dal *Committee on Oversight and Reform* della Camera dei Rappresentanti su tre distinti profili, relativi a "*Its impact on our civil rights and liberties*", "*Ensuring Transparency in Government Use*" e "*Ensuring Commercial Transparency & Accuracy*".

dycam), ha deciso di sospendere le forniture alle forze dell'ordine[71], ed anche *Big Tech* come Amazon, Microsoft e IBM hanno annunciato una moratoria o di volere uscire dal mercato delle TRF[72].

Sempre negli Stati uniti, inoltre, si sta sollevando un ampio moto di protesta contro queste tecnologie, coinvolgendo la società civile, centri di ricerca e istituti universitari, impegnati nel sottolineare i pericoli generati per i diritti fondamentali e gli interi ordinamenti democratici[73].

Anche in Europa si sta progressivamente sviluppando una riflessione critica sulle problematiche legate al riconoscimento facciale, sia a livello di società civile[74], sia a livello di istituzioni politiche. Al di là del-

[71] K. CRAWFORD, *Regulate facial-recognition technology*, in *Nature*, 29 agosto 2019, 565.

[72] R. HEILWEIL, *Big Tech Companies Back Away from Selling Facial Recognition Technology to Police. That's Progress*, in *Vox*, 11 giugno 2020 [bit.ly/3dDCHI6]. Sebbene alcune di queste compagnie rimangano nel business della produzione di tecnologie di sorveglianza attraverso la partnership con società minori e nella fornitura dei servizi di *cloud*; cfr. M. KWET, *The Microsoft Police State: Mass Surveillance, Facial Recognition, and the Azure Cloud*, in *The Intercept*, 14 luglio 2020 [bit.ly/3rVcIRw].

[73] Si considerino, fra i molteplici, gli studi promossi dalla *Algorithmic Justice League* (cfr. LEARNED-MILLER, V. ORDÓÑEZ, J. MORGENSTERN, J. BUOLAMWINI, *Facial Recognition Technologies in the Wild: A Call for a Federal Office*, 29 maggio 2020), l'*Alan Turing Institute* (cfr. LESLIE, *Understanding bias in facial recognition technologies: an explainer*, *The Alan Turing Institute*, 2020), l'*Electronic Privacy Information Center* (EPIC) [bit.ly/3dFtEGL], l'*American Civil Liberties Union* (ACLU) (cfr. A. HASAN, *2019 Proved We Can Stop Face Recognition Surveillance*, in *ACLU*, 17 gennaio 2020); o da centri di ricerca affiliati a istituzioni universitare, come il *Georgetown Center on Privacy & Technology* (cfr. C. GARVIE ET AL., *The Perpetual Line-Up. Unregulated Police Face Recognition in America*, cit.), l'*AI Now Institute* della New York University (cfr. AI NOW INSTITUTE, *AI Now Report 2019*, dicembre 2019).

[74] Sulla messa al bando del riconoscimento facciale utilizzato per l'identificazione e la profilazione, si pensi alla posizione di associazioni come *Big Brother Watch* (cfr. *Face Off. The lawless growth of facial recognition in UK policing*, maggio 2018), o *European Digital Rights* (EDRi) (cfr, *Ban Biometric Mass Surveillance: A set of fund rights requests for the European Commission and EU Member States*, maggio 2020), [bit.ly/3wtZM8G]. Nel settembre 2020 è stata inoltre lanciata una petizione #BanFacialRecognitionEurope avente lo stesso scopo [bit.ly/31UV3Pf]. Attualmente è in corso anche una raccolta di firme, che terminerà il 1° maggio 2022, per una iniziativa dei cittadini europei finalizzata a richiedere alla Commissione "il divieto delle pratiche di sorveglianza biometrica di massa" [bit.ly/3sSAXRV].

le iniziative di singoli Paesi volte ad approfondire le problematiche in questione, come nel Regno Unito[75], è nei documenti ufficiali delle istituzioni dell'UE che si registrano le prime prese di posizione[76]. Così il Parlamento europeo, come accaduto con la risoluzione del 2019 su "Una politica industriale europea globale in materia di robotica e intelligenza artificiale"[77], o la Commissione, che nel *White paper* del 2020 dedicato all'IA ha espresso serie preoccupazioni per le applicazioni di quest'ultima a "scopi di identificazione biometrica a distanza", o per "l'impiego di riconoscimento facciale negli spazi pubblici", in quanto portatore di "specifici rischi per i diritti fondamentali": in relazione a queste tematiche verrà avviato "un ampio dibattito sulle circostanze specifiche che potrebbero giustificare tale uso, e sulle garanzie comuni"[78]. In una bozza preliminare dello stesso *White paper* si paventava

[75] Nel Regno Unito, dove – come si vedrà – le TRF hanno cominciato a diffondersi considerevolmente nell'ultimo quinquennio, specie tra le forze di polizia, la *House of Lord* sta attualmente discutendo di una possibile moratoria nell'utilizzo di questi strumenti [bit.ly/2PBaDx6].

[76] Ma non solo: anche il Gruppo di esperti ad alto livello sull'intelligenza artificiale, istituito dalla Commissione europea, ha chiarito che l'identificazione automatica «desta enormi preoccupazioni di natura sia giuridica che etica, in quanto può avere effetti non previsti sotto molti aspetti a livello psicologico e socioculturale. Per salvaguardare l'autonomia dei cittadini europei è necessario ricorrere alle tecniche di controllo tramite l'IA in modo proporzionato. Definire chiaramente se, quando e come l'IA può essere utilizzata per l'identificazione automatica degli individui e differenziare tra l'identificazione di un individuo e la sua tracciatura e localizzazione, e tra sorveglianza mirata e sorveglianza di massa, sarà fondamentale per ottenere un'IA affidabile»; cfr. GRUPPO DI ESPERTI AD ALTO LIVELLO SULL'INTELLIGENZA ARTIFICIALE, *Orientamenti etici per un'IA affidabile*, aprile 2019, p. 130.

[77] Cfr. PARLAMENTO EUROPEO, *Una politica industriale europea globale in materia di robotica e intelligenza artificiale* (2018/2088(INI)), 12 febbraio 2019, 13, ove si esprime profonda preoccupazione per l'utilizzo di applicazioni di IA, ivi compreso il riconoscimento facciale e vocale, in programmi di "sorveglianza emotiva", ossia di monitoraggio delle condizioni mentali dei lavoratori e dei cittadini per aumentare la produttività e conservare la stabilità sociale, talvolta combinati con sistemi di "credito sociale", come ad esempio già accade in Cina; si sottolinea infatti che «tali programmi contraddicono per loro natura i valori e le norme europei che tutelano i diritti e le libertà degli individui».

[78] EUROPEAN COMMISSION, White Paper "*On Artificial Intelligence - A European approach to excellence and trust*", COM(2020) 65 final, 19 febbraio 2020, 21 s.

più esplicitamente la possibilità di proibire l'uso di queste tecnologie da parte di soggetti pubblici e privati per un periodo variabile dai tre ai cinque anni[79], ma il discorso sull'opportunità di una moratoria che riguardi le autorità pubbliche è stata successivamente ripreso anche dal Garante europeo della protezione dei dati[80] e ribadito dal Parlamento europeo[81].

Come si vedrà nel corso della trattazione, non tutti gli impieghi di queste tecnologie pongono i medesimi problemi. Un sistema di riconoscimento facciale per consentire l'accesso alla propria abitazione con il supporto di una *smart card* non è equiparabile all'utilizzo da parte delle forze di polizia per identificare le persone inconsapevoli tra la folla[82]. Gli usi privati o – per così dire – "ricreativi" di queste tecnologie, tuttavia, non devono distogliere l'attenzione dalla capacità di monitoraggio, controllo e tracciamento estremamente invasivo offerta dalle TRF, attraverso le quali è possibile ricostruire lo stile di vita, le abitudini, le preferenze, le relazioni interpersonali su larga scala[83]. Come accennato all'inizio, le potenzialità di questi strumenti di sorveglianza possono risultare decisive, ad esempio, per contrastare i crimini più efferati, ma possono costituire ausili potentissimi in mano a regimi oppressivi o imprese senza scrupoli[84]. Occorre quindi «definire le condi-

[79] J. DELCKER, B. SMITH-MEYER, *EU considers temporary ban on facial recognition in public spaces*, in *Politico*, 16 gennaio 2020 [politi.co/31PG9tS].

[80] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust*, 29 giugno 2020, p. 66.

[81] EUROPEAN PARLIAMENT, Resolution *"Artificial intelligence: questions of interpretation and application of international law"*, P9_TA(2021)0009, 20 gennaio 2021, p. 56.

[82] CNIL, *Facial recognition: for a debate living up to the challenges*, 19 dicembre 2019, 4.

[83] M. HIROSE, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, in *Connecticut Law Review*, 49, 5, 2017, 1591 ss.

[84] Ritornano alla memoria le considerazioni di Carl Schmitt a proposito della "fede nella tecnica", che ricordano come «la tecnica è sempre e soltanto strumento ed arma e proprio per il fatto che serve a tutti non è neutrale»; cfr. C. SCHMITT, *Il concetto di «politico»*, in ID., *Le categorie del 'politico'*, il Mulino, Bologna, 1972, 172 ss. (178).

zioni necessarie per evitare che la società della sorveglianza si risolva nel controllo autoritario, nella discriminazione, in vecchie e nuove stratificazioni sociali produttive di esclusione, nel dominio pieno di una logica di mercato che cerca una ulteriore legittimazione proprio nella tecnologia»[85].

È una sfida che, oggi, deve essere inevitabilmente raccolta dal diritto e dai legislatori. Secondo certe visioni estremistiche, occorrerebbe abolire del tutto l'utilizzo di TRF; secondo altre, invece, il ricorso a questa tecnologia dovrebbe essere attentamente regolato e necessariamente limitato, per consentire così di poterne beneficiare in termini giuridicamente ed eticamente sostenibili[86]. L'aspirazione è stabilire se, e a quali condizioni, sia possibile impiegare le TRF con uno "*human-centred approach*", ovvero secondo la prospettiva antropocentrica propugnata dalla Commissione europea sin dai primi documenti del 2018 sull'IA[87], che riesca a coniugare le istanze economiche e securitarie con la tutela dei diritti fondamentali delle persone all'interno delle società democratiche[88]. Allo stato, nessun legislatore nell'area europea – a

[85] S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997, 165.

[86] NAKAR, D. GREENBAUM, *Now you see me. Now you still do: facial recognition technology and the growing lack of privacy*, in *Boston University Journal of Science & Technology Law*, 23, 2017, 98, che riporta come esempio l'attentato durante la maratona di Boston del 15 aprile 2013 e gli studi che dimostrano come, dalle immagini acquisite dalle telecamere dei circuiti di sorveglianza nei pressi del luogo dell'attentato, l'utilizzo di strumenti di riconoscimento facciale più avanzati avrebbero consentito di identificare l'attentatore con estrema velocità; cfr. J.C. KLONTZ, A. JAIN, *A Case Study on Unconstrained Facial Recognition Using the Boston Marathon Bombings Suspects*, in *Computer*, 46, 11, 2013, 91 ss.

[87] Cfr. EUROPEAN COMMISSION, Communication "*Artificial Intelligence for Europe*", COM(2018) 237 final, 25 aprile 2018, ove si esplicitano i tre pilastri dell'iniziativa: "*boost the EU's technological and industrial capacity and AI uptake across the economy*"; "*prepare for socio-economic changes*"; "*ensure an appropriate ethical and legal framework*". Qui si anticipa l'obiettivo di costruire uno "*human-centric, inclusive approach to AI*" (13), poi sviluppato in altri documenti, come EUROPEAN COMMISSION, Communication "*Building Trust in Human-Centric Artificial Intelligence*", COM(2019) 168 final, 8 aprile 2019, e ID., White Paper "*On Artificial Intelligence - A European approach to excellence and trust*", cit.

[88] Aspetto particolarmente rimarcato in A. ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazio-*

quanto risulta – ha espressamente raccolto questa sfida, mancando una normativa che si riferisca espressamente a queste tecnologie e ponga le sopra citate condizioni. Anche la riflessione giuridica sul punto appare piuttosto contenuta, lasciando pressoché inesplorata la complessità delle questioni problematiche che originano dalle TRF, a partire dal loro impatto sui diritti fondamentali e dalla pretesa regolativa che il diritto è chiamato ad avanzare.

2. *Percorso di analisi*

L'ipotesi di fondo alla presente analisi è che tecnologie innovative come quelle di riconoscimento facciale siano in grado di perpetrare nuove e insidiose forme di limitazione alle libertà di singoli o dei gruppi sociali; per certi versi, pongono l'esigenza di riconfigurare le modalità di tutela stessa di alcuni diritti fondamentali. Di contro, la normazione giuridica, per riuscire a porre un argine efficace a questa capacità invasiva e consentire di beneficiare delle possibilità concesse da queste tecnologie, è chiamata necessariamente ad uno sforzo di ripensamento di strumenti, tecniche e contenuti di regolazione.

Il diritto costituzionale offre un punto di vista privilegiato per indagare la correlazione che intercorre tra le TRF, la tutela dei diritti fondamentali e l'ambizione del diritto ad offrire una disciplina di questi fenomeni.

A partire da questo angolo prospettico, la riflessione verrà articolata nel seguente percorso.

Nel Capitolo I si cercherà di indagare più da vicino, attingendo anche alla letteratura informatica, quale sia il funzionamento delle TRF, come si sviluppi il procedimento di riconoscimento facciale e quali siano le principali funzionalità per le quali è possibile farvi ricorso (par. 2). Per evidenziare alcune problematiche emergenti destinate a riflettersi sul piano propriamente giuridico, occorrerà rapportare le TRF nei più ampi contesti entro cui – e grazie ai quali – hanno trovato

ne europeo tra mercato unico digitale e tutela dei diritti fondamentali, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini, Pisa, 2020, 13 ss.

sviluppo, ovvero l'IA, i *big data* e il *machine learning*. Questa operazione deduttiva permetterà di comprendere meglio – ma non anche di giustificare pienamente – l'aspirazione delle TRF, rispettivamente, a "leggere" le emozioni umane, nella misura in cui si accogliesse una certa ideologia riduzionista tesa ad assimilare l'intelligenza umana con quella artificiale (par. 3.1); riuscire a inferire dall'espressione del volto alcuni tratti della psiche, della personalità e delle più intime preferenze, in accordo con quello che è stato definito il passaggio dalla "causazione" di fenomeni alla "correlazione" dei dati (par. 3.2); esercitare un controllo sulle TRF, a fronte della sempre più ampia autonomia che le macchine stanno acquisendo rispetto all'essere umano (par. 3.3).

Nel Capitolo II verrà offerta una panoramica sui diritti fondamentali che le TRF sono in grado di incidere e limitare sotto diversi profili. A questo riguardo, la riflessione muoverà dalla sfera dei diritti che, secondo una certa accezione, sono riconducibili alla personalità, primo fra tutti il diritto alla identità personale (par. 2). Di seguito, verranno esaminati ulteriori diritti non esclusivamente riconducibili a questa dimensione, quali il diritto alla riservatezza e alla *privacy* (par. 3), e il diritto alla protezione di dati personali (par. 4). L'analisi si sposterà su altri diritti fondamentali pertinenti al singolo individuo, ovvero la libertà personale (par. 5), e quelli che presentano una vocazione proiettata maggiormente verso la dimensione pubblica e collettiva, nella specie la libertà di riunione e di manifestazione del pensiero (par. 6). Da ultimo, verranno prese in considerazione le diverse accezioni dell'eguaglianza coinvolte, intesa qui come divieto di discriminazioni verso determinate categorie di persone (par. 7) e di tutela specifica nei confronti di soggetti in particolari condizioni di bisogno (par. 8).

In assenza di una normativa tesa a disciplinare direttamente le TRF, e a fronte della scarsità del dato giuridico riferibile anche solo per analogia a queste tecnologie, nel Capitolo III l'indagine si sposterà sulla normativa attualmente vigente dalla quale ricavare un inquadramento giuridico più organico sulle TRF, anche in grado, per un verso, di intercettare alcune delle problematiche più spinose che queste tecnologie pongono e, per l'altro, di misurarsi trasversalmente con le limitazioni ai diritti fondamentali richiamati sopra. L'attenzione verrà quindi rivolta alla disciplina sul trattamento dei dati personali, offerta dai molteplici livelli di governo coinvolti (par. 2), per esplicitarne

l'efficacia e verificarne le insufficienze al cospetto di tecnologie che, sotto molti aspetti, ne pongono in crisi i fondamenti e ne eludono le garanzie.

Inizialmente occorrerà misurarsi con la nozione di dati biometrici, cui dovrebbe essere ricondotta la tipologia di dati tipicamente processati dalle TRF. Già dai limiti di questa nozione emergeranno alcune criticità di fondo nell'impianto dell'intera disciplina (par. 3).

Ulteriormente, si indagheranno i fattori che offrono un fondamento giuridico al trattamento dei dati mediante riconoscimento facciale (par. 4). Si sottolineeranno, in particolare, le carenze dell'istituto del consenso esplicito (par. 4.1) e il regime previsto in presenza di interessi pubblici (par. 4.2), per affermare, da una parte, la necessità di un intervento legislativo specificatamente rivolto alle applicazioni di queste tecnologie, e, dall'altra, stabilire una base normativa adeguata a circostanziare le limitazioni ai diritti fondamentali nel rispetto del principio di proporzionalità (par. 4.3).

Di seguito verranno messi alla prova gli ulteriori principi a presidio della protezione dei dati personali (par. 5). Il riconoscimento facciale, in particolare, fa emergere le problematicità in punto di rispetto dei principi di limitazione delle finalità del trattamento (par. 5.1), minimizzazione dei dati impiegati (par. 5.2), conservazione degli stessi (par. 5.3).

La protezione dei dati viene integrata anche da una serie di diritti attribuiti all'interessato, da esercitare a seguito di sottoposizione a riconoscimento facciale (par. 6): si tratta, nello specifico, del diritto ad acquisire consapevolezza del trattamento (par. 6.1) ed esprimere una autodeterminazione sui propri dati (par. 6.2); ottenere tutela nei confronti di quelle decisioni algoritmiche in grado di massimizzare il potere di sorveglianza del riconoscimento facciale, ovvero le decisioni completamente automatizzate (par. 6.3) e le pratiche di profilazione (par. 6.4); aprire le c.d. *black box* entro cui vengono celati i meccanismi algoritmici e poterne comprendere il funzionamento (par. 6.5). Occorrerà verificare, inoltre, in che termini il riconoscimento facciale possa essere falsato e reso meno accurato da parte delle distorsioni (c.d. *bias*) destinate a produrre effetti, per lo più discriminatori, nei confronti dei soggetti sottoposti a riconoscimento, e in che modo il diritto riesca ad accordare rimedio o prevenire tali fenomeni (par. 7). Infine, si darà conto di come i principali capisaldi della tutela dei dati

personali abbiano trovato recente applicazione in un contenzioso giurisdizionale che – nella scarsità di casi verificatisi finora – ha messo in luce i complessi equilibri e i bilanciamenti in gioco nella disciplina delle TRF (par. 8), fornendo spunti rilevanti anche per giudicare lo stato dell'arte nel nostro ordinamento e, in particolare, l'impiego da parte delle forze dell'ordine del sistema S.A.R.I. (par. 9).

Nel Capitolo IV si darà conto di come il complesso di principi e diritti appena ricostruiti operino in concreto in quella che può essere definita la prossima frontiera di sviluppo delle TRF, ovvero i sistemi di informazione centralizzati gestiti a livello europeo. Tali sistemi sono destinati a strutturare stabilmente l'impiego delle TRF nei Paesi membri dell'UE e, nel prossimo futuro, cambieranno il modo stesso di intendere la tutela dei dati personali.

In assenza di una disciplina esplicitamente riferita alle TRF, e verificati i limiti della normativa attualmente in vigore, nel Capitolo V l'analisi si sposterà specificatamente sul piano della regolamentazione giuridica, per indagare quali siano gli strumenti normativi idonei a offrire una disciplina alle tecnologie in questione e regolare quindi le interferenze sui diritti fondamentali sopra descritte.

A questo scopo, si guarderà alle risposte offerte dagli ordinamenti in cui queste tecnologie trovano impiego e alla prassi sorta in esito ai tentativi di regolazione. La convinzione maturata è che, se la volontà non è solamente quella di bandire l'uso delle TRF, allora non sia sufficiente formulare una disciplina in termini puramente sanzionatori e interdittivi (par. 1). Attingendo al più ampio strumentario della "*regulation*", si cercherà di ipotizzare la necessità di combinare differenti tecniche regolatorie per esprimere un diverso approccio: si fa riferimento alla c.d. "regolazione del rischio" (par. 2), l'auto-regolazione (par. 3), la co-regolazione (par. 4), la valenza normativa assunta dal *design* dei sistemi tecnologici (par. 5), e alcune delle forme con cui venire incontro alle esigenze di flessibilità richieste alla normazione giuridica, quali le tecniche di sperimentazione regolativa (par. 6.1) e la *soft law* (par. 6.2). Le diverse combinazioni che ne possono derivate, tuttavia, non devono prescindere dalla cornice regolatoria offerta dalle norme giuridiche, chiamate ad assolvere specifiche funzioni (par. 7).

In conclusione verranno svolte alcune considerazioni di sintesi sul percorso affrontato.

CAPITOLO I

RICONOSCIMENTO FACCIALE: TECNOLOGIE E PROBLEMATICHE INNOVATIVE

SOMMARIO: 1. Considerazioni introduttive: i caratteri propri delle TRF. – 2. Come funzionano le TRF. – 3. Riconoscimento facciale e problematiche specifiche. – 3.1. La pretesa di "leggere" le emozioni: IA e algoritmi. – 3.2. Le inferenze dai tratti somatici alle intimità della psiche: *big data*. – 3.3. Un modo nuovo e incomprensibile di riconoscere i volti: *machine learning*.

1. *Considerazioni introduttive: i caratteri propri delle TRF*

La panoramica introduttiva ha dato conto della crescente diffusione delle TRF e ha lasciato intravedere come questi strumenti di sorveglianza – che ne siamo consapevoli o meno – riescano a sollevare seri pericoli che i legislatori pare non siano ancora pronti a fronteggiare. Prima di sviluppare l'analisi sul piano propriamente giuridico, però, occorre stabilire cosa si intenda per TRF.

A questo scopo, si cercherà innanzitutto di chiarire più da vicino quale sia il funzionamento di queste tecnologie, ovvero il procedimento entro cui si sviluppa il riconoscimento facciale, quali sono gli scopi cui tale riconoscimento è preordinato e in che modo tale procedimento sconti inevitabilmente un certo margine di errore nei suoi esiti finali.

Di seguito, per addentrarsi ulteriormente nelle peculiarità che qualificano il riconoscimento facciale, occorrerà rapportare queste tecnologie, in una sorta di relazione di *species* a *genus*, nel più ampio contesto dei sistemi di intelligenza artificiale, dei *big data* e del *machine learning*. Ciascuno di questi tre ambiti è strettamente interconnesso e le innovazioni a loro riconducibili costituiscono altrettanti fattori che hanno contribuito al rapido sviluppo delle TRF. Questa operazione deduttiva consentirà di mettere in luce certe connotazioni ideologiche e alcuni rischi nell'impiego di questi strumenti con cui anche il diritto deve misurarsi per risultare efficace.

2. *Come funzionano le TRF*

Il riconoscimento facciale consiste nel trattamento automatizzato di immagini digitali che contengono volti di persone, per il perseguimento delle più molteplici utilità. A livello tecnico, tuttavia, il riconoscimento facciale si sviluppa lungo un procedimento preordinato a sua volta al raggiungimento di alcune finalità determinate.

Cominciando da questo procedimento, pur nella diversità e complessità degli algoritmi che possono animare il riconoscimento facciale, sembra possibile comunque distinguere, con una certa approssimazione e semplificazione, la seguente sequenza di fasi[1].

a) *Acquisizione dell'immagine*: è la rappresentazione e conversione in formato digitale del volto di una persona, tramite ad esempio una fotografia o una registrazione video. L'acquisizione può avvenire volontariamente e in ambiente controllato (c.d. sistemi biometrici interattivi), come accade per le fototessere o le foto segnaletiche; oppure involontariamente e in ambienti non controllati (c.d. sistemi biometrici passivi), come accade con le videocamere a circuito chiuso ad ampio spettro che riprendono "dal vivo" in un ambiente chiuso o all'aperto. Da queste modalità e dalle conseguenze sulla qualità delle immagini dipendono molto le prestazioni del software di riconoscimento[2].

b) *Individuazione di un volto*: è il momento in cui si distingue e si isola, all'interno dell'immagine, la presenza di un volto rispetto allo sfondo; operazione che può essere molto complessa soprattutto nei sistemi biometrici passivi.

c) *Normalizzazione*: è il processo di attenuazione delle variazioni all'interno delle regioni del volto a causa, ad esempio, della posizione o dell'illuminazione: tali tecniche possono consistere nella conversione a una dimensione standard, la rotazione o l'allineamento delle distribuzioni del colore. In questa fase, inoltre, possono essere individuati i

[1] U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, cit., 5 ss.; E. LEARNED-MILLER, V. ORDÓÑEZ, J. MORGENSTERN, J. BUOLAMWINI, *Facial Recognition Technologies in the Wild: A Primer*, cit., 9 ss.; S.Z. LI, A.K. JAIN, *Introduction*, cit., 3 ss.

[2] Per questa distinzione, v. anche GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee-guida in materia di riconoscimenti biometrico e firma grafometrica. Allegato A al Provvedimento del Garante del 23 novembre 2014*, 12 novembre 2014, 6.

punti di riferimento (c.d. *landmarks*) corrispondenti a elementi tipici del volto, quali occhi, naso, bocca, contorno facciale.

d) *Estrazione delle caratteristiche*: è il processo finalizzato a isolare ed estrarre le c.d. caratteristiche biometriche distintive e riproducibili dell'immagine digitale del volto di una persona. L'estrazione delle caratteristiche può essere *olistica*, intesa come rappresentazione matematica dell'intera immagine facciale, come risulta dall'analisi dei suoi principali componenti; o basata sui singoli *tratti biometrici*, quale rappresentazione digitalizzata solamente di alcune specifiche caratteristiche localizzate del volto; o una combinazione dei due metodi (metodo di estrazione ibrido delle caratteristiche)[3]. L'insieme delle caratteristiche essenziali viene convertito in una immagine vettoriale chiamata "modello biometrico di riferimento" (c.d. *template* biometrico) – analogamente a quanto avviene, ad esempio, per le impronte digitali – che verrà impiegato in un successivo momento per il confronto con altri *template* biometrici, senza dover necessariamente processare i dati "grezzi" da cui è stato estratto[4].

e) *Registrazione*: è la conservazione dell'immagine o del modello biometrico, che vanno a popolare una "galleria" (solitamente nel caso delle immagini) o vengono archiviati all'interno di *database* ai fini di un successivo confronto.

f) *Confronto*: è il processo che misura le somiglianze tra le caratteristiche o i tratti biometrici di un modello di riferimento con altri modelli di riferimento già registrati nel sistema.

Fin qui ci si trova nell'ambito della "*analisi facciale*", un concetto ombrello che racchiude quelle tecniche di elaborazione delle immagini, ma che non implica l'identificazione in senso stretto della persona interessata[5]. Rientrano ancora nell'analisi facciale, inoltre, le tecniche con cui è possibile procedere ad una classificazione dei singoli attributi facciali, ove cioè si vanno ad analizzare elementi distinguibili in diverse

[3] GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile*, cit., 2.

[4] Cfr. GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, WP193, 27 aprile 2012.

[5] U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, cit., 7.

categorie *qualitative* (come genere, razza o provenienza etnica), ovvero classificabili tramite una *stima* allorché siano meglio rappresentabili con un numero (come l'età), ovvero grazie ai quali è operabile una classificazione in base alla *espressione facciale*, come sorrisi, pose corrucciate, sguardi arrabbiati[6].

Per comprendere l'utilità del procedimento di riconoscimento facciale, tuttavia, occorre indagare le finalità con le quali viene operato il confronto, ovvero la verifica/autenticazione, l'identificazione e la categorizzazione; ciascuno dei quali – come si vedrà – sollevano problematiche giuridiche differenti, soprattutto in termini di limitazione dei diritti fondamentali[7].

I) *Verifica/Autenticazione*: è il caso della c.d. comparazione uno-a-uno, che può avvenire in una duplice modalità[8]. Nella prima, il sistema è chiamato a verificare se l'immagine acquisita corrisponda a quella riferibile ad una persona già conosciuta e individuata, anche attraverso la presentazione di un documento di identità (verifica). Questa modalità di verificazione comincia ad essere diffusa negli aeroporti, ove si confronta l'immagine dei passeggeri e la fotografia sul passaporto, o il *template* biometrico contenuto nel chip, per stabilire una corrispondenza e conseguentemente l'identità personale[9]. Nella seconda modalità, il sistema si limita a verificare se l'immagine catturata ritragga la stessa persona raffigurata in un'altra immagine, senza conoscere l'identità della persona in questione o dandola per presupposta (autenticazione). È il caso, ad esempio, in cui il riconoscimento facciale è utilizzato al posto dei dati alfanumerici di *login/password* che si immettono per accedere ad un dispositivo o servizio, oppure per sbloccare un comune *smartphone*[10].

[6] E. LEARNED-MILLER, V. ORDÓÑEZ, J. MORGENSTERN, J. BUOLAMWINI, *Facial Recognition Technologies in the Wild: A Primer*, cit., 4 s.

[7] GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile*, cit., 2. Si consideri come nel precedente documento del 2003 la finalità della categorizzazione non veniva indicata, a riprova della evoluzione della tecnologia nel settore.

[8] E. LEARNED-MILLER, V. ORDÓÑEZ, J. MORGENSTERN, J. BUOLAMWINI, *Facial Recognition Technologies in the Wild: A Primer*, cit., 6.

[9] FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27 November 2019, 7.

[10] GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile*, cit., 3.

II) *Identificazione*: è il caso della comparazione uno-a-molti, in cui ci si interroga sull'identità del soggetto la cui immagine facciale viene acquisita, tramite il confronto con le immagini di altre persone raccolte in una galleria, o più spesso dei modelli biometrici all'interno di un *database*, alla ricerca di una possibile corrispondenza[11]. È una tecnica impiegata, ad esempio, per identificare le persone che lavorano in uno specifico luogo o per rintracciare una persona ricercata dalle forze dell'ordine[12]. È questa la finalità che si considera più tipica delle TRF.

III) *Categorizzazione*: consistente nell'estrarre le caratteristiche dall'immagine di una persona (conosciuta o meno) al fine di classificarla in una o più categorie in base agli attributi indicati sopra (ad esempio, a età, sesso, abitudini di consumo, ecc.). In questo caso, non è necessario che un sistema di categorizzazione disponga di un processo di registrazione. Un esempio di categorizzazione è offerto dalle *console* di gioco che impiegano un sistema di controllo gestuale che individua i movimenti dell'utilizzatore. La telecamera condivide le immagini con un sistema di riconoscimento facciale che suggerisce l'età probabile, il sesso e l'umore del giocatore[13]. La categorizzazione, dunque, non implica che le TRF siano utilizzate per identificare i singoli individui, ma solo per estrarre una o più caratteristiche da impiegare nei più svariati modi.

Da ultimo, bisogna sempre tenere a mente che le TRF compiono valutazioni attraverso algoritmi che effettuano *calcoli probabilistici* circa la corrispondenza tra l'immagine di una persona e la sua presenza in un *database*. Il sistema, una volta lanciata una ricerca, restituisce un certo numero di risultati, la cui quantità può essere liberamente scelta, ordinati in base alla probabilità che la persona interessata possa essere o meno ricompresa. Il riconoscimento facciale, dunque, non avviene mai con esattezza, ma è sempre associato ad una percentuale variabile di *errore*.

Tra gli elementi che influenzano tale percentuale vi è la qualità e la risoluzione dell'immagine[14], il riflesso della luce, il movimento della

[11] *Ivi*, 7.

[12] GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile*, cit., 3.

[13] *Ivi*, 4.

[14] Per la quale possono influire fattori come l'apertura del diaframma, il tempo di

persona ripresa, l'inclinazione e la posa del volto, ma anche l'età, il colore e le condizioni della pelle del soggetto, l'espressione, persino la pettinatura dei capelli o la presenza di trucco[15]. A condizionare molto il riconoscimento, inoltre, è anche – come anticipato – l'ambiente entro cui l'immagine viene acquisita, ovvero contesti controllati, come uffici di polizia o di frontiera, oppure ambienti in cui le condizioni di luce, distanza e posizione della persona non sono sotto controllo.

Un errore potrà determinare un *falso-positivo*, nel quale il sistema ritiene erroneamente che vi sia una corrispondenza con una immagine presente nella galleria, permettendo così ad un estraneo di accedere ad un determinato ambiente (in caso di verifica), o facendo scattare un controllo di polizia sulla persona sbagliata (in caso di identificazione); oppure potrà originare un *falso-negativo*, nel quale il sistema ritiene erroneamente che non vi sia una corrispondenza con una immagine presente nella galleria, impedendo così al proprietario di accedere al proprio *smartphone* (in caso di verifica), o consentendo ad una persona pericolosa di superare i controlli ad un valico di frontiera (in caso di identificazione).

Tra falsi-positivi e falsi-negativi tende ad esservi un *trade-off*, in relazione ad una soglia che definisce la sensibilità del sistema. Per cui, più alta è questa soglia e maggiore la sensibilità del sistema, minore sarà il tasso di falsi-positivi (perché l'algoritmo, in ipotesi, tenderà a verificare che ci sia una più esatta coincidenza tra le immagini), ma maggiore sarà il tasso di falsi-negativi (perché, in ipotesi, pur essendo le immagini raffiguranti la stessa persona, la diversità nelle rappresentazioni impedisce al sistema di ravvisare una coincidenza); e viceversa[16]. Per questo, a seconda di come si imposta tale soglia di sensibilità, lo stesso sistema avrà un rendimento differente.

esposizione, le aberrazioni, la capacità di risposta dei sensori digitali; cfr. S.Z. LI, A.K. JAIN, *Introduction*, 7.

[15] C. GARVIE, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, in *Georgetown Law, Center on Privacy and Technology*, 16 maggio 2019 [bit.ly/3dyZjJT].

[16] FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., 9; E. LEARNED-MILLER, V. ORDÓÑEZ, J. MORGENSTERN, J. BUOLAMWINI, *Facial Recognition Technologies in the Wild: A Primer*, cit., 11. Per questo si è soliti considerare congiuntamente falsi-positivi e falsi-negativi e valutare un sistema tenendo ferma una delle due soglie: ad esempio, la soglia di falsi-negativi viene rapportata ad una soglia fissa di falsi-positivi dell'1%.

Attualmente sono stati sviluppati algoritmi altamente performanti e sofisticati che, con immagini di buona qualità, consentono di identificare un soggetto la cui immagine è acquisita in ambienti controllati con un tasso di errore dello 0,1% nel confronto con gallerie di decine di milioni di immagini[17]. Tuttavia, non è possibile rispondere in termini assoluti e astratti alla domanda su quanto sia "accurato" o "adatto" un sistema di riconoscimento facciale. In questa valutazione intervengono diverse variabili su cui parametrare il tasso di errore accettabile, a partire dal contesto o le finalità del riconoscimento – ad es. nell'uso a scopi di marketing sarà accettabile un tasso di errore maggiore rispetto all'uso nel corso di indagini penali, ma in quest'ultimo caso occorre domandarsi se sia più accettabile collocare la soglia di sensibilità più in alto o in basso. L'efficacia e l'accuratezza di un sistema potrà variare in base alle caratteristiche somatiche dei soggetti da riconoscere, se diversificate o troppo simili[18] (i gemelli, allo stato attuale della tecnologia, sono sempre destinati a trarre il sistema in inganno[19]), oppure dei soggetti le cui immagini popolano le gallerie o addirittura – come si vedrà meglio – delle immagini prese in considerazione al momento della costruzione degli algoritmi[20].

[17] Si riporta in P. GROTHER, M. NGAN, K. HANAOKA, *Face Recognition Vendor Test (FRVT). Part 2: Identification*, NIST, dicembre 2020, 4, come certi algoritmi altamente performanti compiano adesso errori con una soglia inferiore al 0.1% confrontando immagini di buona qualità con gallerie contenenti le foto di 12 milioni di persone. Si riporta in J. GALBALLY, P. FERRARA, R. HARAKSIM, A. PSYLLOS, L. BESLAY, *Study on Face Identification Technology for its Implementation in the Schengen Information System*, JRC-34751, luglio 2019, 67, come l'identificazione in ambienti non controllati possa però arrivare anche ad un tasso di errore del 2,8% in presenza di soglie di sensibilità alte.

[18] V. i dati citati in P. GROTHER, M. NGAN, K. HANAOKA, *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*, NIST, dicembre 2019, per comprendere come i moderni sistemi di riconoscimento facciale, testati con una galleria di immagini di persone diversificate per provenienza e età, riescano a produrre 1 falso-positivo su 10.000 verifiche, ma utilizzando immagini di persone omogenee per età e provenienza, la percentuale salga anche di 20 volte.

[19] J. GALBALLY, P. FERRARA, R. HARAKSIM, A. PSYLLOS, L. BESLAY, *Study on Face Identification Technology for its Implementation in the Schengen Information System*, cit., 58.

[20] È il problema dei dati con cui vengono "allenati" gli algoritmi, su cui v. *infra* Cap. III, par. 7.

3. *Riconoscimento facciale e problematiche specifiche*

3.1. *La pretesa di "leggere" le emozioni: IA e algoritmi*

A partire dagli anni '70 del XX° secolo, la branca della "visione computazionale" ha cominciato a specializzarsi all'interno del più ampio settore dell'IA, acquisendo una propria identità quale ambito dell'informatica che si occupa della estrazione di informazioni dalle immagini, secondo proprie metodologie, paradigmi e problematiche[21]. La crescente disponibilità e lo sviluppo di mezzi, strumenti e risorse ha creato un enorme interesse nella capacità di elaborazione delle immagini per le più varie applicazioni, dando così slancio allo studio specializzato del riconoscimento facciale[22].

Alla base della crescente diffusione delle TRF vi è una evoluzione tecnologica che sta seguendo un incremento esponenziale, secondo quanto ipotizzato dalla c.d. legge di Moore[23]. Nell'ultimo ventennio, fattori come l'accesso a tecnologie a basso costo, lo sfruttamento di un enorme potere computazionale robusto, l'elaborazione di algoritmi sempre più sofisticati e, soprattutto, la disponibilità di enormi quantità di dati (c.d. *big data*), specie personali, hanno impresso una accelerazione impressionante nella ricerca e sviluppo delle TRF e, più in generale, dei sistemi di IA[24].

Nonostante le peculiarità sviluppate, le TRF possono ancora collocarsi per molti aspetti all'interno del settore dell'IA. Questa contestua-

[21] A. FUSIELLO, *Visione computazionale: Tecniche di ricostruzione tridimensionale*, FrancoAngeli, Milano, 2018, 17 ss.

[22] S.Z. LI, A.K. JAIN, *Introduction*, cit., 1.

[23] La c.d. legge di Moore, formulata pubblicamente da Gordon Moore nel 1974, afferma che la complessità dei microcircuiti (ad es., misurata dal numero di transistori per chip o per area unitaria) raddoppia periodicamente, con un periodo originalmente previsto in 12 mesi, allungato a 2 anni verso la fine degli anni Settanta e dall'inizio degli anni Ottanta assestatosi sui 18 mesi; cfr. B. RICCÒ, *Legge di Moore*, in *Enciclopedia della Scienza e della Tecnica*, 2008. Tale legge è riferibile alla capacità di calcolo nel suo complesso, come ricorda M. TEGMARK, *Vita 3.0. Essere umani nell'era dell'intelligenza artificiale*, Raffaello Cortina Editore, Milano, 2018, 97.

[24] M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges*, in M. EBERS, S. NAVAS NAVARRO (a cura di), *Algorithms and Law*, Cambridge University Press, Cambridge, 2020, 61.

lizzazione offre una prospettiva che – come detto – non solo aiuta a comprendere come funzionano le TRF, ma contribuisce ad evidenziare meglio la portata di una certa "ideologia tecnicista"[25] dal quale neppure queste ultime sfuggono.

Senza voler entrare nel dibattito scientifico specialistico che da sempre si misura con il problema definitorio[26], basti qui considerare come *intelligenza artificiale* la capacità che i software o le macchine possiedono di realizzare un determinato obiettivo con un certo grado di autonomia, percependo l'ambiente circostante e decidendo le migliori azioni per raggiungere i risultati prefissati[27].

Sempre da un punto di vista tecnico, i processi "mentali" che muovono l'IA sono determinati dagli *algoritmi*, ovvero – grossomodo – quelle sequenze di istruzioni che dicono a una macchina o ad un software, in maniera precisa e univoca, quali operazioni effettuare per ottenere un determinato risultato[28].

[25] Per una critica alla filosofia scientifica contemporanea che ha indotto una separazione tra la realtà, scientificamente e oggettivamente misurabile, e ogni scopo inerente, quale puro ideale o valore giudicato irrazionale, non oggettivo, in quanto non dimostrabile scientificamente, cfr. H. MARCUSE, *L'uomo a una dimensione. L'ideologia della società industriale avanzata*, Einaudi, Torino, 1974, spec. 158 ss., nell'ambito della nota analisi sulla razionalità tecnologica della civiltà industriale avanzata e sulla relativa tendenza totalitaria a sostituire i bisogni sociali con i bisogni individuali e assorbire così l'individualità personale attraverso la strumentalizzazione e l'omologazione.

[26] Basti rinviare al principale manuale introduttivo allo studio dell'IA, ove si fornisce un set di definizioni di IA, a seconda se riferite al pensiero o al comportamento umano e al pensiero o al comportamento razionale (delle macchine); cfr. S.J. RUSSELL, P. NORVIG, *Intelligenza artificiale. Un approccio moderno*, I, Pearson Prentice Hall, Milano-Torino, 2010, 4 ss.

[27] L'IA è stata recentemente definita come «software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal»; cfr. HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, *A definition of AI: main capabilities and disciplines*, aprile 2019. A partire da questa definizione, si consideri anche la tassonomia sviluppata nella prospettiva di "policy, research and industry" in EUROPEAN COMMISSION, JRC, *AI Watch. Defining Artificial Intelligence*, 2020, ove si riporta un'ampia *review* delle definizioni date a livello scientifico e istituzionale.

[28] Cfr. P. DOURISH, *Algorithms and their others: Algorithmic culture in context*, in

Ai limitati fini del presente discorso, merita ricordare che già John McCarthy – colui che negli anni '50 si ritiene abbia coniato il termine stesso "intelligenza artificiale" – metteva in luce come "non ci sia una definizione solida di IA che non sia messa in relazione con l'intelligenza umana", poiché "non possiamo descrivere in generale che tipo di procedure computazionali possiamo qualificare come intelligenti"[29]. Da sempre, dunque, si verifica una *tensione* tra intelligenza umana e intelligenza artificiale, nella quale la seconda cerca di emulare e rivaleggiare con la prima, allo scopo anche di superarla[30]. Non interessa qui stabilire se tale sorpasso sia già avvenuto o meno, a fronte della diffusione capillare che i sistemi di IA hanno oramai raggiunto nelle nostre vite quotidiane[31], quanto piuttosto sottolineare i rischi e le

Big Data & Society, 3, 2, 2016, 3 ss., ove si definisce, in termini generali, un algoritmo, come "descrizione formalizzata di una procedura computazionale", che si declina in vari significati in combinazione con altri concetti: algoritmo come "automazione"; algoritmo come "codice", seppur in attesa di essere operazionalizzato in un linguaggio di programmazione specifico; algoritmo come "architettura", se si guarda alla sua distribuzione in componenti, moduli e sistemi più ampi; algoritmo come "materializzazione", che assume concretezza entro un sistema che lo rende operativo, come un qualsiasi hardware. Più ampiamente, v. anche C. TOFFALORI, C. BOLOGNA, *Algoritmi. Raccontare la matematica*, il Mulino, Bologna, 2015.

[29] J. MCCARTHY, *What is Artificial Intelligence?*, 12 novembre 2007 [stanford.io/3cRtYmv].

[30] L. ALEXANDRE, *La guerra delle intelligenze. Intelligenza artificiale* contro *intelligenza umana*, EDT, Torino, 2018.

[31] In effetti, non si tratta più solamente di macchine in grado di rivaleggiare con gli uomini in ambiti ristretti, come il gioco degli scacchi. L'IA si è diffusa capillarmente nelle vite di ogni singola persona e di ogni comunità, raggiungendo un grado di pervasività inimmaginabile, come evidenziato, con molti esempi concreti, in T. SCANTAMBURLO, A. CHARLESWORTH, N. CRISTIANINI, *Machine Decisions and Human Consequences*, in K. YEUNG, M. LODGE (a cura di), *Algorithmic Regulation*, Oxford University Press, 2019, 49 ss. Questa diffusione è tale da aver superato un punto di non ritorno, oltre il quale non possiamo più fare a meno di queste tecnologie; sottolinea A SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1, 2019, 69 ss., come questa "tendenza espansiva" della tecnologia ci catturi proprio a partire dalla sua forza pratica, rendendoci sempre più dipendenti dall'algoritmo. Una panoramica dei differenti settori interessati da questa diffusione è offerta in A. LONGO, G. SCORZA, *Intelligenza artificiale. L'impatto sulle nostre vite, diritti e libertà*, Mondadori, Milano, 2020, 141 ss.

distorsioni derivanti da una certa idea di intelligenza e di cognizione che questa diffusione porta con sé[32].

Si tratta di quell'approccio *riduzionista* che tende ad assimilare l'intelligenza umana e quella artificiale, riconducibile alla teoria della "cibernetica" formulata da Norbert Wiener negli anni '40, secondo la quale i meccanismi di comunicazione e di controllo nelle macchine e negli organismi viventi sarebbero sostanzialmente analoghi, e dunque riproducibili con schemi comuni di origine algoritmica[33].

Tuttavia, sul piano tecnico prima che etico-filosofico, vi è la consapevolezza delle enormi difficoltà nel ridurre la complessità e la dinamicità del pensiero umano a modelli computazionali[34]. Allo stato attuale della cibernetica e dell'IA, infatti, le macchine non possono raggiungere ancora alcune qualità dell'essere umano, prima fra tutte l'intuizione intellettuale, ovvero la capacità del pensiero di cogliere l'essenza di una cosa e il suo senso globale, indipendentemente dal procedimento logico di tipo dimostrativo adoperato[35]. L'uomo inoltre possiede qualità come coscienza, consapevolezza, creatività, cognizione, emozione, le quali costituiscono a loro volta l'essenza di una persona umana al cuore della sua dignità[36]; peraltro, non essendo ancora

[32] A. SANTOSUOSSO, *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Mondadori, Milano, 2020, 11 ss.

[33] Cfr. N. WIENER, *Cybernetics. Or Control and Communication in the Animal and the Machine*, MIT Press, Cambridge, 1948, richiamato di recente da A SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, cit., 65, e da P. MORO, *Macchine come noi. Natura e limiti della soggettività robotica*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, GFL, Milano, 2020, 48 ss.

[34] Cfr. M.A. BODEN, *L'Intelligenza Artificiale*, il Mulino, Bologna, 2019, 119 ss. Ciò non esclude l'esistenza di progetti riccamente finanziati volti a simulare il funzionamento completo del cervello umano attraverso l'uso di supercomputer – come ad esempio lo "*Human Brain Project*" in UE; cfr. https://www.humanbrainproject.eu/en/

[35] P. MORO, *Macchine come noi*, cit., 51 ss.

[36] «Per parafrasare il Vangelo di Giovanni, il Verbo si è fatto macchina, lo spirito soffia anche nell'inorganico e la ragione e il linguaggio, oggettivati in forma di algoritmo, abitano in corpi non umani»; così R. BODEI, *Dominio e sottomissione. Schiavi, animali, macchine, Intelligenza Artificiale*, il Mulino, Bologna, 2019, 297, cui si rinvia per una analisi, «senza cadere nel catastrofismo o nel feticismo tecnologico» (*ivi*, 299), sulla irriducibilità dell'essere umano alla macchina, a partire dai limiti dei «pensieri ciechi» formulati da Leibniz, ossia l'idea che si possa pensare senza avere coscienza dei

pienamente comprensibili all'uomo e non potendo essere ricondotte a singoli stati biologici, non è neppure immaginare che si possano replicare e sostituire con componenti artificiali[37].

Volendo quindi stabilire una analogia tra stato mentale e logica delle macchine, è possibile collocarsi solamente sul piano della accettabilità dei risultati e non della identità delle procedure di ragionamento e di decisione[38].

Quanto detto vale anche, e soprattutto, per le TRF. I computer "vedono" le immagini e riconoscono le facce in termini profondamente differenti rispetto agli esseri umani. A partire da un'immagine digitale espressa tramite una griglia di pixel, ovvero righe e colonne di numeri indicativi di intensità di colore e di luminosità, un software rintraccia schemi che *verosimilmente* indicano la presenza di elementi facciali. Siamo ben lontani dallo stato di consapevolezza della presenza di un volto e di intuizione di quanto esso vuole esprimere. Nonostante ciò, la ricerca nel campo delle TRF si sta muovendo verso obiettivi che tendono a riprodurre i risultati di questo stato, come emerge paradigmaticamente in quelle implementazioni del riconoscimento facciale che si dichiarano in grado di rilevare e decifrare le *emozioni* di una persona.

Queste ultime sono tecniche di analisi delle emozioni (c.d. *affective computing*[39]) che possono essere impiegate in una molteplicità di ambiti: si pensi alla medicina e, ad esempio, alla possibilità di aiutare i bambini affetti da autismo a sviluppare capacità emotive; ma applicazioni sempre maggiori si ritrovano in ambito commerciale, per la rile-

significati e dei contenuti pensati, e degli equivoci con cui si può interpretare il «cogito ergo sum» di Cartesio, tagliando fuori dal "pensare" gli affetti o le sensazioni (spec. 309 ss.).

[37] Riporta invece J. KAPLAN, *Intelligenza artificiale Guida al futuro prossimo*, Luiss, Roma, 2017, 31, come questa aspirazione fosse ricorrente sin dalla genesi degli studi pioneristici dei citati John McCarthy e Norbert Wiener.

[38] P. MORO, *Macchine come noi*, cit., 54. Osserva inoltre R. CINGOLANI, *L'altra specie. Otto domande su noi e loro*, il Mulino, Bologna, 2019, 123, come sia possibile che un giorno si arrivi a progettare un algoritmo che riesca a simulare l'autocoscienza umana, ma certamente esso non avrà la stessa capacità di influenzare il comportamento di una macchina come la biochimica in senso lato fa con gli esseri umani.

[39] Cfr. R.V. PICARD, *Affective computing*, MIT Press, Cambridge, 1997.

vazione delle preferenze e delle risposte dei consumatori[40], e in settori ove vengono direttamente chiamati in causa altri diritti fondamentali, come nelle attività di polizia (si pensi alla pratica degli interrogatori), nelle assunzioni dei colloqui di lavoro, nella valutazione degli studenti[41]. Tutte ipotesi che, a ragione, suscitano serie preoccupazioni[42]. Le ricerche in questo ambito muovono dal presupposto, da una parte, che vi sia una corrispondenza biunivoca tra le manifestazioni esterne dell'espressione facciale e il proprio attuale stato emotivo e, dall'altra, che le TRF siano in grado di cogliere esattamente tutte le microespressioni del volto rilevanti e combinarle per ricostruire olisticamente lo stato emotivo[43].

La pretesa di guardare a queste tecnologie nella prospettiva riduzionista richiamata sopra, tuttavia, mostra tutta la sua fallacia nella misura in cui esclude dalla valutazione fattori come la comunicazione interattiva, la connessione empatica, la capacità di interpretazione dei sentimenti a partire dal senso comune o dalla sensibilità culturale, l'analisi del contesto[44].

Alcuni *Big tech* come Microsoft, IBM e Amazon hanno sviluppato nel tempo algoritmi di riconoscimento facciale che si basano su studi del linguaggio non verbale condotti negli anni '60 dallo psicologo Paul Ekman, che indicò sei emozioni come universali, identiche in tutto il mondo e chiaramente riconoscibili a prescindere dal contesto culturale: rabbia, disgusto, paura, felicità, tristezza e sorpresa[45]. Tuttavia, am-

[40] Cfr. G. LUGLI, M. RIANI (a cura di), *Espressioni ed impronte facciali nel marketing*, Giappichelli, Torino, 2018.

[41] Cfr. AI NOW INSTITUTE, *AI Now Report 2019*, dicembre 2019, 50 ss. Più approfonditamente, v. anche *infra* Cap. II, par. 7.

[42] Queste applicazioni dell'*affective recognition* «may pose risks of great concern»; cfr. CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on Facial Recognition*, T-PD(2020)03rev4, 28 gennaio 2021, 5.

[43] X. LI, ET AL., T*owards Reading Hidden Emotions: A comparative Study of Spontaneous Micro-expression Spotting and Recognition Methods*, in *arXiv:1511.00423v2 [cs.CV]*, 8 febbraio 2018.

[44] D. LESLIE, *Understanding bias in facial recognition technologies: an explainer*, cit., 32.

[45] Come riportato in AI NOW INSTITUTE, *AI Now Report 2018*, dicembre 2018, 14. I lavori di Elkman hanno consentito di sviluppare diversi approcci per codificare il comportamento, ovvero il "*message-based measurement*", in cui si guarda al significato

pi studi dimostrano come, in realtà, anche solo il modo con cui le persone comunicano emozioni apparentemente chiare nei sei stati appena richiamati varia considerevolmente tra culture, situazioni e persino tra le singole persone nelle diverse circostanze. Allo stesso tempo, configurazioni simili delle espressioni facciali possono variabilmente esprimere una o più emozioni complesse[46].

Da qui la proposta di sviluppare TRF variabili in base al contesto e a specifici usi[47], o addirittura di riuscire a misurare le emozioni di un soggetto prescindendo dalle espressioni facciali o corporee e basandosi unicamente su inferenze a partire dal contesto stesso[48]. Si tratta comunque di tentativi *in fieri* che non distolgono da un punto fondamentale: non è possibile trascurare la distanza che intercorre tra i freddi calcoli computazionali, che consentono di rintracciare schemi numerici ricorrenti etichettandoli come "emozioni", e la concreta dinamica interpersonale e interattiva che genera una esperienza umana condivisa[49]. Questa irriducibilità dell'essere umano nei confronti delle macchine è un punto da tenere presente nel corso di tutta la trattazione e che riemergerà, in particolare, al momento di definire i diritti e le pretese che l'essere umano può avanzare nei confronti di decisioni assunte tramite queste tecnologie.

veicolato tramite l'espressione facciale secondo le emozioni descritte nel testo, o il "sign-based *measurement*", in cui si scompone il volto in unità anatomiche. Vi poi il "*dimensional measurement*", che ordina le emozioni su due assi, ovvero gradevolezza-sgradevolezza e eccitazione-sonnolenza. Per una ricostruzione dei diversi approcci, cfr. J.F. COHN, F. DE LA TORRE, *Automated Face Analysis for Affective Computing*, in R.A. CALVO, S.K. D'MELLO, J. GRATCH, A. KAPPAS (a cura di), *The Oxford Handbook of Affective Computing*, OUP, Oxford, 211 ss.

[46] L.F. BARRETT ET AL., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, in *Psychological Science in the Public Interest*, 20, 1, 2019, spec. 46 ss.

[47] Cfr. C. GIFFORD, *The Problem with Emotion-Detection Technology*, in *TheNewEconomy.com*, 15 giugno 2020 [bit.ly/3mvtqWz].

[48] Z. CHEN, D. WHITNEY, *Tracking the Affective State of Unseen Persons*, *Proceedings of the National Academy of Sciences*, 116, 15, 2019, 7559 ss., che propongono di sviluppare una metodologia denominata "*affective tracking*" che prescinda dalle espressioni facciali e corporee, le cui immagini sono giudicate statiche e innaturali.

[49] D. LESLIE, *Understanding bias in facial recognition technologies: an explainer*, cit., 33.

3.2. *Le inferenze dai tratti somatici alle intimità della psiche:* big data

Come anticipato, tra i fattori che di recente hanno consentito un balzo esponenziale nella ricerca e sviluppo delle TRF e, più in generale, dei sistemi di IA, vi è la disponibilità dei c.d. *big data*.

Con questo termine, oramai di uso comune, non si dà conto semplicemente di una quantità enorme di dati o di immagini da processare. Per offrire una descrizione più appropriata si è soliti fare riferimento anche ad altre qualità, riconducibili alle famose tre "V"[50] corrispondenti al "volume" dei dati raccolti[51]; "varietà" delle fonti da cui vengono prodotti i dati; "velocità" di produzione e di analisi dei dati. È possibile aggiungere poi altre "V"[52], come la "veridicità" dei dati che può essere presumibilmente ottenuta grazie alle tecniche di analisi[53], ma soprattutto il "valore" che i *big data* sono oramai in grado di generare nella *digital economy*[54]. Si consideri solamente come Facebook abbia dichiarato di avere due miliardi di utenti al mese, i quali caricano 350 milioni di foto al giorno, potendo quindi usufruire di un rifornimento "praticamente infinito" di dati da elaborare e da cui ricavare un valore economico[55]. Grazie alla crescente disponibilità di dati, si

[50] D. LANEY, *3D data management: controlling data volume, velocity, and variety*, in *Technical report, META Group*, 2001 [gtnr.it/3dK0E0j].

[51] Per dare un'idea della mole in questione, basti notare che siamo oramai entrati nella "Zettabyte era", in cui il traffico di dati annuale si misura in grandezze come decine di Zettabyte, pari a 10^{21} bytes. A livello globale, mentre nel 2016 sono stati prodotti 6.8 Zb, le previsioni stimano che nel 2021 verranno prodotti 20.6 Zb annui; cfr. *Cisco Global Cloud Index: Forecast and Methodology, 2016–2021*, White Paper, [bit.ly/3wBIcQ7].

[52] Cfr. M.C. CARROZZA ET AL., *AI: profili tecnologici. Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'Intelligenza Artificiale*, in *BioLaw Journal*, 3, 2019, 241, che aggiungono la "variabilità", secondo cui il contenuto dei dati muta di significato a seconda dell'analisi a cui è sottoposto.

[53] S. SICULAR, *Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three "V"s*, in *Forbes*, 27 marzo 2013 [bit.ly/2PvmQn8].

[54] M. DELMASTRO, A. NICITA, *Big data*, il Mulino, Bologna, 2019, 26 ss.

[55] Cfr. J. BENNET, *Saving face: Facebook Wants Access Without Limits*, in *The Center for Public Integrity*, 1 agosto 2017 [bit.ly/39Q1Zlo]. Questa posizione di vantaggio è sottolineata anche da F. PAOLUCCI, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *MediaLaws*, 1, 2021, 2.

pensa che il mercato delle TRF sia destinato a raddoppiare nel corso dei prossimi anni[56].

Se poi si guarda alla dimensione dinamica con cui da "semplici" dati si passa a creare *big data*, è possibile identificare quella che viene chiamata la "catena di valore del dato", nella quale si distinguono le c.d. *big data analytics* e il c.d. *data mining*, attraverso cui avviene l'estrazione delle informazioni dai dati[57] e, dai dati esistenti, si generano nuovi dati rilevanti tramite la loro combinazione, aggregazione e scomposizione[58].

I *big data* e le tecniche di *analytics* non producono solamente enormi vantaggi in termini di minori costi, più ampia capacità e maggiore velocità di elaborazione delle informazioni[59]. Più in generale, grazie anche al crescente sviluppo dei sistemi di IA cui si è fatto rife-

[56] In U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, cit., 8, è riportato che tra il 2016 e il 2019 le TRF hanno generato un mercato globale di 3-5 miliardi di dollari, mentre tra il 2022 e il 2024 ci si aspetta un incremento pari a 7-10 miliardi di dollari.

[57] Si dà qui per presupposta la distinzione tra "dati", quali frammenti di informazione allo stato grezzo; "informazioni", costituite dall'organizzazione contestualizzata dei dati per veicolare un significato; "conoscenza", quale assimilazione delle informazioni e comprensione del modo in cui esse vanno utilizzate; cfr., fra tanti, C. HESS, E. OSTROM, *La conoscenza come bene comune. Dalla teoria alla pratica*, Mondadori, Milano, 2009, 9.

[58] M. DELMASTRO, A. NICITA, *Big data*, cit., 27 s. Più in particolare, in una prima fase di questa catena troviamo la fase di acquisizione dei dati, resa più diffusa e capillare – non sempre con la consapevolezza degli interessati – grazie al network di sensori integrati in dispositivi che elaborano autonomamente informazioni. Si tratta dell'universo dell'*Internet of Things* (*smartwatch*, *smart TV*, domotica, ecc.) e dell'*ubiquitous computing*, in cui ogni cosa e ogni persona è *online* e interconnessa ovunque tramite internet. La seconda fase è la preparazione e conservazione dei dati, prodromica al momento centrale delle analisi (*analytics*), che ricomprende l'esplorazione, la trasformazione e la modellazione in grado di estrarre informazioni e generare nuovi dati rilevanti (c.d. *data mining*). Ad essa è connesso anche lo stoccaggio dei dati e la loro conservazione, che avviene sempre più non in memorie fisiche, bensì in *clouds* virtuali che sfruttano volumi adeguati ai *big data*. Infine vi è lo sfruttamento dei risultati, in grado di generare valore economico e muovere la c.d. Industria 4.0.

[59] Cfr. C. ACCOTO, *Il mondo dato. Cinque brevi lezioni di filosofia digitale*, Egea, Milano, 2017, 38.

rimento, stiamo assistendo a profondi cambiamenti a livello economico, sociale e persino antropologico[60]. Al giorno d'oggi si ritiene che i dati siano divenuti la "nuova valuta"[61] dell'economia digitale. Secondo alcuni è in corso quella che viene definita come la progressiva "datificazione"[62] delle società, ovvero la quantificazione/conversione dei processi vitali in flussi di dati da elaborare tramite algoritmi e generare così altre informazioni per una molteplicità di scopi, molti dei quali lucrativi[63]. La diffusione di queste tecnologie starebbe inoltre cambiando il modo con cui l'essere umano si relaziona nel mondo, conosce, giudica e agisce entro di esso; addirittura, nel modo con cui percepisce se stesso[64].

Anche nel campo del riconoscimento facciale la possibilità di disporre di quantità enormi di immagini e di tecniche algoritmiche di analisi sempre più complesse ha profondamente mutato – come si vedrà nel prossimo paragrafo – queste tecnologie e il loro impatto sulla vita quotidiana[65]. A questo punto del discorso, tuttavia, si vuole mettere in luce un punto, molto rilevante per le TRF, che costituisce un portato fondamentale di questa diffusione dei *big data*, riassumibile come il passaggio dalla "*causazione*" alla "*correlazione*"[66].

[60] Cfr. A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal*, 1, 2019, 4.

[61] W.D. EGGERS, R. HAMILL, A. ALI, *Data as currency. Government's role in facilitating the exchange*, in *Deloitte Review*, 13, 2013, 19 ss.

[62] Cfr. V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data: A Revolution that will Transform How We Live, Work and Think*, John Murray, London, 2013, 154 ss.; C. SARRA, *Il mondo-dato. Saggi su datificazione e diritto*, Cleup, Padova, 2019, spec. 29 ss.; N. COULDRY, J. YU, *Deconstructing datafication's brave new world*, in *New media & society*, 2018, 1 ss.

[63] Osserva A. VESPIGNANI, *L'algoritmo e l'oracolo. Come la scienza predice il futuro e ci aiuta a cambiarlo*, Il Saggiatore, Milano, 2019, 52, come nel 1986 il 92% dei dati veniva immagazzinato in forma analogica, nel 2007 la cifra si è invertita, con il 94% delle informazioni custodite in digitale.

[64] A. PIRNI, A. CARNAVALE, *The challenge of regulating emerging technologies. A philosophical framework*, in E. PALMERINI, E. STRADELLA (a cura di), *Law and Technology. The Challenge of Regulating Technological Development*, PUP, Pisa, 2013, 59, che individuano proprio in quest'ultimo elemento il discrimine tra tecnologie moderne e nuove tecnologie.

[65] Cfr. A. VINAY ET AL., *Cloud Based Big Data Analytics Framework for Face Recognition in Social Networks using Machine Learning*, in *Procedia Computer Science*, 50, 2015, 623 ss.

[66] Cfr. N. SILVER, *The Signal and the Noise. Why So Many Predictions Fail – but*

Le *data analytics*, infatti, si fondano su tecniche di correlazione induttiva e di inferenza probabilistica che prescindono completamente dalla "comprensione" del dato processato. Invece di capire o spiegare il significato dei dati o il loro nesso causa-effetto, gli algoritmi sono in grado di scoprire schemi e correlazioni ricorrenti all'interno di enormi quantità di dati a partire dalla loro frequenza statistica. Basta dunque conoscere "cosa" e non "perché", con un approccio epistemologico che capovolge secoli di pratiche di conoscenza e sfida i metodi umani di comprensione su come assumere decisioni e comprendere la realtà[67]. Si è giunti persino a pronosticare la "fine della teoria", o l'obsolescenza dei metodi scientifici, dal momento che "con un numero sufficiente di dati, le cifre parlano da sole"[68].

Considerare solamente l'efficienza della correlazione, prescindendo completamente dal nesso causale, apre tuttavia ad un rischio che pare evidente nel caso delle TRF. Si tratta della possibilità che la correlazione arrivi a "*forzare*" i dati, cioè che vada a individuare nessi che non hanno necessariamente una ragion d'essere sul piano della causalità, ma solamente su di un piano puramente statistico[69]. Tanto più ciò può accadere in quelle ipotesi in cui i dati processati dagli algoritmi non sono dati direttamente riferibili ad un fenomeno, ma vengono utilizzati dati a loro volta prodotti da altri algoritmi, oppure dati vicarianti o indiretti (c.d. *proxy*).

Da questo punto di vista, le FRT possono essere usate – e addirittura ritenute più accurate degli esseri umani – per riconoscere una determinata caratteristica della persona o del comportamento, a prescin-

Some Don't, Penguin, New York, 2012, 185 ss., che riporta come esempio la previsione dei terremoti; V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data: A Revolution that will Transform How We Live, Work and Think*, cit., 6 ss. Più di recente v. M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges*, cit., 45; A. CELOTTO, *Come regolare gli algoritmi. Il difficile bilanciamento tra scienza, etica e diritto*, in *Analisi giuridica dell'Economia*, 1, 2019, 48.

[67] Cfr. V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data: A Revolution that will Transform How We Live, Work and Think*, cit., 7, che riassumono questo passaggio con "non knowing *why* but only *what*".

[68] C. ANDERSON, *The End of Theory: the Data Deluge Makes the Scientific Method Obsolete*, in *Wired Magazine*, 23 giugno 2008 [bit.ly/3fGoxZu].

[69] M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges*, cit., 45.

dere da ulteriori fattori di spiegazione acclarati e concorrenti. Il pericolo insito in un simile approccio, tuttavia, è quello di scivolare insidiosamente nei peggiori scenari rievocati dal determinismo antropologico di matrice lombrosiana[70].

Non a caso, i primi sviluppi delle TRF in questo senso sono stati preconizzati, tra l'altro, da quegli studi che asseriscono la precisa esistenza di una correlazione tra i tratti somatici e l'attitudine criminologica, ravvisando una macrodistinzione tra coloro che rispettano la legge, accomunati da un più ampio grado di rassomiglianza, e i criminali, distinguibili per un più elevato grado di differenza rispetto alle persone "normali"[71].

Analogamente, le TRF sarebbero in grado di inferire dai tratti somatici del volto l'orientamento sessuale di una persona, con una correttezza del 81% per gli uomini e il 71% per le donne[72].

Le più recenti ricerche si sono spinte anche nel valutare alcuni tratti della personalità, come scrupolosità o nevroticismo, con un tasso di successo variabile tra 79-88% in relazione a quanto autodichiarato dalle persone[73]; nonché le preferenze politiche (liberale/conservatore),

[70] Sull'orientamento antropometrico lombrosiano, secondo cui il delinquente è un tipo antropologico di individuo che, a causa di anomalie congenite e chiaramente distinguibili, sarebbe fatalmente portato al delitto, basti rinviare a F. MANTOVANI, *Il problema della criminalità. Compendio di scienze criminali*, Cedam, Padova, 1984, 99 s.

[71] X. WU, X. ZHANG, *Automated inference on criminality using face images*, in *arXiv:1611.04135v1 [cs.CV]*, 26 maggio 2017, che riportano i risultati di una ricerca condotta tramite l'impiego di *machine learning* supervisionato (v. prossimo par.) per elaborare 1.856 immagini di persone, metà delle quali condannate per reati.

[72] Y. WANG, M. KOSINSKI, *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images*, in *Journal of Personality and Social Psychology*, 114, 2, 2018, 246 ss. La ricerca è stata condotta tramite l'elaborazione di 35.326 immagini facciali tramite reti neurali profonde (v. prossimo par.). La percentuale di successo salirebbe rispettivamente a 91% e 83% se il sistema analizza 5 immagini di una persona. La ricerca muove dalla c.d. teoria dell'ormone prenatale, secondo cui vi sarebbe una relazione tra l'esposizione ormonale nella vita prenatale e l'orientamento sessuale; ma anche tale teoria è oggetto di ampie discussioni. Cfr. A.F. BOGAERT, M.N. SKORSKA, *A short review of biological research on the development of sexual orientation*, in *Hormones and Behavior*, 119, 2020.

[73] A. KACHUR ET AL., *Assessing the big five personality traits using real-life static facial images*, in *Nature Scientific Reports* 10, 2020, il cui studio è stato condotto sottoponendo 31.367 immagini appartenenti a 1.245 individui a reti neurali artificiali (v.

con un tasso di successo pari al 72% nell'analisi di coppie di immagini affiancate[74].

Numerose altre applicazioni sono in via di sviluppo, come ad esempio la creazione di moderni poligrafi in grado di stabilire dalle microespressioni facciali se una persona stia mentendo o meno[75]. Simili strumenti in futuro potranno essere messi a disposizione di studi legali, istituti bancari, compagnie assicurative, per effettuare test nei colloqui di assunzione o per tutelarsi contro tentativi di frode. Di recente, in ambito europeo, questi sistemi sono stati impiegati anche nei controlli agli aeroporti[76].

Al di là del problema sul "se" sia tecnicamente ed eticamente possibile inferire da una immagine facciale lo stato mentale, i tratti psicologico o aspetti intimi della personalità, occorre anche domandarsi "cosa" se ne vuol fare con i risultati del rilevamento. Tramite queste informazioni, infatti, è possibile, ad esempio, svolgere diagnosi mediche, predire i comportamenti, ma anche indirizzare le condotte tramite input persuasivi, sino a cercare di controllare e manipolare le emozioni[77].

prossimo par.) per valutare i c.d. "*Big Five personality traits*" (*agreeableness*, *conscientiousness*, *extraversion*, *neuroticism*, *openness*).

[74] M. KOSINSKI, *Facial recognition technology can expose political orientation from naturalistic facial images*, in *Scientific Reports*, 100, 2021, che ha predisposto lo studio a partire dalla elaborazione di 1.085.795 immagini di individui diversi, per stabilire una correlazione tra immagine del volto e appartenenza politica (liberale/conservatore), con un tasso di successo pari al 72% nell'analisi di coppie di immagini affiancate, con un risultato migliore del caso (50%) e dell'osservazione umana (55%).

[75] Cfr. J. BITTLE, *Lie detectors have always been suspect. AI has made the problem worse*, in *MIT Technology Review*, 13 marzo 2020.

[76] È accaduto con il progetto sperimentale iBorderCtrl, finanziato dall'UE tramite il programma Horizon 2020; cfr. D. DEAHL, *The EU Plans to Test an AI Lie Detector at Border Points*, in *The Verge*, 31 ottobre 2018 [bit.ly/3upzVgg]; N. LOMAS, *'Orwellian' AI lie detector project challenged in EU court*, in *Techcrunch*, 5 febbraio 2021 [tcrn.ch/2R4qrsv].

[77] Cfr. C. BURR, N. CRISTIANINI, *Can Machines Read our Minds?*, in *Minds and Machines*, 29, 3, 2019, 461 ss., cui si rinvia anche per ulteriori studi attraverso cui si combinano le tecniche di *machine learning* e valutazioni psicologiche in prospettiva psicometrica.

In definitiva, per quanto qui interessa maggiormente, il legame che si viene ad instaurare fra TRF e *big data* implica che le inferenze statistiche non siano sempre comprensibili o dimostrabili altrimenti, oltre a spalancare un panorama di nuove possibilità e pericoli sui possibili utilizzi a fini di sorveglianza delle informazioni così generate.

3.3. *Un modo nuovo e incomprensibile di riconoscere i volti:* machine learning

Si è già detto di come i computer "vedano" le immagini rintracciando schemi di pixel corrispondenti all'immagine di un volto. Nelle prime TRF questi schemi venivano stabiliti secondo un approccio *top-down*, in quanto definiti direttamente dall'uomo tramite la codificazione delle conoscenze comuni di caratteristiche e proprietà delle immagini facciali[78]. Queste metodologie aprivano a diversi problemi, a partire dalle inevitabili discrasie conseguenti alla traduzione in conoscenze matematiche del linguaggio naturale attraverso cui esprimere le molteplici diversità dei tipi facciali. Tali metodologie, inoltre, funzionavano bene quando le immagini venivano acquisite in scenari control-

[78] Per una ricognizione di questi primi studi pionieristici nel settore, v. S.Z. LI, A.K. JAIN, *Introduction*, cit., 1 ss.; J. GALBALLY, P. FERRARA, R. HARAKSIM, A. PSYLLOS, L. BESLAY, *Study on Face Identification Technology for its Implementation in the Schengen Information System*, cit., 29 ss.; K. GÜVEN, *Facial Recognition Technology: Lawfulness of Processing under the GDPR in Employment, Digital Signage and Retail Context*, Tilburg University, 2019, 8 ss., a partire dagli studi negli anni '70 di Goldstein, Harmon e Lesk, che per identificare automaticamente le facce elaborarono 21 marcatori individuali, oltre a tener conto dello spessore delle labbra e il colore dei capelli; agli studi sul finire degli anni '80 di Sirovich e Kirby, che iniziarono ad applicare l'algebra lineare al problema del riconoscimento facciale su immagini di piccole dimensioni, i quali consentirono negli anni '90 a Kanade, Turk e Pentland di affinare il c.d. "approccio Eigenface", basato sul confronto dell'immagine di una persona non nota con le caratteristiche (*eigenfaces*) estratte da altre immagini di persone note, ciascuna relativa, ad esempio, alla linea dei capelli, la simmetria, la larghezza del naso, o più spesso non corrispondenti a caratteristiche intelligibili della faccia. Con questo metodo si dimostrò la possibilità di realizzare sistemi di riconoscimento delle facce che operino in tempo reale. Su questi passaggi, v. anche Y. MING-HSUAN, D. J. KRIEGMAN, N. AHUJA, *Detecting Faces in Images: A Survey*, in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24, 1, 2002, 34 ss.

lati, con soggetti ripresi frontalmente e in condizioni ottimali di luce, posizionamento o espressione.

Nell'ambito della richiamata evoluzione tecnologica nel settore dell'IA e in concomitanza alla diffusione dei *big data*, anche la *computer vision* ha vissuto un cambiamento di paradigma, con il passaggio dal vecchio approccio *top-down* ad uno definibile come *bottom-up*. Grazie a metodi a base statistica, non è più l'uomo che scrive gli algoritmi ad indicare quali sono le caratteristiche da estrare dall'immagine di un volto, ma sono gli algoritmi che vengono "*allenati*" per imparare da soli e ricavare, a partire da enormi *dataset* di immagini acquisite in condizioni anche non ottimali, le caratteristiche (c.d. *features*) dei volti che si ritengono più ricorrenti (nell'ordine di milioni); *a prescindere*, quindi, dall'intervento umano che "insegni" alla macchina cosa sia una faccia e come debbano essere distinte le singole parti di essa[79]. Questo passaggio è stato possibile grazie alla elaborazione di algoritmi di *machine learning*, o apprendimento automatico. Su questi ultimi occorre svolgere qualche chiarimento per esplicitare alcune conseguenze inerenti alle TRF.

Con il *machine learning* i computer non vengono più programmati in termini logico-deduttivi, nella sequenza: si pone un problema, lo si formalizza matematicamente, lo si traduce in un algoritmo. Le macchine, di conseguenza, non si limitano più a elaborare istruzioni, intese come regole predeterminate con condizioni fisse attraverso cui realizzare certi obiettivi in modi precisi[80]. Gli algoritmi, invece, imparano da

[79] Tra le prime tecniche ispirate a questo nuovo paradigma occorre segnalare il metodo "Viola-Jones" (cfr. P. VIOLA, M. JONES, *Rapid Object Detection Using a Boosted Cascade of Simple Features*, in *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2001, 511 ss.), che permette solamente di individuare il volto (c.d. *face detection*) e non di identificare una persona, ma che si rivela particolarmente robusto. Con questo metodo, in buona sostanza, spetta all'essere umano, nello scrivere l'algoritmo, specificare quali siano le caratteristiche "invarianti" da ricercare (c.d. *pattern*), ma sarà poi l'algoritmo a imparare da solo, grazie alle immagini con cui viene allenato, a ricercare autonomamente tali caratteristiche, a partire dai contorni che, ad esempio, distinguono lo stacco tra la linea degli occhi e la fronte, o quello che distingue il naso.

[80] A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Riv. Int. Fil. Dir.*, 8, 2019, 90 ss.

soli a svolgere il proprio compito a partire dai dati e dall'esperienza[81]. Più in particolare, questa tecnologia si basa sul riconoscimento di schemi (c.d. *patterns*), o sottoschemi, all'interno di dati non strutturati utilizzati per allenare (*training*) gli algoritmi, e sulla comparazione di nuovi dati con gli schemi riconosciuti in precedenza, allo scopo di rintracciare analoghe ricorrenze e riuscire addirittura a *predire* nuove correlazioni[82].

In alcune varianti, questa programmazione contempla l'intervento umano per aiutare a distinguere gli schemi, come nel caso dell'apprendimento supervisionato o in quello per rinforzo; in altri casi, è l'algoritmo che addirittura impara da solo a riconoscere questi *patterns*, come nell'apprendimento non supervisionato[83].

Anche da questo punto di vista, in continuità con quanto osservato sui *big data*, si sta diffondendo un approccio per cui non è dirimente avere dei modelli generativi per cercare di comprendere le relazioni causali di un fenomeno, ma è sufficiente avere moltissimi dati relativi al fenomeno stesso con cui allenare gli algoritmi per riuscire a fare delle predizioni statisticamente sempre più accurate[84].

[81] A. VESPIGNANI, *L'algoritmo e l'oracolo*, cit., 65 ss.; B. BUCHANAN, T. MILLER, *Machine Learning for Policymakers. What It Is and Why It Matters*, Harvard Kennedy School, Belfer Center for Science and International Affairs, Paper, giugno 2017.

[82] Analogamente, secondo M. VAN OTTERLO, *A machine learning view on profiling*, in M. HILDEBRANDT, K. DE VRIES (a cura di), *Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology*, Routledge, Abingdon, 2013, 46, con *machine learning* si può intendere «any methodology and set of techniques that can employ data to come up with novel patterns and knowledge, and generate models (e.g. profiles) that can be used for effective predictions about the data».

[83] Si è soliti distinguere tre tipologie di *machine learning*, ovvero l'apprendimento supervisionato, quello non supervisionato e quello per rinforzo. Nel primo, il programmatore non si limita ad addestrare l'algoritmo fornendogli dati da cui imparare (*input*), ma indica anche quali sono i risultati attesi (*output*) con l'obiettivo di consentire al sistema di riconoscere i *pattern*. Nel secondo, invece, il programmatore non fornisce alcuna correzione, ma il sistema imparerà da sé a riconoscere gli schemi. Nel terzo, il programmatore offrirà una serie di *feedback* che dicono al sistema cosa è stato fatto bene e cosa male. Cfr. M.A. BODEN, *L'Intelligenza Artificiale*, cit., 47 s.

[84] R. KITCHIN, *Big Data, new epistemologies and paradigm shifts*, in *Big Data & Society*, 1, 2014, 1 ss.

Il *machine learning* ha trovato grande sviluppo grazie al supporto offerto dalle reti neurali artificiali, o *Artificial Neural Network* (ANN), ovvero sistemi di elaborazione delle informazioni basati su una struttura fisica e su una logica di funzionamento del tutto diverse da quelle dei computer classici. La ANN, infatti, rappresenta una architettura computazionale fondata sul modello del sistema nervoso ed ispirata al paradigma connessionistico proprio delle reti neurali e del cervello umano[85].

Grazie a questa struttura, le ANN sono più flessibili e non si limitano, come i computer tradizionali, a svolgere operazioni predeterminate in cui, a partire da input simbolici e precisi, si riesce a restituire un output, ma possono arrivare a risolvere qualsiasi classe di problema[86].

Le ANN, inoltre, acquisiscono la capacità di imparare i *patterns* e le associazioni tra di essi anche a partire da dati "caotici" e incompleti, senza aver bisogno di essere esplicitamente programmate, ma solo attraverso l'analisi di esempi[87]. Si intuisce come questa capacità sia fondamentale per il riconoscimento facciale, ove le immagini dei volti presentano molto "rumore" e non offrono certo un dato simbolico tipicamente chiaro e pulito.

Il sistema, inoltre, apprende autonomamente dai propri errori, grazie al tipo e al "peso" delle connessioni che si instaurano tra i "neuroni" della rete, sfruttando le tecniche citate di apprendimento supervisionato, non supervisionato o per rinforzo. Di converso, però, l'architettura e il funzionamento delle ANN è molto complesso e diviene estremamente difficoltoso risalire in termini comprensibili al

[85] M. TEGMARK, *Vita 3.0. Essere umani nell'era dell'intelligenza artificiale*, cit., 107. In sostanza, una ANN è costituita da una rete in cui molteplici unità computazionali sono interconnesse e distribuite in parallelo, di modo che ciascuna unità è in grado di ricevere segnali da diverse altre unità e risolvere problemi complessi. Le ANN poi sono solitamente strutturate su più strati di unità interconnesse, in modo che il primo strato di unità acquisisce gli input, uno o più strati intermedi lo elaborano, mentre l'ultimo strato rilascia l'output; cfr. A. VESPIGNANI, *L'algoritmo e l'oracolo*, cit., 69 ss.

[86] S. BEDESSI, *Intelligenza artificiale e fenomeni sociali. Previsioni con le reti neurali*, Maggioli, Santarcangelo di Romagna, 2019, 10 ss.

[87] Cfr. M.A. BODEN, *L'Intelligenza Artificiale*, cit., 82.

procedimento logico che ha portato ad una determinata soluzione, sfuggendo così – ancora una volta – al controllo dell'essere umano.

Infine, uno sviluppo nell'ambito delle reti neurali multistrato è costituito dal *deep learning*. Anche qui, l'aspetto fondamentale che interessa sottolineare è che l'estrazione delle caratteristiche dei dati in input per ottenere i risultati di output non è opera degli esseri umani, ma viene appresa in automatico per gradi successivi di astrazione e classificazione in maniera non lineare[88]. I *pattern* presenti nei dati vengono dunque riconosciuti a vari livelli gerarchici: ad esempio, dai pixel di un'immagine digitale ai rilevatori di contrasto, ai rilevatori di contorni, ai rilevatori della forma, alle parti degli oggetti, agli oggetti stessi[89].

Questa tecnologia ha consentito di compiere passi da gigante nell'ambito del riconoscimento facciale[90]. Nel 2012 ha destato enorme scalpore la capacità dei computer di Google di analizzare autonomamente le immagini e distinguere tra volti umani e felini[91]. Ma oggi è possibile rintracciare caratteristiche e proprietà latenti all'interno delle immagini, permettendo così non solo di individuare i volti, ma addirittura di distinguere tra facce diverse e selezionare le immagini di facce appartenenti alla medesima persona[92].

[88] C. ACCOTO, *Il mondo dato*, cit., 75.

[89] M.A. BODEN, *L'Intelligenza Artificiale*, cit., 50.

[90] S.Z. LI, A.K. JAIN, *Introduction*, cit., 10.

[91] Nel 2012 i laboratori di Google hanno integrato sedicimila computer per formare un'enorme rete neurale dotata di un miliardo di connessioni, equipaggiata con il *deep learning*. La rete è stata sottoposta a dieci milioni di immagini casuali tratte da video di YouTube, senza che queste fossero state etichettate. Il sistema è riuscito a distinguere i volti umani con l'81,7% di precisione, parti del corpo umano con il 76,7% di precisione, e gatti con il 74,8% di precisione. Cfr. L. CLARK, *Google's Artificial Brain Learns to Find Cat Videos*, in *Wired*, 26 giugno 2012 [bit.ly/3cUmBuD].

[92] Tra i modelli algoritmici più efficaci di questo tipo va segnalato quello della rete neurale convoluzionale (*Convolutional Neural Network* – CNN), che – semplificando al massimo – opera attraverso la scomposizione delle griglie di pixel in parti più piccole, chiamate *kernel*, che l'algoritmo cerca di rintracciare e mappare nell'immagine. L'analisi viene così strutturata in strati gerarchicamente organizzati, in cui ciascuno strato combina le caratteristiche dei precedenti strati ad un livello sempre più elevato di complessità e astrazione: così, ad esempio, con uno strato si riesce a selezionare bordi, linee, punti e macchie, con un altro si distinguono nasi, occhi e orecchie, ed in-

Con riguardo alle soluzioni tecnologiche qui brevemente descritte interessa segnalare un aspetto complessivo destinato a condizionare la disciplina giuridica delle TRF, ovvero la circostanza che le macchine si stanno rendendo progressivamente *autonome* rispetto agli esseri umani[93].

Grazie agli sviluppi tecnologici appena richiamati, le TRF, e più in generale l'IA, sono sempre più in grado di agire in maniera imprevedibile. La capacità di imparare direttamente dai dati senza l'intervento dell'uomo, o l'incapacità umana di ricostruire la linea di ragionamento seguita dai sistemi di *machine learning*, rendono continuamente più difficile esercitare un controllo su queste tecnologie. E nel momento che questi sistemi algoritmici vengono impiegati come supporto per assumere decisioni che impattano sulla vita e sui diritti delle persone, o addirittura ci si affida loro per prendere decisioni in maniera interamente automatizzata, questo controllo diviene di cruciale importanza per poter reagire contro i risultati che ne conseguono. Più questi sistemi si rendono autonomi rispetto all'intervento umano, dunque, più viene posta a repentaglio l'autonomia dell'uomo: l'*auto-nomia* dell'uomo trova così un nuovo nemico nell'*auto-mazione* in questo tipo di macchine[94].

fine con un altro si rintraccia l'intera struttura facciale. Questa tecnica sfrutta solitamente il *machine learning* supervisionato, cioè impara da enormi *dataset* di immagini "etichettate" dall'essere umano, il quale per ciascuna identifica e classifica il tipo di dato in modo da distinguere la classe o le classi rilevanti per l'analisi dell'algoritmo. Cfr. D. LESLIE, *Understanding bias in facial recognition technologies: an explainer*, cit., 10. Questi sistemi possono anche non seguire esattamente il procedimento di riconoscimento facciale descritto in precedenza, non avendo bisogno, ad esempio, che l'immagine del volto venga "normalizzata" attraverso la ricerca dei c.d. *landmarks*.

[93] L. FLORIDI, J.W. SANDERS, *On the Morality of Artificial Agents*, in *Minds and Machines*, 14, 3, 349 ss.; cfr. A. SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, Wolters Kluwer-Cedam, Padova, 2016, 330 ss.

[94] Riprendendo A. SIMONCINI, *Sovranità e potere nell'era digitale*, in T.E. FROSINI, O. POLLICINO, E. APA, M. BASSINI (a cura di), *Diritti e libertà in Internet*, Le Monnier, Firenze, 2017, 25.

CAPITOLO II

DIRITTI FONDAMENTALI A RISCHIO

SOMMARIO: 1. Considerazioni introduttive: l'impatto trasversale sui diritti. – 2. Le TRF nel prisma dei diritti della personalità: l'identità personale, tra mondo reale e mondo virtuale. – 3. Il "diritto ad essere lasciato solo" e le sue successive evoluzioni. – 4. La tutela dei dati personali e l'eco dei primi timori. – 5. Effetti diretti e indiretti sull'*habeas corpus.* – 6. Anonimato e spazio pubblico. – 7. TRF e le diverse dimensioni dell'eguaglianza: nuove forme di discriminazioni. – 8. (*segue*) …e una accentuazione della posizione di svantaggio delle bisognose.

1. *Considerazioni introduttive: l'impatto trasversale sui diritti*

Una volta inquadrato più specificatamente il funzionamento delle TRF, occorre adesso stabilire quali siano le libertà su cui esse sono in grado potenzialmente di incidere, e in che modalità ciò possa avvenire.

È una analisi che solo di recente comincia ad essere oggetto di attenzione sistematica in ambito europeo[1], sebbene nella dottrina statunitense il tema si sia già affacciato oramai da un ventennio[2], anche in

[1] Da ultimo v. FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., 4 ss.

[2] Con riguardo all'ordinamento statunitense, di recente v. *Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations*, Congressional Research Service (R46541), settembre 2020, ove si fonda la tutela delle libertà limitate dalle TRF nel Quarto Emendamento relativo alla protezione contro perquisizioni e sequestri irragionevoli, il Primo Emendamento relativo alla libertà di parola e di riunione pacifica, il V Emendamento contenente la "*Due Process Clause*" e il XIV Emendamento contenente la "*Equal Protection Clause*". Ma v. già K.A. BENNETT, *Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveillance Systems*, in *North Carolina Journal of Law & Technology*, 3, 1, 2001, 151 ss.; J.J. BROGAN, *Facing the Music: The Dubious Constitutionality of Facial Recognition Technology*, in *Hasting Communications and Entertainment Law Journal*, 25, 1, 2002, 65 ss.; R.H. THORNBURG, *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of*

ragione dell'ampio impiego che Oltreoceano trovano queste tecnologie.

Da questo punto di vista, tra le particolarità uniche che contraddistinguono le TRF, oltre a quelle già segnalate, vi è anche la capacità di condizionare contestualmente e trasversalmente una molteplicità di libertà e diritti fondamentali. Tanto queste tecnologie sono versatili, tanto possono combinare limitazioni a diritti e libertà in una pluralità di dimensioni.

Per dar conto di questa intrusività, pur con i necessari distinguo in relazione all'utilizzo concreto che può esser fatto del riconoscimento facciale, si cercherà di operare una scomposizione in relazione alle singole libertà, anche allo scopo di illustrare come esse vengano in gioco sia nei loro significati più tradizionali, sia nelle accezioni assunte grazie alle modalità di esercizio e di offesa consentite dalle innovazioni tecnologiche.

Punto di partenza sarà l'impatto sulla categoria dei diritti della personalità, a cominciare dal diritto all'identità personale, per poi affrontare ulteriori diritti che non sono esclusivamente riconducibili alle accezioni con cui vengono ricondotti a tale categoria. Si tratta del diritto alla riservatezza e il contiguo diritto alla *privacy*, nelle diverse dimensioni in cui si articolano, e il diritto alla protezione dei dati personali, nel contesto delle nuove forme di sorveglianza digitale.

Di seguito verranno trattati altri diritti di libertà "classici", primi fra tutti quelli riconducibili alla libertà personale, nella complessità con cui essa è concepibile rispetto al tradizionale *habeas corpus*, e ad alcune libertà suscettibili di essere esercitate nella dimensione pubblica, che possono essere messe a repentaglio dalla incapacità di sottrarsi al controllo di queste tecnologie.

Da ultimo l'analisi si sposterà sugli effetti prodotti in termini di diseguaglianze, sia nelle discriminazioni che possono derivare da questi procedimenti algoritmici, sia nell'accentuazione della posizione di svantaggio in cui si trovano persone già bisognose di maggior tutela.

Current Uses Under the Fourth Amendment, in *The John Marshall Journal of Information Technology & Privacy Law*, 20, 2, 2002, 321 ss.; S. MCCOY, *O'Big Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology*, *ivi*, 20, 3, 2002, 471 ss.; R. IRAOLA, *Lights, Camera, Action! – Surveillance Cameras, Facial Recognition Systems and the Constitution*, in *Loyola Law Review*, 49, 4, 2003, 773 ss.

La specificità di queste forme di sorveglianza è tale che il loro impiego, soprattutto in spazi pubblici o in contesti sociali, è in grado di scoraggiare e dissuadere l'esercizio del tutto legittimo delle proprie libertà (c.d. *chilling effect*)[3], incutendo uno vero e proprio stato di soggezione e di timore. Le indagini statistiche sulle reazioni delle persone alla prospettiva di essere sottoposte a riconoscimento facciale sono indicative al riguardo: negli Stati Uniti, ad esempio, indagini recenti dimostrano come vi sia una certa fiducia quando le TRF vengono impiegate dai pubblici poteri, meno quando vi fanno ricorso i privati[4], sebbene questi dati non tengano conto di alcune vicende di cronaca ancora più recenti che hanno scatenato ampi movimenti di protesa contro questi strumenti di sorveglianza[5]; nell'UE, i dati dell'Agenzia per i Diritti Fondamentali attestano come solamente il 17% dei cittadini europei siano disposti a condividere le proprie immagini facciali con le pubbliche amministrazioni a scopi identificativi[6]. Queste impressioni generali, come si vedrà, trovano piena giustificazione in punto di diritto.

[3] Si legge in COUNCIL OF EUROPE, COMMITTEE OF MINISTERS, *Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies*, 11 giugno 2013, come le forme di sorveglianza di massa «can have a chilling effect on citizen participation in social, cultural and political life and, in the longer term, could have damaging effects on democracy». Più ampiamente, cfr. N.M. RICHARDS, *The Dangers of Surveillance*, in *Harvard Law Review*, 126, 2013, 1946 ss., che sottolinea i rischi di "auto-censura" in termini di «speech, action, or even belief». Cfr. anche *The Chilling Effect in Constitutional Law*, in *Columbia Law Review*, 69, 5, maggio 1969, 808 ss.

[4] Cfr. A. SMITH, *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, in *Pew Research Center*, 5 settembre 2019 [pew-rsr.ch/39P3Pmz], ove si riporta come il 56% degli americani si fidino dell'uso responsabile di queste tecnologie da parte delle forze di polizia, mentre il 59% le ritenga un mezzo accettabile per garantire la sicurezza negli spazi pubblici. Solo il 36%, invece, dichiara di fidarsi delle società private e il 18% delle imprese inserzionistiche.

[5] Il riferimento è ai movimenti di protesta sorti a seguito dell'uccisione nel 2020 di alcune persone nere e appartenenti a minoranze etniche, che hanno portato all'intensificazione nell'utilizzo di TRF; v. *infra* Cap. II, par. 6.

[6] Cfr. T. CHRISTAKIS, *EU citizens reluctant to share their biometric data with public authorities finds FRA*, in *Ai-Regulation.Com*, 3 marzo 2020. I dati sono disponibili su: [bit.ly/3sWDwCo].

2. *Le TRF nel prisma dei diritti della personalità: l'identità personale, tra mondo reale e mondo virtuale*

L'uso di tecnologie di sorveglianza basate su riconoscimento facciale favorisce incredibilmente quel processo di superamento del confine tra analogico e digitale[7], tale da rendere complessivamente inestricabile esperienza *online* e *offline*[8]. Se il volto delle persone viene comunemente percepito come la "finestra dell'anima"[9], le TRF sono in grado di guardare attraverso questa finestra e disvelare numerosi tratti della personalità.

È come se ci si collocasse al centro di un prisma, dal quale – spostando il discorso sul piano propriamente giuridico – è possibile intercettare numerose facce di quelli che, secondo un'accezione della risalente dottrina civilistica, compongono i c.d. "diritti della personalità"[10]. Si tratta di diritti accomunati dalla riconducibilità alla sfera dell'identità, dell'identificabilità, dell'autopercezione di un soggetto

[7] Cfr. R. BRIGHI, *Dati informatici e modelli dei dati. Verso "una nuova dimensione della realtà"*, in R. BRIGHI, S. ZULLO (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015, 281 ss., sulla interazione tra dati e realtà, di cui essi offrono una rappresentazione ma che, allo stesso tempo, sono in grado di modificare.

[8] Osserva L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano, 2014, come oramai viviamo all'interno di una *infosfera*, intesa non più come ambiente virtuale sorretto da un mondo "materiale", ma come un mondo in se stesso, sempre più comprensibile soltanto come informazione (55 ss.). Entro di esso pratichiamo esperienze "*onlife*", nelle quali viene meno il confine tra le esperienze *offline*, basate sul carbonio e legate all'analogico, e quelle *online*, basate sul silicio e legate al digitale, in un fenomeno di reciproca interdipendenza e condizionamento (47 ss.).

[9] S. PORTER ET AL., *Is the Face a Window to the Soul? Investigation of the Accuracy of Intuitive Judgments of the Trustworthiness of Human Faces*, in *Canadian Journal of Behavioural Science*, 40, 3, 2008, 171 ss.

[10] Per la metafora del prisma, cfr. G. FINOCCHIARO, *Identità personale (diritto alla)*, *Dig. disc. priv., sez. civ.*, Agg. V, 2010, 723. L'immagine sociale di un soggetto potrebbe essere rappresentata come un prisma composto da molte facce, corrispondenti alla reputazione, quale giudizio degli altri su un soggetto; i dati personali, quali informazioni su un soggetto; l'identità personale, intesa come proiezione sociale della sua personalità; il nome, quale identità anagrafica; la riservatezza, in ciò che è oggetto di esclusione dalla conoscenza altrui (*ivi*, 734).

all'interno di una comunità; fattori che ne rendono incerti i reciproci confini[11]. Basti considerare l'art. 1, c. 1, della legge n. 675/1996, che accosta il trattamento dei dati personali alle condizioni del rispetto della riservatezza e dell'identità personale[12].

Per comprendere in che termini, sul piano giuridico, le TRF siano in grado di imporre dei veri e propri condizionamenti alla personalità[13], occorre iniziare a guardare entro questa categoria di diritti e verificare, da una parte, quali forme di tutela vengono offerte e, dall'altra, quale sia l'impatto di queste tecnologie su tali posizioni giuridiche soggettive.

Il primo e più comprensivo diritto della personalità può essere considerato il *diritto all'identità personale*. Come noto, tale diritto nasce e si sviluppa nell'ordinamento italiano come elaborazione dottrinale e giurisprudenziale[14], evolvendo da una nozione ritagliata sulla tute-

[11] Sulle difficoltà nello stabilire i confini dei diritti della personalità, cfr. V. ZENO-ZENCOVICH, *Personalità (diritti della)*, cit., 433 ss., che individua come criteri per delimitare i diritti della personalità la identità e identificazione del soggetto nei suoi diversi aspetti oggettivi e soggettivi, da una parte, la autopercezione che il soggetto ha di se stesso e la percezione che del soggetto dà il resto della comunità, dall'altra. All'A. si rinvia altresì per la distinzione, con la rispettiva dottrina rilevante, tra la c.d. teoria monista e pluralista della personalità, ovvero la tendenza a identificare un unico e generale diritto della personalità, oppure ricondurre la tutela della personalità alle specifiche situazioni protette dall'ordinamento. Secondo A. DE CUPIS, *I diritti della personalità*, in A. CICU, F. MESSINEO (diretto da), *Trattato di diritto civile e commerciale*, IV, I, Giuffrè, Milano, 1973, 13 ss., i diritti della personalità vengono ritenuti altresì come "diritti essenziali" alla personalità, la cui proiezione nel diritto positivo muta in relazione alla sensibilità dell'ambiente sociale, alla coscienza morale, alla percezione della posizione dell'individuo in seno alla società. V. anche P. RESCIGNO, *Personalità (diritto della)*, in *Enc. giur.*, XXIII, 1991; e D. MESSINETTI, *Personalità (diritti della)*, in *Enc. dir.*, XXXIII, 1983, 355 ss.

[12] Sulla ampiezza delle libertà chiamate in causa da questa normativa, v. U. DE SIERVO, *Tutela dei dati personali e riservatezza*, in AA.VV., *Diritti. Nuove tecnologie. Trasformazioni sociali. Scritti in memoria di Paolo Barile*, Cedam, Padova, 2003, 306 ss.

[13] Sulla praticabilità tecnica di nuove e sottili forme di controllo e quindi, per certi aspetti, anche di condizionamento della personalità, v. COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, 26 novembre 2010, 5.

[14] Cfr. V. ZENO-ZENCOVICH, *Identità personale*, in *Dig. disc. priv., sez. civ.*, IX, 1993, 294 ss.; G. PINO, *Il diritto all'identità personale*, cit., 56 ss.; intesa inizialmente,

la dei segni distintivi ad una concepita – secondo le parole della Corte costituzionale – come il «diritto ad essere sé stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo»[15].

Si tratta, quindi, di un diritto dall'immediato rilievo costituzionale, nella misura in cui si riferisce tanto al pieno sviluppo della persona, quanto all'interesse delle comunità a conoscere la reale identità dei suoi componenti[16]. Anche una rappresentazione di fatti in sé non diffamatoria, ma non vera perché inesatta, deformante, omissiva, può quindi trovare tutela in tale diritto, sia a protezione del singolo, sia

con un'accezione ristretta e di elaborazione prettamente civilistica, come la sintesi del complesso delle risultanze anagrafiche o contenute nei registri pubblici che servono ad identificare e distinguere un soggetto. Sugli sforzi dogmatici per inquadrare tale diritto e sulla ricerca del relativo fondamento costituzionale, che ha svincolato la riflessione dalla sola prospettiva civilistica iniziale, v. L. TRUCCO, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Giappichelli, Torino, 2004, 217 ss. Le principali posizioni al riguardo sono riportate *infra* in nota 16.

[15] C.cost., sent. n. 13/1994, 5.1 cons. dir. Per una definizione dottrinaria, v. G. FINOCCHIARO, *Identità personale (diritto alla)*, cit., 726, che inquadra l'identità personale come «l'immagine sociale di un soggetto quale oggettivamente rilevabile», intesa né come l'immagine che il soggetto ha di sé (verità personale), che può in ipotesi estreme anche essere scorrelata dalla realtà, né l'insieme dei dati oggettivi riferibili al soggetto (verità storica), ma come sintesi costituita dall'immagine, socialmente mediata o oggettivata, del soggetto stesso.

[16] Cfr. P. BARILE, *Diritti dell'uomo e libertà fondamentali*, il Mulino, Bologna, 1984, 26, che osserva quindi come la Costituzione assicuri garanzia all'identità personale innanzitutto tramite il sistema delle libertà, che di tale identità garantiscono lo sviluppo e la tutela. Per questo, nella ricerca del fondamento costituzionale di questo diritto, sulla scorta della citata sent. della Corte costituzionale n. 13/1994, che fa riferimento al «patrimonio irretrattabile della persona umana», si assiste ad una contrapposizione tra chi fa leva sull'art. 2 Cost. intesa come norma a fattispecie aperta (v. *infra* par. 3) e chi (come in A. PACE, *Il c.d. diritto all'identità personale e gli artt. 2 e 21 della Costituzione*, in G. ALPA, M. BESSONE, L. BONESCHI (a cura di), *Il diritto alla identità personale*, Cedam, Padova, 1981, 36 ss.), con una interpretazione più restrittiva e ancorata al testo, fa ricorso alla tutela della propria dignità contro rappresentazioni false e disonoranti, individuando il fondamento non già nell'art. 2 Cost., bensì nel combinato disposto tra l'art. 21, c. 1, ove consente di vietare e punire il subiettivamente falso, e l'art. 3, c. 1, che nel tutelare la "dignità sociale" vieta di pregiudicare l'altrui onore, ancorché difendendo fatti veri.

nell'interesse dell'opinione pubblica a una corretta rappresentazione delle posizioni, delle idee, del patrimonio ideale, politico e sociale di persone e gruppi[17].

L'introduzione della citata legislazione sul trattamento dei dati personali, poi, ha sancito anche qui un mutamento di paradigma[18], in cui ad una "libertà da", consistente nel diritto a ricevere una corretta e non infedele rappresentazione della personalità di un soggetto[19], si aggiunge anche una "libertà di", nel momento in cui si afferma, come manifestazione del potere di autodeterminazione[20], il diritto alla costruzione e alla tutela della propria identità, non in astratto ma nello specifico del contesto delle relazioni sociali in cui si è immersi[21]. In questo senso, l'identità va così a costituire la «proiezione nel sociale dell'essere», non solo nei suoi segni distintivi, ma anche «in tutti i suoi

[17] S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006, 81.

[18] Osserva G. RESTA, *Identità personale e identità digitale*, in *Il diritto dell'informazione e dell'informatica*, 3, 2017, 513 e 521 ss., come l'art. 1, della legge n. 675/1996 e l'art. 2 del d.lgs. n. 196/2003 si limitino a richiamare l'identità personale ma non a definirne i contenuti, sebbene questa normativa abbia avuto il pregio di trasformare la tutela rimediale dell'immagine personale, concepita come risultato di un autonomo percorso definitorio lasciato all'individuo rispetto al quale grava un dovere generale di astensione, ad una tutela non limitata solamente alla garanzia di una non interferenza, ma improntata ad un ruolo attivo di supervisione e controllo dei pubblici poteri rispetto ad un processo in atto, continuamente esposto a varie forme di interferenza.

[19] Così in base alla nota Cass., sez. I, 22 giugno 1985, n. 3769 (c.d. caso Veronesi), ossia la prima decisione della Cassazione sul punto, che si riferisce «all'interesse a non vedere alterato, travisato, offuscato, contestato il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale, ecc.». Per una casistica giurisprudenziale più approfondita, v. G. FINOCCHIARO, *Identità personale (diritto alla)*, cit., 725 s., ove si specifica che la distorsione dell'identità può essere causata dal travisamento, da omissioni, da confusione, da decontestualizzazione, ma non nella tutela della mera autorappresentazione della propria personalità

[20] Cfr. *infra* par. 4.

[21] F.D. BUSNELLI, *La persona alla ricerca dell'identità*, in *Rivista critica del diritto privato*, 1, 2010, 12 ss. Osserva G. FINOCCHIARO, *Identità personale (diritto alla)*, cit., 723, come tale diritto ruoti attorno al concetto di relazione, quale veicolo attraverso cui la personalità si rivela, e di dignità, che costituisce il fondamento nella costruzione dei diritti della personalità che non abbiano ad oggetto la fisicità della persona.

attributi e le sue qualità, portatrice ed elaboratrice di pensieri e di idee che si manifestano in comportamenti ed azioni»[22].

In questa prospettiva, il diritto all'identità personale ha manifestato nel tempo una mutevolezza tale da arricchirsi di nuovi contenuti, dall'identità genetica all'identità sessuale[23]. Per quanto qui interessa maggiormente, lo sviluppo delle tecnologie dell'informazione e della comunicazione, il moltiplicarsi delle attività svolte nel mondo virtuale, l'avvento dei *social network*, hanno indotto ad affiancare alla categoria della "identità personale" quella della "identità digitale".

Della nozione di identità digitale preme qui sottolineare una duplice accezione, rispettivamente in senso ampio e più ristretto[24]. Nel primo caso, l'identità digitale può essere intesa come sinonimo di identità "in rete", in accordo anche con il significato fatto proprio dalla "Dichiarazione dei diritti in Internet" del 2015[25]; nel secondo caso, ci si può riferire all'identità digitale, alla stregua di quanto stabilito dal Codice dell'amministrazione digitale, come «la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale»[26].

[22] R. TOMMASINI, *L'identità dei soggetti tra apparenza e realtà: aspetti di una ulteriore ipotesi di tutela della persona,* in G. ALPA, M. BESSONE, L. BONESCHI (a cura di), *Il diritto alla identità personale*, cit., 83.

[23] Cfr. L. TRUCCO, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, cit., 171 ss.

[24] Per una distinzione tra accezione ampia e ristretta di identità digitale, v. G. RESTA, *Identità personale e identità digitale*, cit., 514 ss.; I. TARDIA, *L'identità digitale tra memoria ed oblio*, ESI, Napoli, 2017, 66 ss., che osserva come la prima accezione venga contrapposta all'identità e al corpo fisico, mentre la seconda sia legata a problematiche come quella del "furto di identità". Per quanto riguarda il problema della identificazione in rete, v. L. TRUCCO, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, cit., 114 ss., che distingue il profilo "soggettivo", legato all'interrogativo su "chi siamo" in rete, da quello "informativo", legato a "cosa ne è delle nostre informazioni quando navighiamo".

[25] Tale documento, approvato il 28 luglio 2015 dalla Commissione appositamente istituita dalla Camera dei Deputati, dedica specifica menzione a quella che viene definita come «la rappresentazione integrale e aggiornata della proprie identità in Rete» (art. 9). Valorizza questo aspetto T. PASQUINO, *Identità digitale della persona, diritto all'immagine e reputazione*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, GFL, Milano, 2019, 101 ss.

[26] Art. 1, c. 1, lett. u-*quater*, d.lgs. n. 7 marzo 2005, n. 82, recante "Codice

Delle molteplici problematiche e implicazioni giuridiche legate all'ammissibilità di una autonoma e distinta nozione di identità digitale rispetto alla identità personale[27], occorre porre l'attenzione su due fenomeni collegati rispettivamente alle due accezioni appena riportate.

L'identità digitale in senso stretto risulta finalizzata a facilitare il riconoscimento dell'utente e consentire di accedere in sicurezza e più agevolmente a beni e servizi messi a disposizione – stante la definizione sopra riportata – dalle pubbliche amministrazioni, ma anche da istituti di credito o assicurativi, oppure per accedere a dispositivi elettronici dai quali svolgere molteplici operazioni; tutte ipotesi per le quali, come detto, sta prendendo campo l'impiego di TRF a fini di verifica o autenticazione. Ai fini del presente discorso, tra le forme di tutela da apprestare, occorre richiamare quella rivolta contro il fenomeno dei furti di identità digitale[28]. Nel settore delle TRF, si tratta di ipotesi in cui un sistema viene indotto in un falso-positivo allo scopo di potersi sostituire ad altra persona, mediante molteplici tecniche che sono state

dell'amministrazione digitale". Sul "Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese" (SPID), per un inquadramento sistematico, v. A. MASUCCI, *Digitalizzazione dell'amministrazione e servizi pubblici on line. Lineamenti del disegno normativo*, in *Diritto pubblico*, 1, 2019, 136 ss.

[27] Questioni da tempo indagate dalla dottrina, alla quale in questa sede ci si limiterà a rinviare: si pensi ad aspetti come la tutela dell'identità in rete, specie sotto i profili reputazionali, oppure al ricorso a tecnologie di identificazione del soggetto, per superare la condizione di anonimato che la rete favorisce e risalire all'identità reale del soggetto, su cui v. G. RESTA, *Identità personale e identità digitale*, cit., 515, e M. BRUGI, *Dall'identità personale all'identità digitale*, in *Informatica e diritto*, 1-2, 2008, 167 ss.; all'identità digitale come espressione della libertà creativa di un soggetto sottoposta al regime di proprietà intellettuale, su cui v. S. LANDINI, *Identità digitale tra tutela della persona e proprietà intellettuale*, in *Rivista di diritto industriale*, 4-5, 2017, 180 ss.; sino alla soggettività digitale come mezzo e condizione attraverso cui prende forma una nuova configurazione dei diritti fondamentali conosciuti e una apertura a nuove istanze di tutela e poteri, su cui v. G. AZZARITI, *Internet e Costituzione*, in *Costituzionalismo.it*, 2, 2011, 1 ss.; P. PASSAGLIA, *Internet nella Costituzione italiana: considerazioni introduttive*, in *Consulta OnLine*, 2013, 18 ss.; T.E. FROSINI, *Costituzionalismo 2.0*, in *Rassegna parlamentare*, 4, 2016, 675 ss.; e da ultimo F. FAINI, *Diritto all'esistenza digitale*, in *BioLaw Journal*, 3, 2019, 91 ss.

[28] Cfr. G. RESTA, *Identità personale e identità digitale*, cit., 514 ss.; I. TARDIA, *L'identità digitale tra memoria ed oblio*, cit., 66 ss., cui si rinvia anche per il problema della violazione degli *account* dei *social network*.

analizzate dalla letteratura che si è occupata più da vicino della sicurezza contro i cyber-attacchi[29].

Queste ipotesi trovano adesso sanzione penale a seguito dell'introduzione di una nuova circostanza aggravante del reato di frode informatica all'art. 640-*ter* c.p.[30], ovvero che il fatto sia commesso "con furto o indebito utilizzo dell'identità digitale"; il bene protetto tale norma, tuttavia, risulta essere il patrimonio e non l'identità in sé, per cui occorre necessariamente procurare un «ingiusto profitto» per integrare tale fattispecie[31].

Rispetto all'accezione più ampia dell'identità digitale, occorre invece sottolineare alcuni fenomeni che favoriscono non soltanto una rappresentazione infedele della propria identità, ma che si risolvono in una vera e propria "decontestualizzazione" rispetto all'integralità della persona umana. L'identità digitale, infatti, può andare incontro a processi di astrazione e frammentazione con i quali si considerano rilevanti i dati, e quindi gli aspetti, che rappresentano soltanto una parte dell'identità e della individualità complessiva. L'obiettivo è quello di ridurre la persona ad una o più dimensioni specifiche – che sia quella di un certo tipo di "consumatore" o di "soggetto controllato" – e otte-

[29] Sul punto v. anche *infra* Cap. III, par. 5.3.

[30] Osserva P. CIPOLLA, *"Social network", furto di identità e reati contro il patrimonio*, in *Giurisprudenza di merito*, 2012, 12, 2672 ss., come già il reato di frode informatica, all'art. 640-*ter* c.p., offrisse una tutela parziale nei confronti del furto o dell'indebito utilizzo di identità digitale, nella misura in cui l'indebito utilizzo origina da un'azione di hackeraggio considerabile come "alterazione del funzionamento di un sistema telematico", o comunque come "intervento senza diritto su dati, informazioni, programmi", elementi costitutivi di tale fattispecie. Più ampiamente, v. anche R. BARTOLI, *La frode informatica tra modellistica, diritto vigente, diritto vivente e prospettive di riforma*, in *Il diritto dell'informazione e dell'informatica*, 3, 2011, 383 ss.

[31] Aggravante introdotta dall'art. 9 del d.l. 14 agosto 2013 n. 93, convertito con modificazioni dalla legge 15 ottobre 2013, n. 119. In dottrina, v. G. MALGIERI, *Il furto di "identità digitale": una tutela "patrimoniale" della personalità*, in D. FALCINELLI, R. FLOR, S. MARCOLINI (a cura di), *La giustizia penale nella "rete". Le nuove sfide della società dell'informazione nell'epoca di Internet*, Diplap, Milano, 2015, 37 ss., che sottolinea però come il bene giuridico tutelato dal reato di frode informatica sia quello del patrimonio e ciò riduca fortemente il portato di tutela all'identità digitale della novella citata.

nere così una sua particolare funzionalizzazione[32]. Questa decontestualizzazione – che, come si vedrà, trova perfezionamento nelle tecniche di profilazione[33] – può risolversi in una rappresentazione parziale e fuorviante della persona. A partire da essa, poi, vengono prese decisioni che possono variare dal favorire o meno l'accesso di un utente a beni e servizi, la possibilità di visualizzare certi tipi di informazioni piuttosto che altre, sino all'essere oggetto di discriminazioni o essere sottoposti a determinati controlli da parte delle autorità pubbliche[34].

Le TRF, come le tecnologie biometriche in generale, sono in grado di favorire incredibilmente questi processi di decontestualizzazione. I volti delle persone vengono comunemente percepiti come intrinsecamente unici e come una fonte primigenia di identità[35]. Tali tecnologie, tuttavia, sono in grado di "leggere" le caratteristiche uniche del volto e di trasformarle in dati[36], facendo loro smarrire il valore simbolico, culturale e sociale di rappresentazione della personalità[37]. Questa trasformazione digitale, viceversa, è funzionale all'identificazione e al tracciamento, alla riduzione delle persone a punteggi o profili, attraverso i quali è possibile assumere le decisioni appena richiamate[38]. Tramite queste tecniche algoritmiche, l'identità digitale, o meglio le

[32] S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica del diritto privato*, 4, 1997, 606.

[33] V. *infra* Cap. III, par. 6.4.

[34] Cfr. S. MONTELEONE, Privacy, data protection *e identità elettronica. Tra rapidi sviluppi della tecnologia e nuovo approccio europeo*, in M. VILLONE ET AL., *Nuovi mezzi di comunicazione e identità. Omologazione o diversità?*, Aracne, Roma, 2021, 533 ss.

[35] Cfr. M.J. SHEEHAN, M.W. NACHMAN, *Morphological and Population Genomic Evidence that Human Faces Have Evolved to Signal Individual Identity*, in *Nature Communication*, 5, 2014, 1 ss.

[36] Si osserva in GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, cit., p. 2, che «i dati biometrici cambiano in maniera irreversibile la relazione tra corpo e identità, in quanto le caratteristiche del corpo umano possono essere "lette" da una macchina e sottoposte a un successivo trattamento»; sul trattamento dei dati biometrici, v. *infra* Cap. II, par. 3.

[37] Intendendo così la "persona" anche nel suo significato originale di "maschera"; cfr. E. GOFFMAN, *La vita quotidiana come rappresentazione*, il Mulino, Bologna, 2000, 29 ss.

[38] Cfr. D.K. CITRON, F. PASQUALE, *The Scored Society: Due Process for Automated Predictions*, in *Washington Law Review*, 89, 2014, 2 ss.

molteplici identità digitali che un individuo può assumere, si impongono e prendono il sopravvento sull'interezza e l'integrità dell'identità personale, aprendo alle nuove forme di sorveglianza di cui si è parlato introduttivamente. Si concretizza così quella preoccupazione, formulata sul piano etico, che l'identità personale possa risultare progressivamente erosa dai crescenti doveri di identificazione richiesti nelle società contemporanee[39].

3. *Il "diritto ad essere lasciato solo" e le sue successive evoluzioni*

Una ulteriore esigenza di tutela chiamata in causa dalle TRF è quella legata al *diritto alla riservatezza*. Quest'ultimo – come noto – ha trovato ingresso nel nostro ordinamento per via dottrinaria[40] e giurisprudenziale[41], assumendo un contenuto essenzialmente negativo come pretesa di escludere altri dalla conoscenza di vicende strettamente personali e familiari, originariamente riconducibile al "*right to be let alone*" della celebre elaborazione di Warren e Brandeis nel 1890[42].

Quando la dottrina costituzionalistica ha tematizzato il diritto alla riservatezza, sottraendola alla sola visione civilistica che lo riconduceva

[39] Pericolo paventato da COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, cit., 6.

[40] Per una ricostruzione del percorso dottrinario fin dalla sua emersione nella riflessione italiana, v. S. SCAGLIARINI, *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Aracne, Roma, 2013, 43 ss.

[41] Cfr. Cass., sez. I, 27 maggio 1975, n. 2129 (c.d. caso Soraya Esfandiari); per questo *leading case* e la ricostruzione del percorso giurisprudenziale in cui si colloca, oltreché della normativa assai frammentata in tema, che contribuisce così a frammentare la tutela della riservatezza entro diversi ambiti materiali e funzionali, v. il quadro offerto in R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali: una storia di evoluzione e discontinuità,* in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, I, Giuffrè, Milano, 14 ss.; G. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. NANIA, P. RIDOLA (a cura di), *I diritti costituzionali*, II, Giappichelli, Torino, 2006, 621 ss.; G. VISINTINI, *Dal diritto alla riservatezza alla protezione dei dati personali*, in *Il Diritto dell'informazione e dell'informatica*, 1, 2019, 1 ss.

[42] Cfr. L. BRANDEIS, S. WARREN, *The Right to Privacy*, in *Harvard Law Review*, 4, 5, 1890, 193 ss.

ai diritti della personalità, si è cercato più compiutamente di ancorare il fondamento di questo diritto al testo costituzionale e, contestualmente, garantire una certa apertura nei confronti delle nuove istanze di tutela provenienti dalla società, anche per contrastare la crescente capacità invasiva degli strumenti tecnologici. Da qui le diverse prospettazioni teoriche che guardano alla clausola generale all'art. 2 Cost. *ex se* o in combinato disposto con altre specifiche previsioni costituzionali sulle singole libertà[43]. Rimane ferma la difficoltà di muoversi in

[43] Per una ricostruzione degli sforzi teorici volti a ricercare un fondamento nel nostro ordinamento al diritto di riservatezza, è possibile distinguere due grandi filoni, come anche indicato in M. TIMIANI, *Un contributo allo studio sul diritto alla riservatezza*, in *Studi parlamentari e di politica costituzionale*, 2, 2012, 58 ss. Da una parte, la dottrina civilistica si è concentrata sulla ricerca di tale fondamento operando una analogia con la disciplina relativa al diritto di immagine (v. A. DE CUPIS, *I diritti della personalità*, cit., 256 ss.), o al diritto al nome e al diritto all'onore e reputazione (v. G. GIACOBBE, *Riservatezza (diritto alla)*, in *Enc. dir.*, XL, 1989, 1246 ss.). Dall'altra, la dottrina costituzionalistica si è divisa a sua volta tra coloro che hanno rinvenuto un riferimento costituzionale implicito al diritto di riservatezza, come la «dichiarazione di inviolabilità della libertà personale» all'art. 13, estesa anche alla integrità psichica o morale, da intendersi come diritto alla tutela di tutti i beni giuridici attinenti alla persona, compresi quelli afferenti all'interiorità e alla coscienza (F. MODUGNO, *I "nuovi diritti" nella giurisprudenza costituzionale*, Giappichelli, Torino, 1995, 20 s.); o intendendo la libertà personale come una "libertà-situazione" (secondo la ricostruzione in AMATO, *Art. 13*, in G. BRANCA (a cura di), *Commentario della Costituzione*, Zanichelli - Foro italiano, Bologna-Roma, 1977, 1 s.), suscettibile cioè di assumere contenuti diversi e ulteriori nei confronti dei pubblici poteri o dei privati rispetto alla originaria "libertà dagli arresti", in ragione dei limiti che possono imporsi (cfr. G. P. CARETTI, G. TARLI BARBIERI, *I diritti fondamentali Libertà e diritti sociali*, Giappichelli, Torino, 2017, 320 ss.); oppure guardando all'art. 21 Cost., optando per «un'impostazione "induttiva" dei limiti alla libertà di manifestazione del pensiero che si richiamino al "valore" della riservatezza» (cfr. A. PACE, M. MANETTI, *Commento all'art. 21*, in G. BRANCA (fondato da), A. PIZZORUSSO (continuato da), *Commentario della Costituzione*, Zanichelli – Il foro italiano, Bologna - Roma, 2006, 146); oppure, ancora, all'art. 2 Cost., in combinato disposto con le norme relative alla libertà personale, domiciliare e di corrispondenza (cfr. P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., 61); o in combinato, più in generale, con le previsioni che si riferiscono a situazioni, rapporti o ambiti di attività umane giuridicamente protetti da interferenze esterne (artt. 19, 22, 24, 29 ss., 32, ma anche 41, 18) (G. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, cit., 625). Altre ricostruzioni, invece, richiamano come fondamento le clausole generali previste in Costituzionale, segnatamente l'art. 2 nella sua nota ricostru-

una casistica giurisprudenziale frammentata e di operare delicati bilanciamenti con le altre libertà costituzionali in gioco[44].

Quello alla riservatezza è un diritto che, a causa della sua intrinseca storicità, presenta una mutevolezza tale da rendere difficile una precisa delimitazione dei suoi confini, registrando una crescente forza espansiva[45]. Emblematicamente, nell'accezione di "vita privata" stabilita a livello di CEDU e dell'UE, vengono ricomprese la diversa dimensione fisica, psicologica e relazionale della persona, anche in senso non meramente escludente, di cui si può beneficiare persino entro contesti pubblici[46]. La riservatezza, dunque, tende a confondersi con il più am-

zione come norma "a fattispecie aperta" ad altre libertà e ad altri valori personali non espressamente tutelati dal testo costituzionale, e non semplicemente di "chiusura" o "riassuntiva" di tutti i diritti fondamentali menzionati dalla Costituzione (A. BARBERA, *Art. 2*, in G. BRANCA (a cura di), *Commentario della Costituzione*, cit., 1975, 80 ss.). Per i richiami alla riflessione sul punto, v. anche S. SCAGLIARINI, *La riservatezza e i suoi limiti*, cit., 91 ss.

[44] Nella giurisprudenza costituzionale il diritto alla riservatezza è stato qualificato quale «manifestazione del diritto fondamentale all'intangibilità della sfera privata» (sent. n. 366/1991) e attinente alla tutela della vita degli individui nei suoi molteplici aspetti, che trova riferimento negli artt. 2, 14, 15 Cost., oltre che in varie norme dell'UE e convenzionali, quali gli artt. 7 e 8 della CDFUE, l'art. 8 della CEDU, la "Convenzione 108", nonché, da ultimo, il regolamento (UE) n. 2016/679 (v. *infra* Cap. III, par. 2). Sui riferimenti alla riservatezza, in termini diretti o indiretti, vi è un'ampia casistica giurisprudenziale: v. C.cost., sentt. n. 20/2019 (in tema di trasparenza e obblighi di pubblicazione dei dati personali); n. 1/2013 (in tema di intercettazioni telefoniche del Capo dello Stato); n. 271/2005 (sul riparto di potestà legislativa Stato-Regini in tema di tutela dei dati personali); n. 425/2005 (sull'autorizzazione del figlio adottato ad accede alle informazioni sulle sue origini); nn. 173/2009, 149/2008, 372/2006, 135/2002, 463/1994, 81/1993 e 366/1991 (in tema di intercettazioni di comunicazioni); nn. 238 e 257/1996, 218/1994 (in tema di trattamenti sanitari obbligatori); nn. 235/1993, 373/1992 (in tema di pubblicità dei dibattimenti processuali); nn. 16 e 17/1981 (in tema di pubblicità nel processo minorile); nn. 38/1973, 122/1970 (in tema di diritto all'immagine e libertà di stampa). Più in generale, cfr. G. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, cit., 649 ss.; M. TIMIANI, *Un contributo allo studio sul diritto alla riservatezza*, cit., 64 ss.; S. SCAGLIARINI, *La riservatezza e i suoi limiti*, cit., 69 ss. e 86 ss.

[45] G. BUSIA, *Riservatezza (diritto alla)*, in *Dig. disc. pubbl.*, Agg. I, 2000, 477 ss.

[46] Come stabilito anche dalla Corte EDU con riferimento al concetto di "vita privata" all'art. 8 della CEDU, siamo di fronte ad una nozione ampia non suscettibile di una definizione esaustiva (*Pretty v. United Kingdom*, 29 aprile 2002, p. 62), un concet-

pio e articolato concetto della *privacy*, con il quale si trova ad essere inestricabilmente legato.

La *privacy* richiama una nozione di natura filosofico-politica prima che giuridica, sviluppatasi in sistemi di *common law* e presto circolata in altri ordinamenti[47], ove ha acquisito una molteplicità di significati che la porta a sovrapporsi ad altri diritti fondamentali[48]. Operando una concettualizzazione complessiva, se ne può parlare sia in senso negativo, con enfasi nel momento escludente, sia in senso positivo, accentuando il carattere di autodeterminazione dell'interessato. Di conseguenza, nella prima accezione, è possibile distinguere una *privacy* fisica, riferita al proprio corpo; una *privacy* spaziale, con riguardo alla capacità di limitare l'accesso o estromettere terzi; una *privacy* comunicativa, come segretezza nello scambio di informazioni rivolte riservatamente ad altri soggetti; una *privacy* proprietaria, a presidio dell'intenzione di nascondere beni, fatti, attività o informazioni dalla vista di altri. Nella seconda accezione, si può distinguere invece una

to che copre l'integrità fisica e psicologica di una persona. L'art. 8 CEDU non è limitato alla protezione di un "circolo ristretto" in cui l'individuo debba vivere la sua vita personale e da cui escludere interamente il resto del mondo. Esso protegge il diritto di stabilire e sviluppare relazioni con altri esseri umani e la restante parte del mondo (*Bărbulescu v. Romania*, 5 settembre 2017, p. 70), anche in contesti pubblici (*López Ribalda and Others v. Spain*, 17 ottobre 2019, p. 87). La vita privata può includere anche attività di natura professionale o economica (*Denisov v. Ukraine*, 25 settembre 2018, p. 100 s.). L'art. 7 della CDFUE presenta una formulazione analoga all'art. 8 della CEDU, e dunque, in base all'art. 52, par. 3 della CDFUE, risulta possibile operare dei riferimenti incrociati tra la giurisprudenza della CGUE e quella dalla Corte EDU, sebbene gli indirizzi delle due Corti si siano sviluppati seguendo traiettorie in parti differenti; per una relativa disamina, v. G. MARTINICO, *Art. 7. Rispetto della vita privata e della vita familiare*, in AA.VV., *Carta dei diritti fondamentali dell'Unione europea*, in AA.VV., *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017, 119 ss.

[47] Sull'origine della tutela della *privacy* nell'ordinamento britannico e americano, cfr. A. CERRI, *Riservatezza (diritto alla). Diritto comparato e straniero*, in *Enc. giur.*, XXVII, 1991, 1 ss., e, più di recente, A. DI MARTINO, *Profili costituzionali della privacy in Europa e negli Stati Uniti*, Jovene, Napoli, 2017, 37 ss.

[48] Come osserva S. SCAGLIARINI, *La riservatezza e i suoi limiti*, cit., 29 s., la *privacy* ha finito per coincidere sostanzialmente con il concetto stesso di libertà: nel sistema nordamericano, è stata ricondotta alla disciplina della contraccezione, dell'aborto, delle scelte di fine vita, della libertà di scelta in ambito matrimoniale, ecc.

privacy intellettiva, a presidio della propria sfera di pensieri e opinioni; una *privacy* decisionale, rivolta agli aspetti più intimi e sensibili della propria personalità; una *privacy* relazionale, nei confronti dei rapporti con altre persone o della appartenenza ad una comunità sociale; una *privacy* comportamentale, nello svolgimento di attività in pubblico nella misura in cui sia possibile rimanere anonimi; trasversalmente ad ogni altri significato troviamo anche una *privacy* informativa, relativa al controllo che altri soggetti possono esercitare sulle informazioni che riguardano un'altra persona[49].

Anche nel nostro ordinamento è stato compiuto lo sforzo di ricondurre la più ampia nozione di tutela della *privacy* ad un fondamento costituzionale che ne rifletta la complessità, trovando riferimento nella tutela dei diritti inviolabili, l'eguale dignità sociale delle persone e l'intrinseca socialità di questo diritto, con riguardo alle diverse sfere di libertà entro cui la *privacy* può esplicarsi[50].

[49] Così di recente v. B.-J. KOOPS ET AL., *A Typology of Privacy*, in *University of Pennsylvania Journal of International Law*, 38, 2017, 483 ss., che propongono, a livello descrittivo, una classificazione tipologica delle manifestazioni della *privacy* in nove ordinamenti, ovvero USA, Canada, UK, Paesi Bassi, Germania, Italia, Repubblica Ceca, Polonia e Slovenia.

[50] Osserva A. CERRI, *Riservatezza (diritto alla). Diritto costituzionale*, in *Enc. giur.*, XXVII, 1995, 3 s., come se si volesse operare una assimilazione tra riservatezza e *privacy*, occorrerebbe fare riferimento ad una "costellazione di diritti" accomunati non da caratteri strutturali o formali, quanto da una matrice ideale di rifiuto da intrusioni in una sfera riconosciuta come propria della persona e della sua spontanea socialità, e dunque a "diritti" alla riservatezza che attingono al "pieno sviluppo della persona" all'art. 3, c. 2, Cost., e si legano ad altre previsioni costituzionali in relazione ai profili specifici, a partire dall'art. 15. Secondo S. RODOTÀ, *Persona, riservatezza, identità*, cit., 588 ss. e 603, la *privacy* troverebbe fondamento nell'art. 2 Cost., in quanto collocata nella dimensione delle relazioni sociali e del pieno svolgimento della propria personalità, e nell'art. 3 Cost., ove si menziona l'eguaglianza e la "dignità sociale"; è il portato di quel passaggio, da tempo con chiarezza esplicitato, secondo cui la *privacy* perde quella sua dimensione individualistica e di segretezza del diritto all'essere lasciato solo, per acquisire un marcato carattere di socialità e di controllo sulle proprie informazioni, proprio della c.d. autodeterminazione informativa (v. *infra*). Secondo G. BUSIA, *Riservatezza (diritto alla)*, cit., 481 s., vale il riferimento ai diritti inviolabili all'art. 2 Cost., al principio di eguaglianza sostanziale, alla tutela della libertà personale intesa come comprendente l'integrità psichica e coscienziale, nonché alla tutela del domicilio art. 14 Cost.), delle comunicazioni (art. 15 Cost.) e della manifestazione del pensiero (art. 21 Cost.).

Ai fini della presente analisi non è necessario indagare fino a che punto sia ipotizzabile una coincidenza tra riservatezza e *privacy*, o se sia possibile stabilire una assimilazione che dilati la prima fino a farle assumere una portata trasversale, quasi una "nuova dimensione" dei diritti stessi[51]. L'obiettivo, invece, è sottolineare come le TRF siano in grado di insidiare entrambi questi diritti nelle loro più complesse sfaccettature, sia che si intenda oggi la riservatezza come esigenza di tutela dell'intimità contro la diffusione di fatti e informazioni che dovrebbero rimanere privati, sia che si guardi alla *privacy* come situazione più articolata, che rinvia a forme più ampie di tutela della sfera privata e delle varie libertà a questa connesse[52].

Da quest'ultimo punto di vista, le TRF riescono ad incidere su una molteplicità di manifestazioni della *privacy* ben più ricche di quelle ipotizzate nel "*right to be let alone*" di fine XIX° secolo. Si considerino le interferenze con altre libertà fondamentali, che possono sostanziarsi in altrettante invasioni all'interno degli spazi di intimità della vita delle persone, come avviene – lo si vedrà meglio a breve, in termini problematici[53] – per le forme di limitazioni della libertà personale e di quella che è stata appena definita come *privacy* "fisica"; o nel caso delle ingerenze nella libertà di riunione, rispetto alla richiamata *privacy* "comportamentale". Ma si considerino anche le citate applicazioni sperimentali delle TRF, in grado, dalla "lettura" del volto, di disvelare con un certo grado di affidabilità lo stato emozionale, i tratti della personalità, le opinioni politiche o le tendenze sessuali; casi paradigmatici da cui emerge la capacità di queste tecnologie di penetrare le dimensioni più profonde – come richiamate sopra – della *privacy* "intellettiva", "decisionale" o "relazionale". Queste tecnologie, inoltre, sono capaci anche di interferire con la citata *privacy* "informazionale", nella misura in cui determinano la raccolta di informazioni, per il tramite delle attività di sorveglianza; il loro trattamento, nella forma di aggregazione e

[51] In termini problematici, P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., 61.

[52] Riprendendo le diverse accezioni indicate in S. RODOTÀ, *Riservatezza*, *Enc. it.*, VII App., 2007, versione *online*. Sulla cultura giuridica della privacy nel nostro ordinamento, v. S. SCAGLIARINI, *In tema di privacy: virtù e vizi della cultura giuridica*, in *Ars Interpretandi*, 1, 2017, 49 ss.

[53] V. *infra* par. 5.

di usi secondari delle stesse; la loro conservazione in enormi banche dati, con il conseguente rischio di una impropria diffusione[54]. Senza considerare il senso di insicurezza o di esclusione – ovvero il già citato *chilling effect* – che la sottoposizione a TRF è capace di ingenerare. Il caso della *privacy*, nella sua complessità, dunque, appare paradigmatico della capacità di queste tecnologie di incidere trasversalmente su una molteplicità di libertà fondamentali.

4. *La tutela dei dati personali e l'eco dei primi timori*

A fronte della sottolineata capacità invasiva di nuove tecnologie algoritmiche come le TRF, è già emerso come la tutela della riservatezza e della *privacy* si siano saldate all'ulteriore dimensione della *tutela dei dati personali*.

È bene anticipare come il diritto alla protezione dei dati si sia arricchito più di tutti di valenze ulteriori rispetto a quelle riconducibili alla sola sfera dei diritti della personalità, per assumere una rilevanza ben più ampia grazie all'universo delle tecnologie dell'informazione e delle comunicazioni. Basti solo considerare la dimensione collettiva assunta dalle piattaforme in rete e dai *social network*, valutabile in termini di dipendenza e di costo dell'eventuale isolamento[55]; la crucialità della gestione dei dati per la libertà di informazione e la costruzione degli ordinamenti democratici[56]; le recenti strategie dell'UE volte a costruire una "economia europea dei dati"[57].

Volendo abbozzare un inquadramento giuridico, *privacy* e protezione dei dati ricevono innanzitutto una disciplina separata a livello

[54] Riprendendo così alcune manifestazioni delle quattro categorie distinte di lesioni alla *privacy* proposte da D. SOLOVE, *A Taxonomy Of Privacy*, in *University of Pennsylvania Law Review*, 154, 3, 2006, 477 ss.

[55] C. CARLETTI, *Diritto alla riservatezza, protezione dei dati personali e spazio digitale nell'ordinamento internazionale*, Editoriale Scientifica, Napoli, 2020, 57.

[56] Sul punto, è sufficiente richiamare gli esempi dell'uso dei *social network* come strumento di veicolo del dissenso politico (*infra* par. 6) e dello scandalo di "Cambridge Analytica" (*infra* Cap. III, par. 6.4).

[57] Cfr. EUROPEAN COMMISSION, *Building a European Data Economy*, COM(2017) 9 final, 10 gennaio 2017.

europeo[58]. Benché la seconda svolga un ruolo rilevante ai fini della garanzia della prima[59], la CDFUE distingue espressamente i beni protetti dall'art. 7 (rispetto della vita privata e della vita familiare) e dall'art. 8 (protezione dei dati a carattere personale), mentre la CEDU, benché non rechi espressa menzione della protezione dei dati, considera la tutela degli stessi come necessariamente caratterizzante, ma distinta, rispetto alla garanzia del diritto al rispetto della vita privata e familiare di cui all'art. 8[60].

Nello specifico del nostro ordinamento[61], si potrebbe dire a grandi linee come la tutela dei dati tragga origine dalla necessità di fronteggiare il pregiudizio collettivo che, grazie alla nascita dell'informatica, derivava potenzialmente dalla diffusione delle prime "banche di dati" elettroniche negli anni '60. Emergeva in questo momento storico una nuova forma di "potere informatico", che apriva a inedite logiche di controllo delle autorità pubbliche, esercitate sui singoli e sulla società per mezzo della schedatura di massa e delle informazioni ottenibili dall'incrocio di dati di diversa natura e provenienza[62].

A fronte di questo nuovo potere, espresso per lo più in maniera

[58] Sulla non coincidenza tra le due figure, v. in dottrina P. DE HERT, S. GUTWIRTH, *Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action*, in S. GUTWIRTH, Y. POULLET, P.D. HERT, J. NOUWT, C.D. TERWANGNE (a cura di), *Reinventing data protection?*, Springer, Berlino, 2009, 3 ss. ; O. POLLICINO, M. BASSINI, *Art. 8. Protezione dei dati di carattere personale*, in AA.VV., *Carta dei diritti fondamentali dell'Unione europe*a, cit., 135 ss.

[59] Sulla interconnessione in questo senso, v. CGUE, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 ottobre 2015, p. 78.

[60] Corte EDU, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, 27 giugno 2017, p. 133. V. *retro* par. 3.

[61] Per una efficace ricostruzione di questa evoluzione in chiave di gestione del rischio, v. A. MANTELERO, *La gestione del rischio*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, Zanichelli, Bologna, 2019, 477 ss.

[62] Cfr. V. FROSINI, *Informatica, diritto e società*, Giuffrè, Milano, 1992, 190. Sottolinea R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali: una storia di evoluzione e discontinuità*, cit., 8 ss., come in questi archivi informatici fosse possibile non soltanto conservare enormi quantità di informazioni, ma soprattutto organizzare e far circolare i dati o interconnettere i sistemi. Sul sostanziale vuoto legislativo entro cui sono proliferate le prime banche di dati, v. anche G. BUTTARELLI, *Banche dati e tutela della riservatezza. La* privacy *nella Società dell'informazione*, Giuffrè, Milano, 1997, 106 ss.

occulta, i cittadini hanno manifestato una crescente esigenza di trasparenza. Nella legislazione degli anni '80, tale esigenza ha preso forma in una protezione non fondata più sulla mera reazione individuale innanzi ad una violazione, bensì su un potere di controllo diretto e continuo sui dati e su coloro che raccolgono dati, nella prospettiva di garantire una circolazione "controllata" delle informazioni[63].

Successivamente, i cambiamenti imposti dalla diffusione dei *personal computer*, la più ampia trasformazione del sistema informativo e la valenza economica acquisita dalle informazioni nel sistema produttivo, hanno indotto i cittadini a reclamare un controllo ancora più stringente sui propri dati e, soprattutto, una partecipazione più attiva alla relativa gestione[64]. Si assise così alla diffusione di una nuova generazione di interventi legislativi che, a partire dalla metà degli anni '90, accorda un ruolo centrale al consenso informato dell'interessato[65] e alla trasparenza del trattamento che consegue anche solo dalla mera raccolta dei dati[66].

[63] Cfr. V. FROSINI, *Informatica, diritto e società*, cit., 200 ss.; S. RODOTÀ, *Tecnologie e diritti*, il Mulino, Bologna, 1995, 61 ss. e 105 ss., che rilevano come, con tale legislazione, il potere di controllo individuale venisse allargato attraverso un ampliamento dei casi in cui la legittimità della raccolta richiedeva il consenso dell'interessato; si attribuisse un potere generale di sorveglianza ad organi appositamente creati; si accordasse un diritto di accesso diretto agli interessati.

[64] Si osserva in V. ZENO-ZENCOVICH, *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium iuris*, 1997, 469, come il consenso dell'interessato al trattamento dei dati viene generalmente ottenuto dietro un corrispettivo, così da portare ad una progressiva patrimonializzazione degli aspetti della personalità e dei dati rilevatori di essa. Che il valore economico assunto dalle informazioni costituisca uno dei fattori di sviluppo della società dell'informazione è sostenuto anche da S. FARO, *Trattamento dei dati personali e tutela della persona*, in *Dig. disc. pubbl.*, Agg. I, Torino, 2000, 544 ss., che sottolinea come gli operatori economici privati avvertano sempre più l'esigenza di elaborare le informazioni per la realizzazione delle proprie strategie imprenditoriali.

[65] Cfr. S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. Dir. Civ.*, 6, 2001, 626 ss.

[66] V. E. GIANNANTONIO, *Dati personali (tutela dei)*, in *Enc. dir.*, Agg. III, 1999, 484, che osserva come i diritti all'onore, alla riservatezza e alla identità personale hanno per oggetto il valore dell'individuo nella considerazione sociale e disciplinano i dati personali non in sé, ma in quanto la loro comunicazione o la loro diffusione abbiano leso tale valore. L'art. 1, della legge n. 675/1996, invece, identifica come "trattamento"

La consacrazione espressa a livello normativo avviene poi con la già citata legge n. 675/1996, tramite la quale la protezione dei dati personali viene finalizzata alla garanzia di una molteplicità di diritti come quello alla riservatezza e alla identità personale, e più in generale alla garanzia della dignità e delle libertà fondamentali dell'interessato[67].

Si consuma quindi il passaggio da un approccio "statico" della tutela della *privacy*, secondo una accezione "negativa" volta ad escludere la conoscenza e le interferenze altrui dai propri fatti e opinioni, al diritto "positivo" a mantenere un controllo sull'insieme dei dati che costituiscono il riflesso del modo di essere della persona nella società dell'informazione: si sostanzia cosi il concetto di "autodeterminazione informativa"[68], secondo una prospettiva "dinamica" nella quale la tutela segue i dati con la loro circolazione, entro spazi oramai senza confini fisici[69].

Attualmente, i mezzi disponibili all'interno dell'universo digitale e del *web* favoriscono un numero crescente di processi di interazione sociale (si pensi ai *social network*); consentono l'accesso ad una vasta

la raccolta, registrazione, organizzazione, conservazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, cancellazione e distruzione di dati. La comunicazione e la diffusione sono quindi una modalità con cui l'attività disciplinata può manifestarsi.

[67] V. S. CALZOLAIO, *Protezione dei dati personali*, in *Dig. Disc. Pubbl.*, Agg. VII, 2017, 613, che osserva come in realtà il concetto fosse già stato formalizzato tramite l'istituzione del "Garante per la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" (art. 30, c. 1, legge n. 675/1996), che a seguito delle modifiche apportate dall'art. 3, c. 1, del d.lgs. n. 123/1997, assunse la denominazione di "Garante per la protezione dei dati personali".

[68] A partire dalla nozione elaborata dal Tribunale costituzionale tedesco con la sent. del 15 dicembre del 1983; cfr. S. RODOTÀ, *Tecnologie e diritti*, cit., 108; ID., *Persona, riservatezza, identità*, cit., 588 ss.; ID., *Il diritto di avere diritti*, cit., 396. Più in generale, v. anche L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale Scientifica, Napoli, 2016, spec. 96 ss.

[69] Così S. RODOTÀ, *Il diritto di avere diritti*, cit., 397 s., con uno spunto ripreso anche da C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli, 2017, 87. Sul punto, si ricordino le politiche europee volte ad istituire un *Single Digital Market* entro cui venga garantito il "*free flow*" di dati; cfr. EUROPEAN COMMISSION, Communication "*A Digital Single Market Strategy for Europe*" SWD(2015) 100 final, 6 maggio 2015.

quantità di informazioni da cui trarre conoscenze; rendono disponibile la fornitura di beni e servizi in modi fino a poco tempo fa inimmaginati; ma portano con sé anche inedite forme di sorveglianza, controllo, classificazione e selezione delle persone.

Le TRF sono in grado di servire esattamente a questi ultimi scopi. Si risente un'eco dei timori legati a quelle prime forme di controllo derivanti dalla costruzione di "banche di dati" e dalla concentrazione di un nuovo "potere informatico". Compiendo un salto di oltre mezzo secolo, però, ci troviamo immersi in quel processo di "datificazione" della società che, come è stato ricordato, caratterizza l'epoca dei *big data*. Tale processo può anche assumere la forma della c.d. "*dataveillance*" (forma contratta di *data-surveillance*), intesa come "impiego sistematico dei dati personali per indagare o monitorare le azioni o le comunicazioni di una o più persone"[70]. Si tratta di una tipologia di sorveglianza che non assume necessariamente una accezione negativa[71], in quanto può, ad esempio, costituire uno strumento per ottimizzare l'economia o consentire ai cittadini di operare un controllo più efficace sulle politiche dei propri governanti[72]. Come detto introduttivamente, però, l'imperativo che impone di raccogliere sempre più dati e metadati può tradursi, per le autorità di governo, nelle citate pratiche di sorveglianza digitale di massa a tutela della sicurezza pubblica e, per le imprese, nella corsa a comprendere, prevedere e manipolare i comportamenti delle persone e della società, nella forma definita come "capitalismo della sorveglianza"[73]. Ne conseguono nuove possibilità di tracciare, quantificare, prevedere il comportamento umano e le dinamiche sociali che – secondo l'accezione più marcata e ideologica del c.d. "*dataismo*"[74] – si credono addirittura più oggettive di quelle accessibili alla conoscenza umana.

[70] Cfr. R. CLARKE, *Information Technology and Dataveillance*, in *Communications of ACM*, 5, 31, maggio 1988, 499 (trad. nostra).

[71] *Ivi*, 498 s.; R. RALEY, *Dataveillance and Countervailance*. in L. GITELMAN (a cura di), *'Raw Data' is an Oxymoron*, MIT Press, Cambridge, 2013, 121 ss.

[72] Aspetto rimarcato in P. PERRI, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, cit., 25.

[73] V. *retro* Introduzione.

[74] J. VAN DIJCK, *Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology*, in *Surveillance & Society*, 12, 2, 2014, 197 ss.

Si tratta di fenomeni speculari a quelli che interessano il diritto all'identità digitale. Attraverso questi processi trasformativi i corpi delle persone "scompaiono"[75], vengono cioè separati in flussi di dati discreti per essere poi diversamente "assemblati" per le diverse finalità[76]. Le persone possono subire questi fenomeni passivamente o inconsapevolmente, oppure – come accade molto spesso – ne sono pienamente partecipi, contribuendo alla costruzione del proprio "*quantified-self*"[77]. Quelle che in passato potevano apparire fantasie, dunque, costituiscono oggi una realtà sperimentabile da chiunque.

Per fronteggiare questi pericoli è stata paventata la costruzione di categorie giuridiche come l'*habeas data*, in aggiunta al *habeas corpus*, quale portato della proiezione della persona umana nel mondo dei dati ed espressione della sua autodeterminazione informativa[78]. Oppure si è parlato di una "cittadinanza digitale", quale condizione che accompagna le persone nel loro essere nel mondo fisico e nel ciberspazio e, di conseguenza, integra la loro dotazione di diritti[79]. Nel contesto attuale, dunque, la protezione dei dati della persona appare ancor più decisiva che in passato, non soltanto in vista del controllo sui propri dati, ma a presidio più complessivamente del libero sviluppo della personalità, nel rapporto con gli altri consociati e nelle garanzie nei confronti di tutti i soggetti che esercitano un potere sui dati[80]. Anche per questo motivo, la normativa sulla protezione dei dati personali, che peraltro offre il quadro più organico per la disciplina delle TRF, dovrà essere fatta oggetto di specifica attenzione[81].

[75] D. LYON, *La società sorvegliata*, cit., 19.

[76] K.D. HUGGERTY, R.V. ERICSON, *The surveillant assemblage*, in *British Journal of Sociology*, 51, 4, 2000, 605 ss.

[77] Con "*quantified-self*" si intende il coinvolgimento della persona nell'autotracciamento di ogni tipo di informazioni biologiche, fisiche, comportamentali o ambientali; fenomeno sempre più imponente grazie alla diffusione dei c.d. *wearable devices*, di cui gli *smart watch* offrono l'esempio più conosciuto. Cfr. M. SWAN, *The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery*, in *Big Data*, 1, 2, 2013, 85.

[78] Sul punto, basti rinviare a S. RODOTÀ, *Dal soggetto alla persona*, Editoriale Scientifica, Napoli, 2007, 20, e più di recente S. PIETROPAOLI, Habeas Data. *I diritti umani alla prova dei* big data, in T.E. FROSINI, S. FARO, G. PERUGINELLI, *Dati e algoritmi: diritto e diritti nella società digitale*, il mulino, Bologna, 2019, 97 ss.

[79] S. RODOTÀ, *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, 384 s.

[80] S. CALZOLAIO, *Protezione dei dati personali*, cit., 603.

[81] V. *infra* Cap. III, par. 2.

5. *Effetti diretti e indiretti sull'*habeas corpus

Il ricorso alle TRF implica una interferenza anche con ulteriori libertà individuali espressamente sancite dalla Costituzione. Il riferimento va innanzitutto alla *libertà personale*, paradigma e modello per la tutela di altri diritti di libertà. Occorre subito anticipare, tuttavia, come risulti alquanto problematico stabilire se vi sia una correlazione diretta fra TRF e libertà personale. L'esito di questo giudizio, infatti, dipende fondamentalmente dai contenuti e dalla portata che si vuole riconoscere a quest'ultima libertà.

Per stabilire se effettivamente le TRF chiamino in gioco la libertà personale bisogna innanzitutto guardare al bene tutelato e alle facoltà e poteri ricompresi nella libertà all'art. 13 Cost. La dottrina si è interrogata a lungo sul punto, mentre la giurisprudenza costituzionale ha preso forma in una serie di indirizzi invero piuttosto oscillanti a seconda degli elementi e dei criteri cui riferirsi.

Un primo aspetto è quello legato al grado di *coercizione fisica* della misura limitativa della libertà personale[82]. In accordo con una interpretazione più restrittiva, la libertà in questione andrebbe circoscritta alla sola libertà fisica, da tutelare contro misure coercitive arbitrarie, fra cui le tipologie indicate ai commi 2 e 3 dell'art. 13 Cost.: in questo senso, la libertà personale dovrebbe intendersi ricollegata alle garanzie del tradizionale *habeas corpus*[83]. Secondo un certo indirizzo della giuri-

[82] Cfr. ad es. C.cost., sent. 27 giugno 1996, n. 238, sulla questione dei prelievi ematici coattivi, ove la Corte chiarisce come tale misura necessiti di attenta valutazione da parte del legislatore «nella determinazione dei "casi e modi" in cui può esser disposta dal giudice - in quanto non solo interessa la sfera della libertà personale, ma la travalica perché, seppur in minima misura, invade la sfera corporale della persona - pur senza di norma comprometterne, di per sé, l'integrità fisica o la salute (anche psichica), né la sua dignità».

[83] In questo senso, A. PACE, *Problematica delle libertà costituzionali. Parte speciale*, cit., 172 ss. (v. nota 2 per i dovuti distinguo rispetto alla disciplina anglosassone dell'*habeas corpus*), anche in contrapposizione alle ipotesi ricostruttive più ampie di cui si dirà a breve: a detta dell'A., non si può ritenere che la libertà personale tuteli la persona contro misure degradanti della dignità sociale, poiché lascerebbe tale libertà priva di tutele a fronte di limitazioni che non siano socialmente degradanti, e neppure che si estenda alla "libertà spirituale" o "morale", in quanto finirebbe con l'imporre l'intervento dell'autorità giudiziaria a tutte le ipotesi di obblighi personali *ex* art. 23

sprudenza costituzionale, inoltre, viene stabilito – in termini non esenti da criticità – che gli atti che incidono solamente sull'aspetto esteriore dell'individuo, o impongono limitazioni lievi e momentanee, non sarebbero ascrivibili alle garanzie all'art. 13 Cost., nella specie la riserva di legge assoluta e la riserva di giurisdizione[84]. Tuttavia, anche in queste ipotesi, nel caso in cui mancasse il consenso dell'interessato, o comunque vi fossero conseguenze assimilabili nella sostanza ad una coercizione, si dovrebbe ricadere nel regime di tutela all'art. 13 Cost.[85].

Cost. che incidono sulla sfera morale. In senso analogo v. G. FILIPPETTA, *La libertà personale e le libertà di domicilio, di circolazione e individuale*, cit., 560 s. Puntualizza tale distinzione anche L. ELIA, *Libertà personale e misure di prevenzione*, Giuffrè, Milano, 1962, 73, che accede ad una concezione di libertà personale limitata all'*habeas corpus* (86). Con i dovuti distinguo, v. anche G. AMATO, *Art. 13*, cit., 51 s.

[84] V. C.cost., sent. 22 marzo 1962, n. 30, resa a proposito dei rilievi segnaletici di cui all'art. 4 t.u.l.p.s., con cui la Corte ha stabilito che i rilievi fotodattiloscopici non comportano una restrizione della libertà personale, e questo non tanto per la «momentaneità» o «levità» della eventuale coercizione, che potrebbe implicare anche una immobilizzazione del soggetto, quanto per il loro incidere esclusivamente «sull'aspetto esteriore della persona la cui sfera di libertà resta integra». La Corte ha inoltre chiarito che la decisione resa «non è – e non potrebbe essere – una soluzione definitiva», in quanto questa «spetta unicamente al legislatore». Critico su questa decisione A. PACE, *Problematica delle libertà costituzionali. Parte speciale*, cit., 179 s., in quanto dovrebbero rientrare nella tutela della libertà personale tutte le misure coercitive non obbligatorie, indipendentemente dal grado di invasività, o cui potrebbe far seguito una immediata coazione in caso di non ottemperanza. Nella sent. 27 gennaio 1972, n. 13, sull'accompagnamento coattivo *ex* art. 15, c. 2, t.u.l.p.s., la Corte poi ha stabilito che, sebbene vi sia un'interferenza con la libertà personale, tale misura non necessiti di una convalida giurisdizionale *ex* art. 13, c. 3 Cost., poiché «il provvedimento incide in modo del tutto temporaneo» sulla libertà personale. Di interesse anche la sent. n. 105/2001 (e le successive sent. n. 222/2004 e ord. 109/2006), in tema di accompagnamento alla frontiera e trattenimento nei centri di permanenza temporanea dello straniero, ove la Corte riconosce come vi sia un «assoggettamento fisico all'altrui potere» e svolge incidentalmente un riferimento alla «*immediata* coercizione che qualifica, per costante giurisprudenza costituzionale, le restrizioni della libertà personale» (enfasi aggiunta), accostando così il requisito della immediatezza ai criteri tradizionali.

[85] Propende per una distinzione tra coercizione e obblighi anche A. CERRI, *Libertà personale (dir. cost.)*, in *Enc. giur.*, XXI, 1991, 5, salvo poi dover enucleare in termini piuttosto ampi quali ipotesi di obblighi si risolvano sostanzialmente in coercizioni, come ad esempio quegli obblighi che non lasciano alcuna discrezione sull'adempimento, che sono eseguibili in forma specifica, o presidiati da sanzione pe-

Secondo questo indirizzo, dunque, il ricorso alle TRF non inciderebbe sulla libertà personale, a meno che – ma anche qui, come si vedrà, si potrebbe nutrire qualche dubbio – il rifiuto alla relativa sottoposizione non faccia scattare l'uso della forza[86].

In altre pronunce il criterio maggiormente enfatizzato è stato invece quello della "*degradazione giuridica dell'individuo*". Diverse ricostruzioni dottrinarie hanno ricondotto tale degradazione, oltre che alla violazione dell'*habeas corpus*, soprattutto alla lesione della "libertà morale"[87] o della "dignità sociale"[88] della persona nella quale si risolve la coercizione, con una accezione, però, non indenne da criticità nella relativa estensione e nelle tutele ad essa connesse. Nella giurisprudenza costituzionale tale degradazione si fa solitamente conseguire ad una menomazione che implichi un «assoggettamento totale della persona all'altrui potere»[89]. Il più delle volte, tuttavia, la "degradazione" e

nale o che incidono comunque su un diritto inviolabile. Di "linea sottile" che separa coercizione da obblighi pressante parlano anche A. BARBERA, F. COCOZZA, G. CORSO, *Le situazioni soggettive. Le libertà dei singoli e delle formazioni sociali. Il principio di uguaglianza*, in G. AMATO, A. BARBERA (a cura di), *Manuale di diritto pubblico*, I, il Mulino, Bologna, 1997, 245.

[86] Cfr. C.cost., sentt. n. 419/1994, n. 210/1995, n. 194/1996, sulle misure di prevenzione non lesive dell'art. 13 Cost. ove non suscettibili di coercitiva esecuzione. Sull'uso della forza in questo senso v. anche A. PACE, *Problematica delle libertà costituzionali. Parte speciale*, cit., 181 ss.

[87] Il riferimento più ampio alla "libertà morale" è presente invece in P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., 111 s., che ritiene come l'art. 13 Cost. sia ispirato al paradigma della *nonviolenza*, fisica e spirituale, e pertanto varrebbe a coprire anche le violazioni della libertà spirituale che si risolvono, tramite imposizione di obblighi o limiti alla libertà di autodeterminazione, in una restrizione delle possibilità fisiche dell'individuo.

[88] Sarebbero lesive della libertà personale anche le misure che, attraverso limiti alla libertà fisica, colpiscono la "personalità morale" e la "dignità sociale" della persona, (*contra* sent. n. 27/1959, sull'obbligo di non associarsi abitualmente alle persone che hanno subito condanne e sono sottoposte a misure di prevenzione o di sicurezza e di non partecipare a pubbliche riunioni); cfr. A. BARBERA, *I principi costituzionali della libertà personale*, Giuffrè, Milano, 1967, spec. 119 ss.

[89] Secondo questa giurisprudenza costituzionale anche gli atti non coercitivi incidono sulla libertà personale in presenza dei citati elementi; v. C.cost., sent. n. 11/1956, sull'istituto dell'ammonizione, che concretava una restrizione della libertà personale che si risolveva in una sorta di degradazione giuridica attraverso una serie di obblighi

l'"assoggettamento" derivano proprio dalla sottoposizione alla coercizione fisica, così da rendere difficile disgiungere i due profili[90].

A differenza di quanto accade con il criterio della coercizione, adoperando questa seconda accezione non sarebbe del tutto fuori luogo ipotizzare, in termini generali, che la sottoposizione a TRF possa confliggere con la libertà personale. Ci troveremmo dinanzi a misure dirette al singolo in ragione di una sua condotta o della sua presenza in un determinato luogo, in grado, nella sostanza, di produrre una condizione e uno stato psicologico di "assoggettamento" conseguente ad un potere di sorveglianza così penetrante. Questo potere – come già sottolineato – è suscettibile di indurre le persone a cambiare comportamenti e abitudini, pur di sottrarsi a forme di controllo che possono essere percepite anche come umilianti.

La questione rimane aperta, dato che le circostanze e il contesto storico, sui quali influiscono anche le innovazioni tecnologiche e le loro potenzialità lesive, non consentono di delimitare nettamente i confini della libertà personale rispetto alle altre libertà garantite in Costituzione[91], come emerso chiaramente anche di recente con le limitazioni

di fare e di non fare, tra cui quello di non uscire prima e di non rincasare dopo di una certa ora; salvo poi ritenere che non costituisse limitazione *de qua* il foglio di via obbligatorio con ordine di rimpatrio non suscettibile di esecuzione coercitiva (n. 68/1964; n. 210/1995). Favorevole ad estendere la libertà personale, intesa come libertà fisica, anche a questi limitati profili della libertà personale anche M. OLIVETTI, *Diritti fondamentali*, Giappichelli, Torino, 2018, 194 ss.

[90] V. C.cost., sentt. n. 23/1975, in tema di ispezioni sui lavoratori; n. 99/1980, in tema di visite di controllo sui lavoratori; n. 419/1994, sull'istituto del soggiorno cautelare nel contrasto alla criminalità mafiosa, consistente nell'obbligo di soggiorno in una località determinata; ma si consideri anche sent. n. 194/1996, in tema di accertamenti tossicologici del conducente, che non ritiene l'accompagnamento per la sottoposizione al test una limitazione della libertà personale, in quanto il soggetto «non subisce coartazione alcuna, potendosi rifiutare in caso di ritenuto abuso di potere da parte dell'agente», salvo incorrere nel reato *ex* art. 187 c.p.

[91] In questo senso ci si pone in scia della già citata concezione della libertà personale come "libertà-situazione", aperta alla tutela verso quelle forme di esercizio di poteri che, nel momento storico, potrebbero rivelarsi pericolosi per la libertà (cfr. AMATO, *Art. 13*, cit., 1 ss.). Di "questione aperta" circa il confine con le altre libertà, rimessa agli equilibri tra legislatore, giudici e autorità di p.s., parla P. CARETTI, *La libertà personale*, in G. SANTANIELLO (diretto da), *Trattato di diritto amministrativo*, XII, Cedam, Padova, 1990, 64 ss., che propende però per ricondurre alle ga-

imposte dalle misure di contrasto all'emergenza epidemiologica da Covid-19[92].

In ogni caso, sia che si intenda la libertà personale come garanzia della propria persona fisica contro le coercizioni, sia che si estenda tale libertà anche alla dimensione morale, residua la possibilità che la sottoposizione ad un procedimento di identificazione tramite TRF senza il proprio consenso sia configurabile come imposizione di un "obbligo personale", riconducibile al contiguo regime dell'art. 23 Cost.[93]. Quest'ultima previsione assume quindi una valenza residuale[94], tendente ad includere ogni forma di obbligo, imperativo o comando, in senso positivo o negativo[95], non salvaguardata da altra e più intensa tu-

ranzie di tale libertà le misure caratterizzate da "personalità" e per la loro "finalizzazione".

[92] Il problema dei confini della libertà personale rispetto ad altre libertà – segnatamente quella di circolazione – è tornato alla ribalta a causa di tali misure; sul punto, per quanto qui di maggiore interesse, v. R. CHERCHI, A. DEFFENU, *Fonti e provvedimenti dell'emergenza sanitaria covid-19: prime riflessioni*, in *Diritti regionali*, *Forum "La gestione dell'emergenza sanitaria tra Stato, Regioni ed Enti locali"*, 23 aprile 2020, 656 ss.; M. BIGNAMI, *Chiacchiericcio sulle libertà costituzionali al tempo del coronavirus*, in *Questione Giustizia*, 7 aprile 2020, 7; A. RUGGERI, *Il coronavirus contagia anche le categorie costituzionali e ne mette a dura prova la capacità di tenuta*, in *Diritti regionali*, 1, 2020, 375.

[93] Rispettivamente, secondo A. PACE, *Problematica delle libertà costituzionali. Parte speciale*, cit., 174 ss., ove non vi fosse coercizione occorrerebbe più propriamente parlare di "obblighi" ricadenti nell'art. 23 Cost.; secondo P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., 111 s., gli obblighi personali dovrebbero giustificarsi con altri interessi costituzionali e non potrebbero comunque andare a ledere la sfera della libertà morale.

[94] Cfr., da ultimo, D. MORANA, *Articolo 23*, in F. CLEMENTI, L. CUOCOLO, F. ROSA, G.E. VIGEVANI (a cura di), *La Costituzione italiana. Commento articolo per articolo*, I, il Mulino, Bologna, 2018, 160. Si legge in C.cost., sent. n. 115/2011, come la riserva di legge all'art. 23 Cost. «ha indubbiamente carattere relativo, nel senso che lascia all'autorità amministrativa consistenti margini di regolazione delle fattispecie in tutti gli ambiti non coperti dalle riserve di legge assolute, poste a presidio dei diritti di libertà, contenute negli artt. 13 e seguenti della Costituzione» (5 cons. dir.).

[95] Tra i tentativi di offrire una definizione di "prestazione personale", si segnala quella tendente a ricondurvi «tutte le attività che si traducono nell'esplicazione di energie fisiche e intellettuali, limitando le facoltà di determinazione, da parte del privato, della destinazione delle energie medesime», comprensiva anche degli obblighi di «presentazione personale» (cfr. A. FEDELE, *Art. 23*, in G. BRANCA (a cura di), *Com-*

tela riconosciuta in Costituzione, prestando così la garanzia della riserva di legge relativa ivi stabilita[96].

Al di là della valutazione astratta sulla pertinenza delle TRF rispetto alla libertà personale, occorre domandarsi se l'impiego di queste tecnologie, soprattutto a scopi identificativi nell'ambito del procedimento penale, sia in grado di produrre effetti equivalenti a quelli delle misure presidiate dalle garanzie all'art. 13 Cost., determinando così un sostanziale aggiramento della tutela costituzionale.

L'interrogativo si risolve, innanzitutto, nella possibilità o meno di assimilare le TRF alla stregua di "*mezzi atipici di ricerca della prova*", ossia mezzi di ricerca della prova diversi da quelli espressamente disciplinati dal codice e ammissibili ai sensi dell'art. 189 c.p.p.[97].

Su questo versante, in assenza di una disciplina legislativa che spe-

mentario della Costituzione, Zanichelli - Foro italiano, Bologna-Roma, 1978, 43; in senso conforme, L. ANTONINI, *Art. 23 Cost.*, in A. CELOTTO, R. BIFULCO, M. OLIVETTI (a cura di), *Commentario alla Costituzione*, Utet, Torino, 2006, 491 s.). La dottrina e la giurisprudenza vi farebbero dunque rientrare varie fattispecie come il servizio militare; il servizio di lavoro in caso di guerra; le prestazioni richieste dall'autorità sanitaria comunale nell'interesse dei servizi di difesa in caso di epidemia; le prestazioni richieste in caso di tumulti, di pubblici infortuni, di comune pericolo, di flagranza di reato; ipotesi il cui oggetto della prestazione è un'attività professionale (es. la prestazione della difesa gratuita per gli avvocati) o i casi in cui oggetto della prestazione è l'assunzione di una carica (es. giudice popolare nelle Corti di Assise) (cfr. A. FEDELE, *Art. 23*, cit., 39 ss.). La giurisprudenza costituzionale, dunque, ne ha definito i contenuti nel corso degli anni, tramite una casistica non lineare che guarda a diversi profili, come le finalità, in presenza di «ragioni di interesse generale» collegate alla tutela di un diritto costituzionale (cfr. C.cost., sent. n. 114/1964, relativa all'imposizione di prestazione rappresentata dal patrocinio gratuito dei non abbienti) o i contenuti della prestazione, come obblighi di «fare» e di «non fare» (C.cost., sent. n. 115/2011, relativa al potere di ordinanza contingibile ed urgente dei sindaci).

[96] Su cui v. anche *infra* Cap. IV, par. 7.

[97] La previsione codicistica si riferisce alla prova non disciplinata dalla legge, che può essere assunta dal giudice se «risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona». Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova. Tale previsione è riferibile anche ai mezzi di ricerca della prova, con la particolarità che il contraddittorio, in tal caso, non è preventivo, ma si svolge successivamente all'acquisizione nel momento in cui il giudice ne valuta l'assunzione in dibattimento; cfr. Cass. sez. un. 28 luglio 2006, n. 26795.

cifichi quali sono i criteri attraverso cui valutare tale ammissibilità, è alle elaborazioni della dottrina e della giurisprudenza che bisogna guardare. A venire in gioco, in particolare, è il c.d. *principio di non sostituibilità*, in forza del quale non è possibile eludere le regole sostanziali e le garanzie previste per l'atto tipico qualificandolo fraudolentemente come atipico; un principio a protezione del canone di legalità che informa il sistema probatorio, ovvero del compito riconosciuto alla legge di tracciare i limiti dell'*an* e del *quomodo*, nel tentativo di bilanciare l'apertura del procedimento penale all'impiego dei più moderni mezzi tecnologici con l'assenza di una esplicita disciplina[98].

In mancanza di riferimenti diretti alle TRF, sono gli indirizzi elaborati rispetto alle videoriprese ad offrire spunti di maggiore interesse in relazione alla tutela dei diritti fondamentali che vengono in concreto implicati.

A questo proposito, occorre innanzitutto distinguere tra le riprese di comportamenti non comunicativi, da ricondurre al regime delle intercettazioni e alle garanzie previste per la libertà di comunicazione all'art. 15 Cost., e riprese di comportamenti non comunicativi, alle quali invece pare possano essere assimilate le TRF[99].

[98] Su tutti, cfr. P. TONINI, *Manuale di procedura penale*, GFL, Milano, 2019, 422 ss.; C. CONTI, *Prova informatica e diritti fondamentali*, in *Diritto penale e processo*, 9, 2018, 1210 ss.; P. TONINI, C. CONTI, *Il diritto delle prove penali*, Giuffrè, Milano, 2014, 196 ss. Il principio si può ritenere emerso di pari passo con la questione della prova incostituzionale, affrontata in C.cost., sent. 19 giugno 1998, n. 229, in tema di sequestro degli appunti dell'indagato predisposti in vista dell'interrogatorio, ove si stabilisce che le norme sul sequestro devono essere lette in modo tale da individuare confini netti rispetto agli altri strumenti predisposti dal codice, evitando di aggirare surrettiziamente la garanzia del diritto al silenzio che spetta all'indagato nell'interrogatorio o la generale inviolabilità della libertà morale *ex* art. 188 c.p.p. Più di recente, v. Cass. SS.UU., 18 luglio 2012, n. 28997, e C.cost., sent. 24 gennaio 2017, n. 20, sulla distinzione tra captazione delle comunicazioni epistolari, per le quali è previsto il sequestro, e delle forme di comunicazione (ad es. telefoniche o informatiche), per le quali è prevista l'intercettazione.

[99] Così sulla scorta della distinzione operata in C.cost., sent. 24 aprile 2002, 135, e Cass. sez. un. 28 luglio 2006, n. 26795, sul rapporto tra intercettazioni di comunicazioni tra presenti e riprese visive; confermata successivamente anche in sent. 4 dicembre 2009, n. 320, in tema di agente segreto attrezzato per il suono, secondo cui, se nell'intercettazione il partecipante alla conservazione non si limita a registrarla, ma ne

Un secondo profilo attiene poi alla tutela offerta in relazione al luogo e alle condizioni in cui avviene la rilevazione. Se le TRF venissero impiegate in luoghi coperti dalla libertà di domicilio, come ad esempio un'abitazione privata, allora in mancanza di una previsione legislativa scatterebbe l'inutilizzabilità delle prove illegittimamente acquisite *ex* art. 191 c.p.p. Quando invece il ricorso a TRF avviene in luoghi "riservati", caratterizzati cioè dalla mancanza di stabilità dell'*ius excludendi* ma coperti dal diritto alla riservatezza, il riferimento si ritiene debba andare non alla garanzia di una previsione costituzionale assistita da riserva di legge, bensì più genericamente all'art. 2 Cost.: rimarrebbe comunque necessaria l'autorizzazione del P.M. per ammetterebbe l'utilizzabilità delle risultanze alla stregua di prova atipica[100]. Se invece il riconoscimento facciale dovesse avvenire in pubblico, allora non sarebbe richiesta l'autorizzazione del magistrato e la polizia giudiziaria potrebbe operare durante le attività inquirenti anche di propria iniziativa[101].

Un'ulteriore questione problematica, che ruota attorno alla capacità delle TRF di aggirare le garanzie previste per il cittadino negli atti compiuti durante le indagini preliminari, attiene alla identificazione in senso stretto[102]. Quest'ultima è costituita dall'atto non garantito con cui si risale alle generalità di una persona fisica individuata che, direttamente o indirettamente, ha avuto a che fare con un reato[103]. Nel caso in cui manchi il consenso dell'interessato e occorra intervenire coattivamente, il codice rende necessaria l'autorizzazione del P.M. per l'identificazione dell'indagato tramite il prelievo di capelli o saliva, o la

trasmette i contenuti alla p.g., in questo caso si rientra pienamente nelle intercettazioni e nelle garanzie all'art. 15 Cost.

[100] Cfr. anche Cass. sez. I, 18 dicembre 2008, n. 4422.

[101] Qualora le immagini fossero riprese nei luoghi domiciliari, ma il comportamento sia in concreto non riservato in quanto liberamente osservabile dagli estranei senza ricorrere a particolari accorgimenti, allora la rilevazione sarebbe assimilata alle videoriprese in luoghi pubblici; cfr. anche C.cost., sent. 7 maggio 2008, n. 149.

[102] Più ampiamente, cfr. P. FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Ipsoa, Assago, 2007, 85 ss., ed i rinvii ivi contenuti.

[103] Art. 349, c. 1, c.p.p. Nei confronti dell'indagato si può procedere «anche eseguendo, ove occorra, rilievi dattiloscopici, fotografici e antropometrici nonché altri accertamenti (c. 2).

comunicazione allo stesso per disporre l'accompagnamento agli uffici di polizia della persona che rifiuti di fornire le proprie generalità, con la possibilità di trattenerla anche per dodici ore[104]. Si consideri, inoltre, che analoghe previsioni a tutela nei confronti dell'accompagnamento coattivo sono previste anche al di fuori del procedimento penale, in tutti quei casi in cui una persona rifiuti di fornire le proprie generalità alle forze dell'ordine o queste abbiano sufficienti indizi per ritenere la falsità delle relative dichiarazioni o dei documenti[105].

La sottoposizione a TRF, non implicando di per sé un intervento coattivo, non sembra giustificare da questo punto di vista la mera estensione delle garanzie sopra richiamate, anche se in questo modo l'assenza del consenso dell'interessato verrebbe del tutto svuotata della sua valenza oppositiva atta ad innescare il necessario intervento del magistrato.

Questa estensione andrebbe esclusa *a fortiori* se si considera la latitudine riconosciuta, nel caso di identificazione coatta, al diritto a non collaborare. Quest'ultimo può essere inteso come diritto a non fornire prove su se stesso, ricavabile dall'art. 24 Cost.[106]. Tale diritto, qualora la persona stessa costituisca "oggetto di ricerca"[107], ovvero, come nella

[104] Art. 349, rispettivamente c. 2-*bis* e c. 4. Nel secondo caso la persona può essere trattenuta fino a ventiquattro ore se l'identificazione risulta particolarmente complessa oppure occorre l'assistenza dell'autorità consolare o di un interprete. In astratto potrebbe venire anche in gioco l'istituto dell'accertamento tecnico operato per conto del P.M. idoneo ad incidere sulla libertà personale: durante le indagini preliminari, il P.M. può nominare consulenti tecnici quando occorra svolgere rilievi segnaletici, descrittivi o fotografici e ogni altra operazione tecnica per cui sono necessarie specifiche competenze, in presenza del consenso dell'interessato (art. 359, c. 1, c.p.p.). Qualora invece manchi il consenso, si può ricorrere al prelievo di capelli, di peli o di mucosa del cavo per determinare il profilo genetico o accertamenti medici con le medesime garanzie previste per la perizia *ex* art. 224-*bis*, ovvero la richiesta di autorizzazione al G.I.P. da parte del P.M.

[105] Cfr. art. 11, d.l. 21 marzo 1978, n. 59, convertito con modificazioni dalla legge 18 maggio 1978, n. 191.

[106] Cfr. M. SCAPARONE, *Elementi di procedura penale. I princìpi costituzionali*, Giuffrè, Milano, 1999, 123.

[107] Sulla distinzione della persona come "organo" e come "oggetto", v. P. FELICIONI, *Considerazioni sugli accertamenti coattivi nel processo penale: lineamenti costituzionali e prospettive di riforma*, in *L'Indice penale*, 1999, 526.

identificazione, il suo corpo costituisca oggetto di prova, si risolve nella facoltà di non compiere alcun movimento fisico. Tuttavia, parrebbe legittima – anche se nient'affatto esente da criticità in punto di coercizione effettivamente subita[108] – l'imposizione di costrizioni che vedono l'interessato partecipare non attivamente, bensì come soggetto passivo di un mero *pati*, come avviene per lo svolgimento di rilievi fotografici o per il prelievo di impronte digitali e materiali organici, quand'anche occorra forzare la persona a subire il rilievo oppure immobilizzarla con la forza[109]. A maggior ragione, da questo punto di vista, la mera ripresa dell'immagine facciale non dovrebbe implicare una compressione della libertà personale.

A conclusioni in parte differenti si potrebbe giungere se si guardasse la questione nella prospettiva della incisione sulla "*libertà morale*", tutelata nell'assunzione della prova in base all'art. 188 c.p.p., ai sensi del quale «non possono essere utilizzati, neppure con il consenso della persona interessata, metodi o tecniche idonei a influire sulla libertà di autodeterminazione o ad alterare la capacità di ricordare e di valutare i fatti»[110]. Tale divieto impedisce il ricorso a metodi che influiscono sulla facoltà di reagire liberamente rispetto agli stimoli, o che sono idonei ad alterare la capacità di ricordare o valutare i fatti (si va dalla tortura fisica o psichica, alla narcoanalisi, l'ipnosi, il poligrafo)[111], o, in generale, riconducibili a manipolazioni psichiche atte a indurre in errore o indebolire la consapevolezza dell'interessato[112].

[108] A. PACE, *Problematica delle libertà costituzionali. Parte speciale*, cit., 179.

[109] M. SCAPARONE, *Elementi di procedura penale. I princìpi costituzionali*, cit., 124; P. FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, cit., 29 ss.

[110] Osserva P. FELICIONI, *Art. 188*, in A. GIARDA, G. SPANGHER (a cura di), *Codice di procedura penale commentato*, I, Wolters Kluwer, Milano, 2017, 1875, come tale norma esprima una regola di fondo a tutela della libertà morale nella formazione della prova, da ritenersi operativa anche in relazione agli strumenti conoscitivi impiegati durante le indagini preliminari, sia per le prove tipiche che per le prove atipiche.

[111] P. TONINI, *Manuale di procedura penale*, cit., 286.

[112] In F. CORDERO, *Procedura penale*, Giuffrè, Milano, 2012, 620, si rileva come «tale divieto colpisce qualunque intervento manipolante, grossolano o sottile: ad esempio le veglie coatte, [...] fame, sete, luce abbagliante, buio, caldo e freddo, esami estenuanti, messinscene traumatiche [...] e minacce, naturalmente [...] ovvero esche quali l'impunità o favori offerti sotto banco».

Questa accezione della libertà morale può essere ricondotta al divieto di «ogni violenza fisica e morale sulle persone comunque sottoposte a restrizioni di libertà», di cui all'art. 13, c. 4, Cost.[113]. Se si tiene fermo il criterio che rapporta le interferenze sulla libertà personale al grado di coercizione, sembrerebbe potersi sostenere che, anche sotto questa luce, la sottoposizione a riconoscimento facciale a scopi meramente identificativi non implichi una incisione sulla libertà morale, in quanto misura priva di quel "rapporto dialogico" tra la persona fonte di prova e l'autorità procedente che sembrerebbe invece richiesto[114]. Una traiettoria argomentativa diversa, invece, si potrebbe seguire se si valorizzasse una accezione più ampia della libertà morale, intesa come forma di autodeterminazione nelle proprie scelte difensive e negli atteggiamenti processuali "sul fatto proprio", a partire dalla regola incoercibile del *nemo tenetur se detegere*[115]. In questo caso, da una parte, potrebbero sorgere problemi già nell'ipotesi di accompagnamento coattivo, in quanto forma di coercizione indiretta che va ad incidere sulla libertà di autodeterminazione così tutelata[116]. Dall'altra, la sottoposizione a riconoscimento facciale in presenza dell'interessato e senza

[113] Cfr. G. VASSALLI, *Il diritto alla libertà morale (Contributo alla teoria dei diritti della personalità)*, in *Studi in memoria di Filippo Vassalli*, II, UTET, Torino, 1960, 1640 s.; P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., 111.

[114] Cfr. P. FELICIONI, *Art. 188*, cit., 1875 s.

[115] Cfr. G. DI CHIARA, *L'imputato e il diritto di difesa: il telaio dell'art. 24 Cost. E il "nuovo" catalogo dei diritti dell'«accusato»*, in G. FIANDACA, G. DI CHIARA, *Una introduzione al sistema penale*, cit., 270 ss., che rileva come l'art. 188 c.p.p. trovi *pendant* nella analoga regola all'art. 64, c. 2, c.p.p., a garanzia dell'imputato, che conferisce a questa forma di tutela della dignità della persona un ruolo centrale nell'impianto codicistico; una tutela peraltro incoercibile, stante l'inidoneità scriminante del consenso della persona.

[116] Cfr. M. NOBILI, *Art. 188 c.p.p.*, in M. CHIAVARIO (diretto da), *Commento al nuovo codice di procedura penale*, II, Utet, Torino, 1990, 396 s., che ravvisa in questa prerogativa una reminiscenza del metodo inquisitorio del processo penale, innegabilmente suscettibile di usi distorti rispetto a misure «destinate comunque ad incidere sulla libertà dell'accusato». Osserva G. VASSALLI, *Il diritto alla libertà morale (Contributo alla teoria dei diritti della personalità)*, cit., 1659 s., come, più in generale, una compressione della libertà morale si verifica nelle ipotesi in cui si incide sul proprio diritto di muoversi, come l'opposto diritto a mantenere la propria immobilità corporale.

il suo consenso, o addirittura in maniera occulta, sembrerebbe stridere con tale *ratio* garantistica, ove quest'ultima venisse concepita non soltanto nella dimensione dialogica con l'autorità procedente, ma fosse estesa anche al corpo della persona, considerato come "fonte di prova" di natura "dichiarativa" in grado di fornire indicazioni equivalenti alle dichiarazioni di chi collabora attivamente con il proprio interlocutore[117]. Pur dovendo salvaguardare le esigenze di segretezza o di rapidità nell'accertamento investigativo-processuale, in questa ipotesi si potrebbe immaginare un contemperamento, rispettoso del canone di proporzionalità[118], con la tutela della libertà di autodeterminazione, ad esempio informando la persona della natura e delle finalità dell'atto che subisce[119].

Problemi ben maggiori sorgerebbero poi dall'uso nel procedimento penale di quelle pratiche di analisi facciale volte a ricostruire la personalità di un soggetto o atte a verificare se stia o meno dicendo la verità[120]. Qui si ricadrebbe *de plano*, innanzitutto, nel divieto posto all'art. 188 c.p.p. di «pregiudicare la libertà morale della persona»[121]. Ma verrebbe seriamente in gioco anche un ulteriore requisito sancito dalla disposizione codicistica, ovvero la «idoneità» di tali tecnologie ad accertare i fatti, considerato che il ricorso a queste forme di riconoscimento e analisi del volto – come visto – vanno incontro a considerevoli margini di incertezza e di errore, di cui occorre senz'altro tener conto in fase di ammissibilità della prova scientifica e nel giudizio sulla relativa attendibilità[122].

[117] Cfr. C. FANUELE, *L'acquisizione occulta di materiale biologico*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2014, 321.

[118] Sulla rilevanza problematica del principio di proporzionalità quale valore generale implicito dell'ordinamento, con cui misurare l'ammissibilità e l'impiego dei nuovi strumenti tecnologici di controlli, v. in generale F. NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Diritto penale contemporaneo*, 2, 2018.

[119] Cfr. C. FANUELE, *L'acquisizione occulta di materiale biologico*, cit., 321.

[120] Cfr. *retro* Cap. I, par. 3.

[121] V. anche M. BONETTI, *Riservatezza e processo penale*, Giuffrè, Milano, 2003, 205.

[122] Si tratta delle problematiche legate all'ammissibilità della prova scientifica e alla verifica della qualità del sapere scientifico introdotto nel processo – di cui qui si può fare un mero cenno – elaborati con gli indirizzi giurisprudenziali inaugurati a partire

Se poi si riconoscesse un collegamento tra questa accezione ampia della libertà morale con un significato di libertà personale non comprensivo soltanto delle incoercibilità fisica, come sopra ipotizzato, allora la sottoposizione a riconoscimento facciale contro il volere dell'interessato potrebbe tradursi – ma il punto è invero problematico – in un condizionamento nella libertà di autodeterminazione tale da ridondare anche sul piano della libertà personale.

Al di là delle possibili interpretazioni estensive delle regole vigenti, tuttavia, bisogna osservare come anche solo la mancanza di una disciplina legislativa produce significative conseguenze in termini di tutela della persona. Questa anomia appare ancor più evidente se si compara la condizione giuridica in cui versano le TRF rispetto ad un altro potentissimo strumento identificativo a disposizione delle forze dell'ordine, quale l'analisi del DNA.

Vi sono certamente macroscopiche differenze tra riconoscimento facciale e identificazione genetica che potrebbero rendere un paragone azzardato: basti pensare alla irripetibilità delle caratteristiche genetiche di ognuno[123], a differenza delle somiglianze nei volti delle persone; l'immodificabilità dell'architettura genetica di qualsiasi individuo nonostante il passaggio del tempo, in contrapposizione al mutare dei trat-

da Cass., Sez. I, 21 maggio 2008, n. 31456 (Franzoni), e da Cass., Sez. IV, 17 settembre 2010, n. 43786 (Cozzini e altri), i quali sviluppano nel nostro ordinamento il c.d. *Daubert test*, introdotto dalla giurisprudenza statunitense a partire dal 1993: si fa riferimento a requisiti quali la verificabilità del sapere scientifico, la falsificabilità, la sottoposizione al controllo della comunità scientifica, la conoscenza del tasso di errore, la generale accettazione nella comunità degli esperti, l'affidabilità e l'indipendenza dell'esperto coinvolto, la considerazione delle finalità per le quali si muove, la possibilità di formulare criteri di scelta tra le contrapposte tesi scientifiche. In dottrina sul punto, v. P. TONINI, *La Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza*, in *Diritto penale e processo*, 11, 2011, 1341 ss.; C. CONTI, *Scienza controversa e processo penale: la Cassazione e il "discorso sul metodo"*, *ivi*, 6, 2019, 848 ss.; più ampiamente, v. anche O. DOMINIONI, *Prova scientifica (dir. proc. pen.)*, in *Enc. dir.*, Annali, II, t. I, 2008, 976 ss.; R. BARTOLI, *Diritto penale e prova scientifica*, in G. CANZIO, L. LUPÁRIA (a cura di), *Prova scientifica e processo penale*, Milano, Wolters Kluwer-Cedam, 2018, 75 ss.

[123] Cfr. P. FELICIONI, *La prova del DNA nel procedimento penale. Profili sistematici, dinamiche probatorie, suggestioni mediatiche*, Giuffrè, Milano, 2018, 27 ss., cui si rinvia anche per gli opportuni approfondimenti nella letteratura sulla genetica forense.

ti somatici[124]; la complessità e delicatezza delle attività tecnico-laboratoriali legate all'analisi del materiale biologico e alla conservazione delle risultanze, rispetto ai processi algoritmici che si svolgono nella dimensione virtuale[125]; l'alta affidabilità dell'identificazione tramite il DNA, a fronte del tasso di errore insito nel riconoscimento facciale, specie se operato dal vivo. In linea di massima, tuttavia, si possono segnalare anche delle analogie suggestive, a partire dalla valenza informazionale del dato genetico e delle immagini facciali, dai quali ricostruire i profili identificativi personali[126]; alla rilevanza dell'elemento probabilistico nel confronto tra il DNA ricavato dal campione biologico e l'indagato, o tra l'immagine e il soggetto ripreso[127]; alle fasi dei rispettivi procedimenti con cui avviene l'identificazione[128].

In contrapposizione al silenzio della legge sulle TRF, l'identificazione genetica trova invece riscontro in una disciplina *ad hoc*. Così, da una parte, si fa riferimento alla legge n. 85/2009 sui cana-

[124] Cfr. L. SCAFFARDI, *Giustizia genetica e tutela della persona. Uno studio comparato sull'uso (e abuso) delle banche dati del DNA a fini giudiziari*, Wolters Kluwer, Milano, 2017, cit., 26; tale immodificabilità rende quindi molto attendibile questa prova ai fini o meno di conferma delle ipotesi accusatorie.

[125] Sulle quali basti rinviare a P. GAROFANO, *Le attività tecniche: dal prelievo alla banca dati del DNA*, in S. SCARCELLA (a cura di), *Prelievo del D.N.A. e Banca dati nazionale*, Cedam, Padova, 2009, 79 ss.

[126] Sulla sempre maggiore attenzione della ricerca e degli studi al passaggio dalla dimensione fisica a quella informazionale della genetica, intesa come relazione consequenziale tra campione biologico, dato genetico e informazioni personali di origine genetica, cfr. M. TOMASI, *Genetica e Costituzione. Esercizio di eguaglianza solidarietà e responsabilità*, Editoriale Scientifica, Napoli, 2019, 5 ss., cui si rinvia per una approfondita analisi sul rapporto tra genetica e costituzionalismo nella prospettiva delle ricadute del principio personalista sulla medicina e ricerca clinica.

[127] P. FELICIONI, *La prova del DNA nel procedimento penale. Profili sistematici, dinamiche probatorie, suggestioni mediatiche*, cit., 26 s.

[128] Sembrerebbe possibile mettere a confronto: raccolta del materiale biologico / acquisizione dell'immagine facciale; estrazione del DNA / individuazione del volto; tipizzazione del profilo genetico / estrazione del modello biometrico; acquisizione e conservazione del profilo del DNA / registrazione del modello biometrico; raffronto tra il profilo acquisito e quelli presenti nella banca dati / confronto del modello biometrico con la galleria dei *template* biometrici già archiviati. Più approfonditamente, v. anche P. GAROFANO, *Le attività tecniche: dal prelievo alla banca dati del DNA*, cit., 79 ss.

li di alimentazione della banca dati nazionale del DNA[129], con la quale si distingue compiutamente a seconda della condizione in cui si trova il soggetto nei cui confronti avviene il prelievo del campione biologico[130]. Dall'altra, rimane fermo il combinato disposto offerto dalla disciplina codicistica sopra richiamata circa le modalità alle quali il prelievo coattivo deve avvenire durante un procedimento penale[131]. Tali coordinate normative, sebbene non possano ritenersi pienamente esaustive, soprattutto dove lasciano un ampio margine di discrezionalità alle forze dell'ordine sulle modalità di intervento, offrono comunque un parametro a garanzia dell'interessato.

Anche qui, tuttavia, la prassi ha da tempo escogitato alcune soluzioni per aggirare le garanzie costituzionali e processuali richiamate. Si tratta, ad esempio, delle pratiche occulte di raccolta del materiale biologico da parte delle forze dell'ordine, che prescindono dal consenso dell'interessato ma che non implicano alcun contatto fisico; pratiche che, fra l'altro, hanno anche ricevuto l'avallo della giurisprudenza di legittimità[132]. Anche in questo caso, però, sono state sollevate riserve a

[129] Cui si aggiunge il regolamento attuativo di cui al d.P.R. 7 aprile 2016, n. 87.

[130] In particolare, la legge n. 85/2009 distingue a seconda che il profilo genetico venga tratto da indagati, imputati o condannati già ristretti nella loro libertà personale (art. 9), che venga acquisito durante un procedimento penale non dalla persona (art. 10), oppure che venga elaborato da materiale biologico prelevato da cadaveri non identificati o da consanguinei di persone scomparse (art. 7, c. 1, lett. c). Nel secondo caso, la legge (art. 9, c. 2) stabilisce, in positivo, che l'acquisizione dei campioni biologici possa avvenire solamente se «si procede» nei confronti dei soggetti indagati, imputati o condannati per delitti non colposi per i quali è consentito almeno l'arresto in flagranza, e fornisce, in negativo, un elenco di reati per i quali non è possibile procedere a tale prelievo; cfr. P. FELICIONI, *L'acquisizione di materiale biologico a fini identificativi o di ricostruzione del fatto*, cit., 196 ss.

[131] La legge si applica in combinato disposto con le previsioni del c.p.p., per cui, se il profilo genetico è ottenuto da un prelievo coattivo senza il consenso dell'indagato, si applica la disciplina della perizia se disposto dal giudice (art. 224-*bis* c.p.p., introdotto dall'art. 24 della legge n. 85/2009) o dell'accertamento tecnico se disposto dal P.M. (art. 359-*bis* c.p.p., introdotto dall'art. 25 della legge n. 85/2009), o dell'identificazione coattiva dell'indagato se effettuata dalla polizia giudiziaria (art. 349, c. 2-*bis*); più ampiamente, v. P. FELICIONI, *L'acquisizione di materiale biologico a fini identificativi o di ricostruzione del fatto*, cit., 213 ss.

[132] Come nel caso in cui tale materiale si sia già staccato dal corpo e dunque non serva alcun intervento coercitivo (Cass., sez. I, 11 marzo 2003, n. 28979); ma si pensi

proposito dell'aggiramento delle forme di tutela da accordare alla libertà morale e di autodeterminazione dell'interessato[133].

Ancora una volta, dunque, si ha la riprova della difficoltà del diritto ad inquadrare e limitare le interferenze che tecnologie e tecniche innovative possono produrre sui diritti fondamentali, sebbene la presenza di una disciplina espressa possa contribuire senz'altro a questo scopo.

6. *Anonimato e spazio pubblico*

Le TRF mostrano un altro aspetto della loro utilità, e al contempo, della loro pericolosità, nel contributo che offrono al presidio della sicurezza pubblica, come accade per le manifestazioni caratterizzate da episodi di violenza.

Si pensi alle proteste che nel 2019 sono divampate a Hong Kong in occasione delle nuove misure legislative sull'estradizione, e a come l'uso di queste tecnologie per identificare i manifestanti abbia portato a utilizzare maschere o ombrelli per coprire i propri volti[134]. Anche negli Stati Uniti, a seguito della uccisione di Breonna Taylor e George Floyd nella primavera del 2020, le forze di polizia di numerose città americane hanno intensificato l'uso di queste tecnologie con la giustificazione di dover identificare gli autori di episodi di violenza durante le proteste che ne sono scaturite in tutto il Paese, contribuendo così a

anche all'ipotesi in cui il campione utilizzato per il test del DNA sia stato prelevato per altri scopi (Cass., sez. I, 22 giugno 1999, n. 10958); più ampiamente, anche per la casistica, cfr. P. FELICIONI, *La prova del DNA nel procedimento penale. Profili sistematici, dinamiche probatorie, suggestioni mediatiche*, cit., 185 ss.

[133] Critica su questa giurisprudenza, C. FANUELE, *L'acquisizione occulta di materiale biologico*, cit., 311 ss., con riferimento alle pratiche attraverso cui la raccolta del campione biologico è il risultato di una attività elusiva della consapevolezza del soggetto di "offrire" materiale probatorio.

[134] B. SCHMIDT, *Hong Kong Police Already Have AI Tech That Can Recognize Faces*, in *Bloomberg*, 22 ottobre 2019 [bloom.bg/3uqBESG]; Z. DOFFMAN, *Hong Kong Exposes Both Sides Of China's Relentless Facial Recognition Machine*, in *Forbes*, 26 agosto 2019 [bit.ly/3mqr4rV].

rendere questi strumenti ancora più invisi[135]. Più di recente, nel gennaio 2021, il Governo russo ha impiegato le TRF per perseguire i manifestanti scesi in piazza a seguito dell'arresto di uno dei leader dell'opposizione politica, Alexei Navalny[136].

Si tratta di esempi che mettono bene in luce come le TRF siano strumenti a disposizione anche di regimi che si dichiarano – a torto o a ragione – democratici per inibire le persone dall'esercitare, più o meno legittimamente, una serie di libertà e diritti. Sono situazioni nelle quali tende ad assottigliarsi il crinale tra tutela dell'ordine pubblico "materiale", inteso come stato materiale di pace, e perseguimento dell'ordine pubblico "ideale", da intendersi come conservazione del regime costituito, che nel nostro ordinamento si ritiene non possa trovare più accoglienza dopo l'esperienza fascista[137]. Queste tecnologie, dunque,

[135] Cfr. D. GERSHGORN, *Facial Recognition Is Law Enforcement's Newest Weapon Against Protesters*, in *OneZero*, 3 giugno 2020 [bit.ly/3mrvz5S]; N. DAVIES, *US police are using facial recognition technology at protests - adding to systemic racism*, in *Business & Human Rights Resource Center*, 18 agosto 2020 [bit.ly/39LPV4q]; K. COX, *Cops in Miami, NYC arrest protesters from facial recognition matches*, in *Ars Technica*, 19 agosto 2020 [bit.ly/3s0lcXv].

[136] Cfr. M. GESSEN, *Across Russia, Pro-Navalny Demonstrations Continue to Build Momentum*, in *The New Yorker*, 2 febbraio 2021 [bit.ly/3dJX46J]; G. STOLYAROV, G. TÉTRAULT-FARBER, *"Face control": Russian police go digital against protesters*, in *Reuters*, 11 febbraio 2021 [reut.rs/3uxNxq5]; ma anche A. ZLOBINA, *Moscow's Use of Facial Recognition Technology Challenged*, in *Human Rights Watch*, 8 luglio 2020 [bit.ly/3uz58Ot].

[137] Si osserva in A. PACE, *Problematica delle libertà costituzionali. Parte speciale*, cit., 285 ss. (e più di recente ID., *La sicurezza pubblica nella legalità costituzionale*, in *Rivista AIC*, 1, 2015) come la sicurezza pubblica vada intesa nel nostro ordinamento come situazione di assenza di pericoli per i cittadini, la quale si identifica con la sussistenza di ordine pubblico "materiale", ossia come stato materiale di pace, e non come ordine pubblico "ideale", quale l'ordine "democratico", o "fascista", pregiudicabile anche in forza di mere manifestazioni del pensiero contrarie ai detentori del potere; si tratta di una impostazione che la giurisprudenza costituzionale più recente ha fatto propria (*ex multis*, sentt n. 285/2019, 237/2006, 290/2001). V. anche art. 159, c. 2, del d.lgs. n. 112/1998, che definisce "ordine pubblico e sicurezza pubblica" come «le misure preventive e repressive dirette al mantenimento dell'ordine pubblico, inteso come il complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale, nonché alla sicurezza delle istituzioni, dei cittadini e dei loro beni». Sul percorso evolutivo e giurisprudenziale

pongono l'interrogativo su quale sia il punto di equilibrio tra esigenze di sicurezza così intese e libertà esercitabili fisicamente nella dimensione pubblica.

Nell'ordinamento degli Stati Uniti la soluzione al problema è stata impostata a partire dal concetto di "privacy di gruppo", nella sua componente relazionale più ampia che la giurisprudenza ha da molti anni ricondotto alla libertà di espressione e di riunione previste entrambe al I Emendamento[138]. Da qui la consapevolezza di come la captazione di immagini facciali negli spazi pubblici possa seriamente interferire con tali libertà, nella misura in cui ci si aspetta di beneficiare della c.d. "anonimità del gruppo"[139]. La ragionevole aspettativa di rimanere anonimi negli spazi pubblici, infatti, viene considerata un elemento fondamentale in una società democratica, ove all'individuo è consentito di esprimere idee e modi di essere anche impopolari, rimanendo protetto da violenze e persecuzioni[140].

ziale del concetto di ordine pubblico nel nostro ordinamento, come più in generale sul tema della sicurezza pubblica, v. T.F. GIUPPONI, *La sicurezza e le sue "dimensioni" costituzionali*, in S. VIDA (a cura di), in *Diritti umani. Trasformazioni e reazioni*, BUP, Bologna, 2008, 275 ss.; M. RUBECHI, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *Federalismi.it*, 23, 2016.

[138] Cfr. US SUPREME COURT, *National Association for the Advancement of Colored People v. Alabama*, 357 U.S. 449, 30 giugno 1958: «Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs» (462), con riguardo alla pretesa del Governo di ottenere la lista degli iscritti alla National Association for the Advancement of Colored People.

[139] J. LAPERRUQUE (a cura di), *Facing the Future of Surveillance. Task Force on Facial Recognition Surveillance*, *Project On Government Oversight (POGO)*, 4 marzo 2019, 25 ss. Per alcuni spunti sulla dottrina e la giurisprudenza americana, che tendono a ricondurre il diritto all'anonimità al Primo e al Quarto Emendamento della Costituzione statunitense, S. NAKAR, D. GREENBAUM, *Now you see me. Now you still do: facial recognition technology and the growing lack of privacy*, in *Boston University Journal of Science & Technology Law*, 23, 2017, 115 ss.; A. KOZINSKI, *Two Faces of Anonymity*, in *Capital University Law Review*, 43, 1, 2015.

[140] J.R. REIDENBERG, *Privacy in Public*, in *University of Miami Law Review*, 69, 1, 2014, 153. In A.F. WESTIN, *Privacy and Freedom*, Athenum, New York, 1967, 31 s., si definisce "anonimità" lo stato in cui l'individuo si trova nello spazio pubblico ma ancora cerca e trova una certa libertà dall'identificazione e dalla sorveglianza. In questo

Anche in Europa, già nel 2013, il Gruppo di lavoro "Articolo 29" metteva in guardia dal pericolo per cui, «nel caso del riconoscimento del volto in cui i dati biometrici sono facilmente ottenibili all'insaputa dell'interessato, un utilizzo indiscriminato metterebbe fine all'anonimato nelle aree pubbliche e consentirebbe la localizzazione continua di persone»[141].

La questione, dunque, si concentra nell'interrogativo sulla misura in cui viene riconosciuta tutela all'*anonimato nello spazio pubblico*, inteso come mancata riconducibilità ad un soggetto specifico di un atto o un comportamento preordinato all'esercizio legittimo di altre libertà[142].

Nell'ordinamento italiano vi è la tendenza a ricondurre l'anonimato alla sfera del diritto alla riservatezza o della tutela dei dati personali[143]. Si sottolinea come nella società dell'informazione non sia concepibile una forma assoluta di anonimato, ma occorra sempre operare una relativizzazione in rapporto a soggetti determinati o circostanze specifiche, con una valutazione da svolgere caso per caso[144]. Ne deriva, inoltre, come nel nostro ordinamento non esista un vero e proprio diritti generale all'anonimato, ma sia necessario fare riferimento a specifiche discipline di settore, le quali possono costituire questa condizione come un vero e proprio diritto, o considerarla come un mero dato di fatto, oppure addirittura prevederne la negazione[145].

senso, si può godere di anonimità anche nella consapevolezza di essere osservati, ma senza aspettarsi di essere necessariamente identificati, e quindi non offrendo ostacoli anche alla possibilità di non rispettare tutte le regole e aspettative sociali.

[141] Cfr. GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, cit., p. 2.

[142] Circa il problema definitorio dell'anonimato, si guarda all'alternativa tra un approccio di tipo formale, ritenendosi cioè anonimo ciò che è privo di nome, o sostanziale, ritenendosi invece anonimo ciò che non è riconducibile ad un soggetto; cfr. G. FINOCCHIARO, *Anonimato*, in *Dig. disc. priv., sez. civ.*, Agg. V, 2010, 13.

[143] Così, rispettivamente, A. CANDIAN, *Anonimato (diritto all')*, in *Enc. dir.*, II, 1958, 499 ss.; G. FINOCCHIARO, *Anonimato*, cit., 12 ss.

[144] G. FINOCCHIARO, *Anonimato*, cit., 14 ss., con una valutazione da effettuare guidati dal canone della ragionevolezza. Il problema è quindi collegato alla qualificabilità di un dato come personale e al concetto di identificabilità della persona (su cui v. anche *infra* Cap. III, par. 3).

[145] Cfr. G. FINOCCHIARO (a cura di), *Diritto all'anonimato. Anonimato, nome e*

L'impiego delle TRF chiama in causa la tutela contro l'identificazione nelle ipotesi in cui un soggetto, attraverso l'esercizio delle proprie libertà, voglia partecipare alla vita pubblica e, finanche, influenzare le istituzioni democratiche. L'attenzione, in particolare, ricade su quelle libertà che costituiscono fattori essenziali per la formazione dell'opinione pubblica democratica e che valgono come strumenti di partecipazione politica. Si tratta di diritti e facoltà riconducibili a quella lettura integrata del principio pluralista e del principio di eguaglianza, intesi «come pilastri di una società aperta che rende possibile (attraverso procedure "comunicative") la realizzazione di identità molteplici»[146].

Tra le libertà che esprimono questa vocazione "pubblica"[147] viene principalmente in gioco la *libertà di riunione*, assieme a quei diritti verso i quali essa manifesta una dimensione "strumentale"[148], tra cui spiccano quelli legati alla libertà di manifestazione del pensiero.

In queste ipotesi, a differenza – come visto – di altri sistemi giuridici, l'ordinamento italiano richiede, come regola, la rivelazione dell'identità di coloro che ne fanno esercizio[149]. Si pensi, con riguardo

identità personale, in F. GALGANO (diretto da), *Trattato di diritto commerciale e di diritto pubblico dell'economia*, XLVIII, Cedam, Padova, 2008, 133-278, con riguardo, ad esempio, alla qualificazione come diritto: dalla legislazione speciale sulle tossicodipendenze; riferito alla madre di non rivelare la propria identità; dalla legge sul diritto d'autore. Si qualifica invece come dovere: in capo al personale sanitario nel caso di trapianti; nella normativa sui collaboratori di giustizia; fino agli obblighi imposti dalla stessa normativa sulla tutela dei dati personali. L'anonimato può configurarsi come principio strumentale all'imparzialità dell'azione amministrativa, come nel caso dei pubblici concorsi e delle gare d'appalto; ma può anche essere negato, come avviene nella legislazione penale antiterrorismo, sull'evasione fiscale o sul riciclaggio.

[146] Cfr. P. RIDOLA, *Libertà e diritti nello sviluppo storico del costituzionalismo*, in R. NANIA, P. RIDOLA (a cura di), *I diritti costituzionali*, I, cit., 132. Sul concetto di "sfera pubblica" quale luogo di libero e aperto dibattito, ove si sviluppano e circolano le idee per la formazione dell'opinione pubblica, v. J. HABERMAS, *Storia e critica dell'opinione pubblica*, Laterza, Roma-Bari, 2006.

[147] M. RUOTOLO, *La libertà di riunione e di associazione*, in R. NANIA, P. RIDOLA (a cura di), *I diritti costituzionali*, II, cit., 677.

[148] A. PACE, *Problematica delle libertà costituzionali. Parte speciale*, cit., 299; P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., 182.

[149] Cfr. G.E. VIGEVANI, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, in *Il Diritto dell'informazione e dell'informatica*, 2, 2014, 215 ss. A

alla libertà di riunione, all'obbligo di preavviso *ex* art. 17, c. 3, Cost. per l'organizzazione di riunioni in luogo pubblico, ma soprattutto – per quanto qui rileva più da vicino – ad alcune delle limitazioni oggettive all'esercizio di questa libertà legate alle particolari modalità di partecipazione.

È il caso del divieto di utilizzare caschi protettivi o «qualunque altro mezzo atto a rendere difficoltoso il riconoscimento della persona» in occasione di manifestazioni che si svolgano in luogo pubblico o aperto al pubblico, ma più in generale al loro impiego in ogni luogo pubblico o aperto al pubblico tranne quando non ricorra un «giustificato motivo»[150]. Analogamente, il t.u.l.p.s. stabilisce un generale divieto di «comparire mascherato in luogo pubblico»[151]. Si tratta di previsioni che, nella loro generalità e astrattezza, risultano problematiche in punto di giustificabilità, nel senso di riconducibilità ai limiti costituzionalmente previsti per la libertà di riunione, in quanto – è stato detto – la copertura del volto non equivale di per sé all'uso di armi o non rende meno pacifica una riunione, ma può integrare anche solo un atteggiamento difensivo contro potenziali azioni fisiche o giuridiche altrui o, tutt'al più, un elemento presuntivo di pericolosità: occorrerebbe dunque valutare caso per caso – ma non ci si nasconde come tale valutazione possa risultare nei fatti difficile – se il

questa logica, anche nella dimensione associativa, possono essere ricollegati l'apertura, la trasparenza e la ricerca del libero confronto compendiati, da una parte, nel divieto di associazioni segrete *ex* art. 18, c. 2, Cost., in quanto, come rileva C. MORTATI, *Istituzioni di diritto pubblico*, II, Cedam, Padova, 1976, 1162, «contrastanti con l'esigenza (essenziale, in quanto connaturata ad ogni assetto democratico) della pubblicità». Dall'altra, nel divieto di associazioni paramilitari con finalità politiche sempre all'art. 18, c. 2, Cost. e nel "metodo democratico" di cui all'art. 49 Cost. Più approfonditamente, v. anche U. DE SIERVO, *La libertà di associazione*, in G. SANTANIELLO (diretto da), *Trattato di diritto amministrativo*, cit., 191 ss.; F. RIGANO, *Art. 18 Cost.*, in A. CELOTTO, R. BIFULCO, M. OLIVETTI, *Commentario alla Costituzione*, cit., 404 ss.

[150] Così in base all'art. 5 della legge 22 maggio 1975, n. 152, come sottolineato da G. TARLI BARBIERI, *Art. 17*, in R. BIFULCO, A. CELOTTO, M. OLIVETTI (a cura di), *Commentario alla Costituzione*, cit., 387 s. Più approfonditamente su questa libertà, v. anche R. BORRELLO, *Riunione (diritto di)*, in *Enc. dir.*, XL, 1988, 1401 ss.; P. GIOCOLI NACCI, *Libertà di riunione*, in G. SANTANIELLO (diretto da), *Trattato di diritto amministrativo*, XII, cit., 157 ss.

[151] Art. 85 del R.d. 18 giugno 1931, n. 773.

travisamento del volto metta effettivamente in pericolo l'ordine pubblico materiale[152].

Allo stato, tuttavia, non sarebbe possibile ricorrere a simili espedienti per sottrarsi al riconoscimento facciale, tanto più che l'identificazione è una precondizione per far valere quelle ipotesi sanzionatorie che colpiscono anche solo la mera partecipazione a certi tipi di riunioni, come problematicamente fanno emergere quelle fattispecie penali adottate in epoca risalente e ancora vigenti[153].

Anche la *libertà di manifestazione del pensiero*, dal canto suo, contribuisce spiccatamente alla formazione di un'opinione pubblica consapevole, in quanto elemento essenziale della vita di uno Stato democratico, secondo quella direttrice che ha trovato esplicitazione nella dimensione partecipativa di tutti i diritti costituzionali codificata nell'art. 3 c. 2, Cost.[154]. A rilevare qui, tuttavia, non è tanto il problema dell'anonimato nella prospettiva della tutela della libertà di espressio-

[152] Per numerosi rilievi critici rivolti a tali previsioni, v. U. ALLEGRETTI, *Legge sull'ordine pubblico e libertà costituzionali*, in *Rivista trimestrale di diritto pubblico*, 1976, spec. 495 ss., ove vengono giudicate espressione della volontà di schematizzare come aggressivi atteggiamenti polivalenti. Tali divieti non sarebbero giustificabili neppure sotto il profilo del contrasto alla possibilità di compiere più agevolmente reati, in quanto, se del caso, la copertura del volto sarebbe mero elemento presuntivo e sintomo di pericolosità, ipotesi che non rientrerebbe nel potere di scioglimento di una riunione in svolgimento ammesso dall'art. 17 Cost.

[153] Si pensi all'art. 655 c.p. che punisce con l'arresto la partecipazione ad una riunione sediziosa, in quanto le manifestazioni e le grida sediziose implicano sempre eccitazione al sovvertimento delle pubbliche istituzioni e pericolo per l'ordine pubblico»; la portata applicativa di questa previsione è stata circoscritta dalla giurisprudenza costituzionale (C.cost., sentt. n. 120/1957 e n. 15/1973), ove si è chiarito che «è necessario che ricorrano contemporaneamente due essenziali requisiti consistenti in una condotta obbiettivamente sediziosa e nella sua pericolosità per l'ordine pubblico. Ora è evidente che l'oggettiva sediziosità di una condotta va di volta in volta accertata, in relazione a circostanze di tempo, di modo e di luogo, tenendo soprattutto conto del suo specifico contenuto. [...] Atteggiamento sedizioso penalmente rilevante è soltanto quello che implica ribellione, ostilità, eccitazione al sovvertimento delle pubbliche istituzioni e che risulti in concreto idoneo a produrre un evento pericoloso per l'ordine pubblico». Giudica comunque problematica la vigenza di questa previsione M. RUOTOLO, *La libertà di riunione e di associazione*, cit., 691.

[154] P. CARETTI, *Comunicazione e informazione*, in *Enc. dir.*, Ann. I, 2007, 223.

ne del proprio pensiero, che essa avvenga tramite stampati[155] o nella sua forma più tipica della società digitale odierna, quale l'anonimato in rete[156]. Piuttosto, si ha riguardo a quella possibilità, originariamente e storicamente connessa alla libertà di riunione, di contrapporsi ai detentori del potere nella discussione dei problemi e nella elaborazione collettiva di proposte politiche[157]. Le TRF, come detto, possono esercitare un effetto deterrente e inibitorio anche su questo versante della libertà di manifestazione del pensiero, come attestano anche le indagini svolte dal Consiglio per i diritti umani delle Nazioni Unite sul ricorso a tecniche di sorveglianza sempre più sofisticate[158]. A risultarne svilita, così, è quella prospettiva "funzionalista" che nel nostro ordinamento ha legato questa libertà alle forme proprie di una democrazia pluralista[159], entro cui la possibilità di esprimere la propria opinione

[155] Anche nell'esercizio della libertà di manifestazione del proprio pensiero si ritiene che non riceva tutela immediata il diritto di rimanere anonimi, in quanto si tende a valorizzare la responsabilità personale di chi diffonde informazioni e la trasparenza, a partire dall'ipotesi di sequestro per la violazione delle norme che la legge prescrive per l'indicazione dei responsabili (art. 21, c. 3, Cost.), la possibilità di rendere pubblici i mezzi di finanziamento della stampa periodica (art. 21, c. 5, Cost.), e più in generale l'obbligo di indicare sugli stampati il nome e il domicilio dello stampatore e, se esiste, dell'editore (art. 2, legge n. 47/1958). Per approfondimenti, v. P. CARETTI, A. CARDONE, *Diritto dell'informazione e della comunicazione nell'era della convergenza*, *Stampa, radiotelevisione, telecomunicazioni, internet, teatro e cinema*, il Mulino, Bologna, 2019, 22 ss. e 49 ss.; B. CUNEGATTI, *Anonimato e libertà di stampa*, in G. FINOCCHIARO (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, cit., 254 ss.

[156] Problematica per la quale si rinvia a M. BETZU, *Anonimato e responsabilità in internet*, in *Costituzionalimo.it*, 2, 2011; M. MANETTI, *Libertà di pensiero e anonimato in rete*, in *Il Diritto dell'informazione e dell'informatica*, 2, 2014, 139 ss.; G. RESTA, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, *ivi*, 171 ss. Si osserva in G.E. VIGEVANI, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, cit., 219, tuttavia, come difficilmente potrebbe trovare ingresso un obbligo generalizzato e assoluto di doversi esprimere rivelando la propria identità, giudicato irrealistico nell'epoca del *web* e dei dibattiti in rete.

[157] A. PACE, *Problematica delle libertà costituzionali. Parte speciale*, cit., 299.

[158] Cfr. HUMAN RIGHTS COUNCIL, *Surveillance and human rights*, cit.

[159] Sul punto, cfr. E. CHELI, *Libertà di informazione e pluralismo informativo negli indirizzi della giurisprudenza costituzionale*, in A. PISANESCHI, L. VIOLINI (a cura di), *Poteri, garanzie e diritti. A sessanta anni dalla Costituzione. Scritti per Giovanni Grottanelli de' Santi*, Giuffrè, Milano 2007, 1406. Osservava C. ESPOSITO, *La libertà di ma-*

viene tutelata come valore in sé e non per i contenuti del messaggio espresso[160].

Nello scenario qui considerato, dunque, la tutela dell'anonimato come strumento di protezione del dissenso sconta una sorta di paradosso: essa potrebbe trovare ingresso solamente all'interno di ordinamenti democratici, ove però la libertà di riunione e di manifestazione del pensiero dovrebbero essere di per sé tutelate; mentre non sarebbe concepibile all'interno dei regimi totalitari, ove l'anonimato minerebbe la legittimazione del potere costituito, apparendo così un controsenso[161].

nifestazione del pensiero nell'ordinamento italiano, Giuffrè, Milano, 1958, 12, come «non la democraticità dello Stato ha per conseguenza» il riconoscimento della libertà di manifestazione del pensiero, ma sono proprio «le ragioni ideali del riconoscimento di quella libertà» che portano «anche alla affermazione dello Stato democratico». Non a caso l'art. 21 Cost. viene qualificato dalla giurisprudenza costituzionale quale "pietra angolare dell'ordine democratico" (sent. n. 84/1969) e "cardine di democrazia" (sent. n. 126/1985).

[160] Sulla mancanza di "limiti logici" a questa libertà, che copre non solo l'attività del mero pensiero, ma anche l'incitamento all'azione, salvo spingere fattivamente a commettere un reato, P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., 228 ss. Ne deriva inoltre che i limiti imposti a tale libertà dal legislatore devono trovare un fondamento costituzionale esplicito o implicito; cfr. A. PACE, M. MANETTI, *Commento all'art. 21*, cit., 40 ss.

[161] Così M. CUNIBERTI, *Democrazie, dissenso politico e tutela dell'anonimato*, in *Il Diritto dell'informazione e dell'informatica*, 2, 2014, 111 ss., salvo poi osservare come l'espressione del dissenso in rete, forma tipica delle società contemporanee, tenda a subire controlli e compressioni anche nei regimi democratici, come testimonia paradigmaticamente la vicenda di *Wikileaks*, su cui v. *retro* nella Introduzione. Quanto ai regimi autoritari, è risaputo come i nuovi *media* e i *social network* siano stati potenti strumenti di veicolo del dissenso, come accaduto nelle c.d. primavere arabe, salvo poi verificare, come sottolinea M. CASTELLS, *Reti di indignazione e speranza. Movimenti sociali nell'era di internet*, Università Bocconi Editore, Milano, 2015, 38 ss., come al successo delle rivolte nordafricane abbiano concorso una molteplicità di fattori, tra cui i *mass media* tradizionali. Di converso, i nuovi *media* possono costituire anche formidabili strumenti di condizionamento delle masse tramite forme di controllo, di disinformazione e di propaganda politica, sia all'interno dei singoli ordinamenti, come dimostra, ad esempio, l'utilizzo della cultura digitale da parte del governo russo (cfr. E. MOROZOV, *L'ingenuità della rete. Il lato oscuro della libertà di internet*, Codice, Torino, 2018, 116 ss.), sia nei confronti di altri Paesi, come emerge dai presunti tentativi di interferenza nelle elezioni statunitensi da parte del governo cinese e russo; cfr. J.E.

Ad ogni modo, riprendendo le considerazioni della *Commission nationale de l'informatique et des libertés*[162], non c'è nessuna legge che imponga l'identificazione di una persona che si muove liberamente in uno spazio pubblico[163]. Mentre per l'esercizio di certe libertà possono esservi divieti – come il non poter nascondere il proprio volto – o obblighi da rispettare – come la sottoposizione a controlli all'interno di specifici luoghi –, si tratta comunque di misure previste e consentite dalla legge a protezione di interessi specifici e meritevoli di tutela. L'erosione generalizzata dell'anonimità in pubblico, invece, è destinata ad alimentare ulteriormente forme di sorveglianza eticamente – prima che giuridicamente – inaccettabili, sia che vengano perpetrate da autorità pubbliche, sia che vengano praticate da imprese private. Tecnologie basate su riconoscimento facciale, che massimizzano la capacità di controllare, tracciare e profilare le persone entro spazi pubblici, possono spingere insidiosamente lungo questa china.

7. *TRF e le diverse dimensioni dell'eguaglianza: nuove forme di discriminazioni*

L'impiego delle TRF è suscettibile di impattare sui diritti fondamentali anche nella prospettiva della violazione del principio di eguaglianza, nella duplice declinazione in senso formale e sostanziale accolta dalla Costituzione[164].

Sotto il profilo dell'*eguaglianza formale*, queste tecnologie possono favorire fenomeni discriminatori in conseguenza di errori compiuti dai sistemi di riconoscimento facciale, consistenti nell'individuare o meno

BARNES, *Russian Interference in 2020 Included Influencing Trump Associates, Report Says*, in *The New York Times*, 16 marzo 2021 [nyti.ms/31Re2KR]; M. PENGELLY, *Russia targeted Trump allies to hurt Biden in 2020 election, US officials say*, in *The Guardian*, 16 marzo 2021 [bit.ly/3rYn4QT].

[162] CNIL, *Facial recognition: for a debate living up to the challenges*, cit., 7 s.

[163] Neppure la legislazione a tutela dei dati personali, come riportato *infra* Cap. III, par. 4.3.

[164] Più ampiamente, v. anche A. CERRI, *Uguaglianza (principio costituzionale di)*, in *Enc. giur.*, XXXII, 1994; M. DOGLIANI, C. GIORGI, *Articolo 3. Costituzione italiana*, Carocci, Roma, 2017.

una corrispondenza – originando quindi falsi-positivi o falsi-negativi – tra l'immagine del volto catturata e le immagini presenti nel *database*. All'origine di queste discriminazioni stanno quelli che comunemente vengono chiamati *bias*, ovvero – come si vedrà approfonditamente più avanti[165] – una sorta di "distorsioni" presenti negli algoritmi di *machine learning* che possono avere origine dalla fase di *design* sino al loro impiego per assumere una decisione. Rinviando ad un momento successivo per la distinzione tra discriminazioni dirette e indirette[166], quel che preme qui rilevare è che a venire in gioco sono proprio alcune delle categorie espressamente indicate dall'art. 3, c. 1, Cost., che presupporrebbero una tutela rafforzata del principio in parola[167].

Si pensi all'ipotesi delle discriminazioni su base *razziale*[168]. Sul versante delle autorità pubbliche, ad esempio, vengono in rilievo le determinazioni assunte dalle forze dell'ordine. Hanno suscitato grande scalpore negli Stati Uniti i casi – purtroppo non infrequenti – di cittadini afro-americani sottoposti ad arresto sulla base di errori compiuti

[165] Cfr. *infra* Cap. III, par. 7.

[166] Cfr. *infra* Cap. III, par. 7.

[167] Osserva L. PALADIN, *Eguaglianza (dir. cost.)*, in *Enc. dir.*, XIV, 1965, 523, come i riferimenti alle categorie indicate all'art. 3, c. 1, Cost. «non rappresentano storicamente né logicamente né letteralmente una serie di limitazioni, ma pongono altrettanti rafforzamenti del principio stesso, che ne lasciano intatta la normale efficacia per tutta la sfera residua delle norme e delle situazioni». In accordo con tale impostazione, osserva C. MORTATI, *Istituzioni di diritto pubblico*, II, cit., 1019, come la proibizione in base a tali categorie abbia «carattere assoluto, sicché deroghe ad essa siano ammissibili solo se espressamente consentite da altre norme costituzionali», salvo poi richiamare anche la "natura delle cose" quale giustificazione, intesa come portatrice di ragioni di ordine naturale, biologico o morale, quale risulta dalla coscienza sociale dominante. Che la legge discriminante in base a questi profili debba superare una "presunzione di incostituzionalità", è affermato da P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., 84.

[168] Sulla opportunità di mantenere il riferimento alla "razza" in Costituzione, v. di recente V. TONDI DELLA MURA, *La parola "razza" nella Costituzione, ovvero: della rilevanza costituzionale di una nozione scientificamente infondata*, in *Dirittifondamentali.it*, 2, 2019, secondo cui va inteso «alle diverse urgenze del contesto storicoculturale di volta in volta prese a riferimento» (7). Favorevole anche P. CARETTI, *A ottant'anni dalle leggi razziali: non solo memoria*, in *Lo Stato*, 6, 2018, 57. *Contra*, A. GRATTERI, G.A. SACCO, *Senza distinzione. Per il superamento della parola razza*, in *Nomos*, 2, 2018, 1 ss., cui si rinvia per una ricostruzione di questo tipo di posizioni.

da sistemi di riconoscimento facciale, i quali vengono tratti in inganno dal colore della pelle o della conformazione del viso, senza che agli interessati venisse concessa prontamente l'opportunità di smentire gli algoritmi[169].

Sul versante dei soggetti privati, invece, si considerino anche solo quegli episodi che hanno origine dal ricorso, all'interno di esercizi commerciali, a sistemi di sorveglianza integrati con TRF per prevenire furti e individuare potenziali ladri[170]. In alcune città queste tecnologie sono state affiancate a sistemi che impediscono addirittura di entrare in un negozio nell'ipotesi in cui l'immagine di una persona sia presente in una "lista nera" condivisa tra più esercizi commerciali che utilizzano la medesima tipologia di rilevamento[171]. Gli errori compiuti dagli algoritmi nei confronti delle minoranze etniche, in questo caso, possono determinare un numero maggiore di controlli, contribuendo così, in una sorta di circolo vizioso, ad alimentare atteggiamenti discriminatori verso coloro che già possono essere oggetto di discriminazioni[172].

Altro profilo a venire in gioco è quello relativo al *sesso*[173]. Si pensi

[169] K. HILL, *Wrongfully Accused by an Algorithm*, in *The New York Times*, 24 giugno 2020 [nyti.ms/3sY0okN], che riporta una vicenda verificatasi a Detroit nel gennaio 2020 e che ha visto come protagonista una persona arrestata sulla base di una presunta corrispondenza con immagini acquisite da un video di sorveglianza all'interno di un negozio rapinato oltre un anno prima. Cfr. anche E. ANDERSON, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit*, in *Detroit Free Press*, 12 luglio 2020 [bit.ly/2Q8cfy7], che riporta invece la vicenda di altra persona, arrestata sempre a Detroit nel maggio 2019 nell'ambito di alcune indagini su un episodio di rapina, a causa di una presunta corrispondenza con una immagine acquisita da un video ripreso con un cellulare; in questo caso, tuttavia, la forma del volto, il tono della pelle e i tatuaggi del soggetto in questione risultavano chiaramente inconciliabili con le immagini del video.

[170] C. LIEBER, *Your Favorite Stores Could Be Tracking You With Facial Recognition*, in *RACKED*, 22 maggio 2018 [bit.ly/3rRV1T2].

[171] A. NG, *With Facial Recognition, Shoplifting May Get You Banned In Places You've Never Been*, in *CNET*, 20 marzo 2019 [cnet.co/39PNiyF].

[172] C. PITTMAN, *"Shopping While Black": Black consumers' management of racial stigma and racial profiling in retail settings*, in *Journal of Consumer Culture*, 20, 1, 2017, 3 ss.

[173] In generale, sulle discriminazioni perpetrate dai sistemi algoritmici contro le donne, v. M. D'AMICO, *Una parità ambigua. Costituzione e diritti delle donne*, Raffaello Cortina Editore, Milano, 2020, 313 ss.

alla vicenda legata al servizio di "*Online Passport Photo Checking*" messo a disposizione dall'*Home Office* del Regno Unito a partire dal 2016, nel quale un algoritmo analizza le immagini facciali inviate dagli utenti per verificarne la sufficiente qualità ed il possibile impiego come fotografie di riconoscimento per il passaporto. Ad una comparazione, è stato dimostrato come il sistema restituisca impropriamente messaggi di errore nel caso delle fotografie di donne dalla pelle nera in una percentuale maggiore rispetto a quanto accade a donne dalla pelle chiara[174]. Si tratta solamente di un esempio, che però dà la cifra di come queste forme di discriminazioni possano risolversi anche nell'impossibilità di usufruire di un servizio e, di converso, in maggiori oneri addossati su coloro che versano in una data condizione o appartengono ad una minoranza.

Limitandoci a richiamare quanto affermato fin dalle prime pronunce della Corte costituzionale, il principio di eguaglianza formale «deve assicurare ad ognuno eguaglianza di trattamento, quando eguali siano le condizioni soggettive ed oggettive alle quali le norme giuridiche si riferiscono per la loro applicazione», così che vi sia trattamento eguale di condizioni eguali e trattamento diseguale di condizioni diseguali[175]. In ciascuna delle ipotesi richiamate non sembrano sussistere

[174] Cfr. A. VAUGHAN, *UK Launched Passport Photo Checker it Knew Would Fail with Dark Skin*, in *NewScientist.com*, 9 ottobre 2019 [bit.ly/3mENaqQ]; M. AHMED, *UK passport photo checker shows bias against dark-skinned women*, in *BBC News*, 8 ottobre 2020 [bbc.in/3tfBkG4], ove si riferisce della sottoposizione di 1000 immagini al sistema, il quale ha restituito un tasso di errore per le donne dalla pelle scura del 22%, a fronte di un tasso di errore per le donne dalla pelle chiara del 14%.

[175] C.cost., sent. 16 gennaio 1957, n. 3. Secondo l'inquadramento in L. PALADIN, *Eguaglianza (dir. cost.)*, cit., 525, «può bene concedersi che la eguaglianza formale sia l'imperativo di non discriminare le persone, individualmente e collettivamente riguardate: ma ciò non toglie che la separazione delle discipline discriminatorie da tutte le altre immancabili differenziazioni delle varie cerchie dei soggetti debba venire pur sempre operata, sindacando esistenza e consistenza dei presupposti oggettivi di giustificazione della diseguaglianza giuridica». Sulla tensione tra esigenze di universalità delle norme, da una parte, e necessità che situazioni analoghe non siano trattate in maniera dissimile e che situazioni diverse non siano trattate nello stesso modo, salvo giustificazioni obiettive, v. A. CELOTTO, *Art. 3, 1° comma*, in A. CELOTTO, R. BIFULCO, M. OLIVETTI (a cura di), *Commentario alla Costituzione*, cit., 69 ss. Sulla vastissima letteratura e giurisprudenza relativa al principio di ragionevolezza, basti rinviare a L. PA-

ragioni oggettive che giustifichino un trattamento differenziato sul piano soggettivo, risolvendosi quindi in discriminazioni illegittime.

8. (segue) *... e una accentuazione della posizione di svantaggio delle persone bisognose*

Come anticipato, a venire in gioco è anche il differente e complementare profilo dell'*eguaglianza sostanziale*, intesa – per quanto qui di maggiore interesse – come norma programmatica che impone un impegno attivo e una specifica attenzione da parte dei pubblici poteri nei confronti dell'individuo concreto, nella sua situazione di svantaggio e nel bisogno di tutela che impedisce il pieno sviluppo della persona[176]. In questo caso, tuttavia, l'impiego delle TRF può risolversi, in senso del tutto antitetico, in una forma di lesione dei diritti che discende direttamente dalla reale condizione soggettiva e sociale della persona, a seguito della mancata considerazione, o addirittura della accentuazione di tale situazione di svantaggio.

Innanzitutto, tra i soggetti che la Costituzione considera in una posizione di debolezza nella dimensione relazionale in cui si trovano vi è il *lavoratore*[177].

LADIN, *Ragionevolezza (principio di)*, in *Enc. dir.*, Agg. I, 1997, 899 ss., e a contributi monografici quali L. D'ANDREA, *Contributo ad uno studio sul principio di ragionevolezza nell'ordinamento costituzionale*, Giuffrè, Milano, 2000; G. SCACCIA, *Gli strumenti della ragionevolezza nel giudizio*, Giuffrè, Milano, 2000; A. MORRONE, *Il custode della ragionevolezza*, Giuffrè, Milano, 2001; F. MODUGNO, *Ragione e ragionevolezza*, Edizioni scientifiche, Napoli, 2009.

[176] Sul punto, si rinvia a A. GIORGIS, *Art. 3, 2° comma*, in A. CELOTTO, R. BIFULCO, M. OLIVETTI (a cura di), *Commentario alla Costituzione*, cit., 94 ss., A. MOSCARINI, *Principio costituzionale di eguaglianza e diritti fondamentali*, in R. NANIA, P. RIDOLA (a cura di), *I diritti costituzionali*, I, cit., 399 ss., e alla dottrina e giurisprudenza ivi richiamata, anche per la problematica delle "azioni positive", nella tensione tra esigenze di riequilibrio e di sostegno e il rischio di integrare "discriminazioni alla rovescia".

[177] Basti osservare che la materia del diritto del lavoro è «uno strumento di eguaglianza (verticale) *tra datori di lavoro e lavoratori*: eguaglianza nel senso di redistribuzione (anche se non, certamente, di assoluto eguagliamento), nonché in quello della riduzione dei caratteri autoritari insiti nel contratto di lavoro subordinato»; cfr. R. DEL PUNTA, *Diritto del lavoro*, GFL, Milano, 2020, 621. Sulla relatività della posizione

Nei confronti di questa categoria, l'uso della TRF acquista significato, innanzitutto, nel momento genetico del rapporto lavorativo. Già da anni vi sono aziende che utilizzano le TRF durante i colloqui di assunzione per valutare i candidati attraverso l'analisi di elementi come le espressioni facciali e il contatto visivo, in combinazione con il tono della voce o la scelta delle parole[178]. In questo modo le persone vengono ordinate entro una graduatoria in base alla previsione di maggior idoneità all'impiego, consentendo così all'intervistatore di risparmiare tempo e di impiegare una metodologia che – si asserisce – sia più neutrale e al riparo dai soggettivismi[179]. Questo tipo di sistemi, sebbene dichiaratamente utilizzati come mero ausilio per il valutatore, hanno attirato numerose critiche, a partire dalle perplessità circa la correlazione tra espressioni facciali e "garanzia di successo" sul piano lavorativo.

Sul punto, sarebbe difficile stabilire, o riuscire a dimostrare, quando la decisione del datore di lavoro nell'assumere o meno una persona, quand'anche supportata da questi mezzi tecnologici, fuoriesca dalla sua sfera di autonomia e dalla libertà di valutazione. Tuttavia, per le medesime ragioni sottolineate sopra, un algoritmo di riconoscimento facciale potrebbe non valutare accuratamente le caratteristiche di un determinato gruppo demografico. In questo caso, vi è il rischio che le espressioni di tali persone vengano fraintese e che queste ultime subiscano inconsapevolmente un trattamento disparitario ingiustificato. Di conseguenza, si potrebbe qui violare il divieto di discriminazioni[180], il quale condiziona le

di debolezza del lavoratore subordinato, in rapporto al tipo di relazione contrattuale, cfr. *ivi*, 375 ss.

[178] J. AVELLA, R. FELONI, *We tried the AI software companies like Goldman Sachs and Unilever use to analyze job applicants*, in *Business Insider*, 3 settembre 2017 [bit.ly/39TzrHs]; C. HYMAS, *AI used for first time in job interviews in UK to find best applicants*, in *The Telegraph*, 27 settembre 2019 [bit.ly/39LV3pl].

[179] Più in generale, v. M. BOGEN, A. RIEKE, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, in *Uptorn*, dicembre 2018, 38.

[180] Cfr. art. 3, c. 1, lett. a, del d.lgs. 9 luglio 2003, n. 216, e del d.lgs. 9 luglio 2003, n. 215, concernenti rispettivamente la parità di trattamento in materia di occupazione e di condizioni di lavoro e tra le persone indipendentemente dalla razza e dall'origine etnica, coprono con la tutela antidiscriminatoria anche l'«accesso all'occupazione e al lavoro, sia autonomo che dipendente, compresi i criteri di selezione e le condizioni di assunzione». Più approfonditamente v. *infra* Cap. III, par. 7. V. anche l'art. 27 del d.lgs. 11 aprile 2006, n. 198 (Codice delle pari opportunità tra uomo e donna), che fa

prerogative del datore di lavoro non soltanto quando il rapporto di lavoro è già stato costituito, ma anche quando, nel momento precedente, viene speso il potere di selezione e di scelta del lavoratore[181].

L'impiego delle TRF, tuttavia, rileva anche in perduranza del rapporto di lavoro, allorché contribuisca al controllo e alla valutazione delle *performance* del lavoratore.

In questo caso trova necessariamente applicazione l'art. 4 dello Statuto dei lavoratori, come novellato dal d.lgs. 14 settembre 2015, n. 151, nell'ambito della riforma del c.d. *Jobs Act*. Nella sua nuova versione, l'art. 4, c. 1, limita l'impiego di «impianti audiovisivi» e altri «strumenti di controllo a distanza» solo «esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale», a condizione di raggiungere un accordo con i sindacati o ottenere un'autorizzazione amministrativa[182].

Attraverso tale previsione si opera un bilanciamento tra l'interesse del datore di lavoro a verificare l'esatta prestazione lavorativa e l'interesse del lavoratore a non vedere aggravata la propria condizione di subordinazione a causa della sottoposizione a forme più penetranti di controllo[183]. Le TRF, dunque, non dovrebbero trovare spazio quali

divieto di «qualsiasi discriminazione per quanto riguarda l'accesso al lavoro, in forma subordinata, autonoma o in qualsiasi altra forma, compresi i criteri di selezione e le condizioni di assunzione».

[181] Cfr. S. BORRELLI, A. GUARISO, L. LAZZERONI, *Le discriminazioni nel rapporto di lavoro*, in M. BARBERA, A. GUARISO (a cura di), *La tutela antidiscriminatoria*, Giappichelli, Torino, 2019, 182 ss. Sul punto, v. CGUE, causa C.54/07, *Centrum voor gelijkheid van kansen en voor racismebestrijding* c. *Firma Feryn NV*, 10 luglio 2008; CGUE, causa 81/12, *Asociaţia Accept* c. *Consiliul Naţional pentru Combaterea Discriminări*, 25 aprile 2013.

[182] Così l'art. 4, legge 20 maggio 1970, n. 300, come modificato dal d.lgs. n. 151/2015 e successivamente integrato dal d.lgs. n. 185/2016, che subordina l'istallazione di tali impianti alla previsione nell'accordo collettivo o, in mancanza, all'autorizzazione amministrativa dell'Ispettorato nazionale del lavoro. Ad esso rinvia peraltro anche l'art. 114 del d.lgs. n. 196/2003; sul complementare aspetto della tutela dei dati personali dei lavoratori, anche in ragione dei trattamenti derivanti proprio dai citati sistemi di sorveglianza, v. *infra* Cap. III, nota 94.

[183] Tali modifiche si giustificano allo scopo di adeguare la disciplina alle nuove possibilità offerte dalle innovazioni tecnologiche e ai mutamenti della disciplina sulla protezione dei dati personali, ma anche per rimediare ai profili di ineffettività della

strumenti di controllo sul lavoratore, essendo ammissibili solamente se riconducibili, ad esempio, alle «esigenze organizzative e produttive» sopra richiamate. Quand'anche vi fossero prestazioni – si pensi alle attività di *front office* o rivolte al pubblico – in cui al lavoratore venisse richiesto un certo approccio caratterizzato da cordialità e affabilità, l'impiego di tali strumenti tecnologici per monitorare questi aspetti non potrebbe legittimamente trovare ingresso nel rapporto di lavoro, in quanto comunque votati all'esclusiva finalità di controllo e non espressione di una scelta organizzativa idonea ad una più efficiente ed economica gestione del servizio[184]. Se invece queste tecnologie fossero impiegate per monitorare l'accesso a determinate aree dei complessi aziendali e per limitare l'accesso solamente ad alcuni dipendenti[185], in ragione delle finalità di «sicurezza del lavoro» o per «la tutela del patrimonio aziendale» indicate dalla norma, allora il ricorso potrebbe ritenersi ammissibile alle condizioni ivi previste, salvo però stabilire se queste forme di sorveglianza non si risolvano in un monitoraggio occulto[186] e, soprattutto, siano proporzionate – nella logica su cui ci si soffermerà[187] – alla finalità perseguitutela a causa del mancato avvio delle contrattazioni sindacali volte a dare attuazione a tale previsione; più ampiamente, v. R. DEL PUNTA, *La nuova disciplina del controllo a distanza sul lavoro (art. 23 d.lgs. n. 151/2015)*, in *Rivista italiana di diritto del lavoro*, 1, 2016, 77 ss.; M.T. SALIMBENI, *La riforma dell'articolo 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, *ivi*, 1, 2016, 589 ss.; A. LEVI (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act*, Giuffrè, Milano, 2016; P. TULLINI (a cura di), *Controlli a distanza e tutela dei dati del lavoratore*, Giappichelli, Torino, 2017; A. SARTORI, *Il controllo tecnologico sui lavoratori. La nuova disciplina italiana tra vincoli sovranazionali e modelli comparati*, Giappichelli, Torino, 2020, 219 ss. Più in generale sulla tematica, v. STOA, *Data subjects, digital surveillance, AI and the future of work*, PE 656.305, dicembre 2020.

[184] Sull'ampiezza delle scelte del datore di lavoro basate su "esigenze organizzative e produttive" che possano comportare indirettamente un controllo a distanza dei lavoratori, v. V. NUZZO, *La protezione del lavoratore dai controlli impersonali*, Editoriale Scientifica, Napoli, 2018, 35 ss., ove si sottolinea come debba esservi un rapporto di proporzionalità tra la decisione sull'assetto aziendale che determina controlli indiretti e l'invadenza che produce sul rapporto di lavoro.

[185] C. BURT, *Intel implements facial recognition security system at offices to identify threats*, in *Biometric Update*, 12 maggio 2020 [bit.ly/3wyCaQn].

[186] Per questa lettura restrittiva e per i rischi di una lettura estensiva della norma, v. V. NUZZO, *La protezione del lavoratore dai controlli impersonali*, cit., 157 ss.

[187] Sul problema della proporzionalità, v. *infra* Cap. III, par. 4.3.

ta.

Ad un regime diverso rispondono i controlli che, in base al c. 2 del citato art. 4, si appuntano sugli strumenti «utilizzati dal lavoratore per rendere la prestazione lavorativa», o che riguardano «gli strumenti di registrazione degli accessi e delle presenze»[188]. In questi casi non trova applicazione il divieto sopra citato in ragione della specifica e limitata finalità di questi controlli, rispetto alla quale – si è detto[189] – il legislatore ha svolto una valutazione *ex ante* di legittimità per la relativa installazione e impiego. Anche qui possono venire in gioco le TRF: nel primo caso, riprendendo l'esempio fatto sopra, in quelle ipotesi in cui la prestazione al pubblico venga fornita da remoto e in videocollegamento; qualora, tuttavia, si integrasse il software di videoripresa con un sistema di rilevamento delle espressioni facciali per valutare le *performance* prestazionali si ricadrebbe ugualmente nel divieto di cui al c. 1[190]. Una simile decisione imprenditoriale comporterebbe l'impiego di strumenti da cui deriva non una valutazione indiretta o involontaria – e quindi ammissibile – come sembrerebbe potersi desumere dalla *ratio* ispiratrice della norma, ma diretta specificatamente ad "osservare" la prestazione lavorativa[191].

Nel secondo caso, invece, il riconoscimento facciale potrebbe essere impiegato a scopo di autenticazione[192], ad esempio per consentire

[188] Art. 4, c. 2, legge n. 300/1970.

[189] Cfr. R. DEL PUNTA, *La nuova disciplina del controllo a distanza sul lavoro (art. 23 d.lgs. n. 151/2015)*, cit., par. 6.

[190] Con riguardo all'impiego di software per eseguire la prestazione di lavoro, implementato con funzioni aggiuntive di controllo, v. A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in P. TULLINI (a cura di), *Controlli a distanza e tutela dei dati del lavoratore*, cit., 18.

[191] Cfr. V. NUZZO, *La protezione del lavoratore dai controlli impersonali*, cit., 37 ss., ove si riporta come esempio paradigmatico l'impiego del braccialetto wireless adottato da Amazon volto a velocizzare la ricerca dei prodotti stoccati nei magazzini e ad aumentare l'efficienza della logistica; il divieto varrebbe ugualmente in quanto «non conta se l'interesse realizzato sia o meno quello della verifica del corretto adempimento: in ogni caso [...] è di per sé il controllo dell'uomo attuato dalla macchina che non rientra nel sistema di tutele delineato dallo Statuto, perché [...] continuativo, incessante, pervicace, onnicomprensivo e, dunque, lesivo della dignità e libertà umana».

[192] Riprendendo la casistica in A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, cit., 19 ss., non riferita esplicitamente al riconoscimento

l'accesso ai locali lavorativi o a determinate aree, con contestuale rilevamento dell'inizio e della fine dell'orario di lavoro. Rimane intatta, anche qui, la necessità di stabilire se simile sistema non valga ad eludere il divieto generale di controlli a distanza e risulti proporzionato alla finalità di registrazione.

Solamente in questa e nella limitata ipotesi richiamata sopra, le informazioni acquisite possono essere impiegate «a tutti i fini connessi al rapporto di lavoro»[193], fra cui rientra il potere disciplinare, la valutazione delle remunerazioni, il miglior impiego delle forze lavorative.

Riprendendo la panoramica sulle categorie di soggetti da tutelare che potrebbero subire una lesione a seguito di riconoscimento facciale, si considerino le condizioni di bisogno in cui versano le persone in ragione dell'età e del decorso del tempo, con riferimento specifico ai *minori* e agli *anziani*.

Per un verso, i minori sono spesso sottoposti alle medesime TRF degli adulti, sebbene non si sappia in che modo essi possano reagire a queste forme di sorveglianza, o che tipo di consapevolezza abbiano delle limitazioni ai propri diritti, o quali conseguenze possano prodursi sul loro sviluppo emotivo e intellettuale[194]. I minori, inoltre, sono esposti a particolari rischi perché, anche in ragione dell'uso abbondante fatto dei *social network*[195], le loro immagini vengono acquisite nei *database* senza che ne siano pienamente a conoscenza o che diano il proprio consenso; una raccolta che, paradossalmente, può essere giustificata con l'obiettivo di migliorare le prestazioni degli algoritmi di *machine learning* impiegati nel riconoscimento facciale[196].

facciale.

[193] Secondo quanto stabilisce il c. 3 dell'art. 4 della legge n. 300/1970, che dunque impone di distinguere tra l'esercizio del potere di controllo, che si concretizza nelle attività ai primi due commi, e l'utilizzo delle informazioni nella gestione del rapporto di lavoro.

[194] L. BARRETT, *Ban Facial Recognition Technologies For Children-And For Everyone Else*, cit., 226 ss.

[195] A. MARWICK, D. BOYD, *Networked Privacy: How Teenagers Negotiate Context in Social Media*, in *New Media & Society*, 16, 7, 2014, 1051 ss.

[196] K. HILL, A. KROLIK, *How Photos of Your Kids Are Powering Surveillance Technology*, in *The New York Times*, 11 ottobre 2019 [nyti.ms/39MzF3l]. V. anche *retro* Cap. II, par. 3.3.

Per l'altro verso, e in aggiunta, i minori possono subire l'impiego di TRF a loro specificatamente destinate, come avviene all'interno dell'ambiente scolastico[197]. Sempre più si assiste alla diffusione di queste tecnologie per ragioni di sicurezza, in particolare – come negli Stati Uniti – per contrastare la piaga delle sparatorie nelle scuole, attraverso sistemi di rilevamento della presenza di armi o altre "anomalie" derivanti, ad esempio, dall'abbigliamento[198]; ma anche per monitorare la frequenza degli alunni, tramite telecamere installate all'ingresso degli istituti o addirittura nelle aule[199]; sino alla possibilità di percepire lo stato emotivo degli alunni durante le lezioni per valutarne il grado di coinvolgimento nella didattica[200]. Con il pretesto di una maggiore esigenza di protezione, dunque, i minori possono addirittura finire per essere oggetto di maggior controllo e tracciamento, destando così serie perplessità circa le ripercussioni a livello pedagogico[201] e, sul piano giuridico, nel rispetto dei principi portanti la disciplina sulla tutela dei dati personali[202].

Come rilevato dal Comitato nazionale di bioetica, le persone ap-

[197] M. ANDREJEVIC, N. SELWYN, *Facial Recognition Technology in Schools: Critical Questions and Concerns*, in *Learning, Media and Technology*, 2, 45, 2020, 115 ss.; T. SIMONITE, G. BARBER, *The Delicate Ethics of Using Facial Recognition in Schools*, in *Wired*, 17 ottobre 2019 [bit.ly/3sXiIe2].

[198] D. HARWELL, *Unproven Facial-Recognition Companies Target Schools, Promising an End to Shootings*, in *The Washington Post*, 7 giugno 2018 [wapo.st/3rYVDWM].

[199] K. PUTHEA, R. HARTANTO, R. HIDAYAT, *A Review Paper on Attendance Marking System Based on Face Recognition*, in *IEEE 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 8 febbraio 2018, 304 ss.

[200] L.B. KRITHIKA, K. VENKATESH, S. RATHORE, M, HARISH KUMAR, *Facial recognition in education system*, in *IOP Conference Series: Materials Science and Engineering*, 263, 4, 2017; M.A.A. DEWAN, M. MURSHED, F. LIN, *Engagement Detection in Online Learning: A Review*, in *Smart Learning Environments*, 6, 1, 2019, 1 ss.

[201] Più ampiamente, sulle nuove forme di sorveglianza sui minori e le ripercussioni sul piano educativo e di tutela della salute psico-fisica, cfr. G.T. MARX, V. STEEVES, *From the Beginning: Children as Subjects and Agents of Surveillance*, in *Surveillance & Society*, 7, 3/4, 2010, 192 ss.

[202] Sull'utilizzo di queste tecnologie per specifiche finalità di sicurezza si sono espresse anche alcune autorità indipendenti di controllo, con particolare riguardo al rispetto del consenso e del principio di proporzionalità; v. *infra* par. 4.1.

partenenti alle fasce di età più bassa o più alta di quella "ottimale" possono andare incontro a una serie di difficoltà nell'uso di queste tecnologie biometriche, qualora non si consideri con la dovuta attenzione la caducità temporale degli elementi fisici usati per il riconoscimento[203].

I test condotti sugli algoritmi di riconoscimento facciale, infatti, dimostrano come vi sia un incremento esponenziale del tasso di errore in relazione alla maggiore e minore età dei soggetti interessati[204]. Sul piano tecnico, in particolare, con specifico riguardo alle persone più giovani, emerge chiaramente come le loro immagini diano origine a una quantità maggiore di falsi-negativi in comparazione a soggetti adulti, a causa della rapida crescita e dei cambiamenti nella fisionomia facciale nel periodo evolutivo. In questo caso, per compromettere l'accuratezza del riconoscimento, è sufficiente che le immagini facciali registrate in gioventù vengano confrontate con immagini dello stesso soggetto dopo che siano trascorsi solamente cinque anni. Per questo, più in generale, si è verificato come lo stato attuale della tecnologia renda meno affidabile l'analisi di immagini di bambini al di sotto dei tredici anni[205].

Si tratta di ipotesi, dunque, che dovrebbero indurre a grande cautela in ragione degli interessi e dei diritti che complessivamente vengono incisi, anche alla luce del rispetto del "*best interests of the child*", quale principio che dovrebbe guidare il bilanciamento dei valori in gioco[206]. Persino nei casi in cui l'impiego di queste tecnologie sembre-

[203] COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, cit., 17.

[204] P. GROTHER, M. NGAN, K. HANAOKA, *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*, cit., 2; N. RAMANATHAN, R. CHELLAPPA, S. BISWAS, *Computational methods for modelling facial aging: A survey*, in *Journal of Visual Languages and Computing*, 20, 2009, 131 ss.; AASHMI, S. SAHNI, S. SAXENA, *Survey: Techniques for Aging Problems in face recognition*, in *MIT International Journal of Computer Science and Information Technology*, 4, 2, agosto 2014, 82 ss.

[205] FRA, *Under watchful eyes – biometrics, EU IT-systems and fundamental rights*, cit., 90.

[206] Sul punto, basti rinviare a E. LAMARQUE, *Prima i bambini. Il principio dei* best interests of the child *nella prospettiva costituzionale*, FrancoAngeli, Milano, 2016, sia in relazione all'espressa menzione al par. 2 dell'art. 24 della CDFUE, nonché sulla normativa secondaria attuativa e sulla giurisprudenza della CGUE che si è appuntata

rebbe più giustificato, come per le indagini su fatti di terrorismo o altri crimini gravi, oppure i controlli di polizia o alle frontiere per rintracciare bambini scomparsi, rapiti o vittime di altri crimini – le stesse ipotesi su cui, peraltro, anche le imprese private hanno posto deroghe alla moratoria sullo sviluppo di queste tecnologie, come accaduto con Amazon[207] e Clearview AI[208] –, rimangono comunque motivi di preoccupazione.

Infine, tra le condizioni che la Costituzione considera tra le più bisognose di azioni positive a tutela, vi sono – per quanto qui rileva – quelle delle persone con *disabilità*. Nonostante la Carta riservi a queste persone un'unica previsione all'art. 38, c. 3, riferita all'educazione e all'avviamento professionale, si può ritenere che esse trovino protezione nell'intero programma di giustizia sociale delineato a livello costituzionale, per come integrato dai documenti internazionali e sovranazionali[209].

Mentre i trattamenti discriminatori che le TRF possono produrre nei confronti delle persone in base al sesso e alla razza hanno ricevuto una relativa attenzione da parte degli studiosi, al contrario sono poco

prevalentemente sul diritto all'ascolto del minore (art. 24, par. 1) e ad intrattenere relazioni regolari con i genitori (art. 24, par. 3) (*ivi*, 111 ss.), sia per la giurisprudenza della Corte EDU che ha elaborato tale concetto, in particolare con riguardo all'art. 6 della CEDU sul principio del giusto processo, in relazione alle garanzie processuali dell'imputato minorenne e all'obbligo di rispettare le sue condizioni di fragilità (*ivi*, 97 s.). Spunti anche in F. PATERNITI, *Figli e ordinamento costituzionale*, Editoriale Scientifica, Napoli, 2019, 143 ss.

[207] Amazon ha consentito l'uso di Rekognition «to help rescue human trafficking victims and reunite missing children with their families»; AMAZON, *We Are Implementing a One-Year Moratorium on Police Use of Rekognition*, 10 giugno 2020 [bit.ly/3dDxWhM].

[208] K. HILL, G.J.X. DANCE, *Clearview's Facial Recognition App is Identifying Child Victims of Abuse*, in *The New York Times*, 10 febbraio 2020 [nyti.ms/39Nilef].

[209] Si ha riguardo al principio personalista, assieme al principio pluralistico e solidaristico all'art. 2 Cost.; la "pari dignità" sancita dall'art. 3, c. 1 Cost., oltre che l'eguaglianza sostanziale al comma successivo; sul punto, per la normativa e la giurisprudenza costituzionale rilevante, ma anche per una ricognizione dei documenti e delle decisioni adottate nell'ambito dell'ONU e dell'ordinamento dell'UE, basti rinviare a G. ARCONZO, *I diritti delle presone con disabilità. Profili costituzionali*, Franco Angeli, Milano, 2020, 139 ss. e 59 ss.; C. COLAPIETRO, *Diritti dei disabili e Costituzione*, Editoriale Scientifica, Napoli, 2011, 56 ss. e 41 ss.

approfondite le conseguenze sulle persone affette da disabilità, le quali, pur rappresentando un campione numericamente inferiore, avrebbero possibilmente maggior bisogno di attenzione in ragione delle specificità e delle caratteristiche differenziate che può assumere una disabilità. In particolare, si pensi a come il tasso di errore nel riconoscimento facciale possa aumentare enormemente in relazione a persone con sindromi craniofacciali, oppure i cui tratti somatici sono stati alterati a seguito di paralisi o, più genericamente, a causa di incidenti o di trattamenti chirurgici[210].

Quelle fin qui ricordate – lavoratori, minori, anziani, disabili – sono solamente alcune delle "categorie" di persone verso le quali il ricorso a TRF può tradursi *ex se* in un pregiudizio in ragione della loro intrinseca condizione. Ciò non toglie, tuttavia, come possano esservi ulteriori soggetti destinati a subire analoghi effetti sfavorevoli, come ad esempio – lo si vedrà – nel caso dei richiedenti asilo[211]. L'impressione complessiva, comunque, è che queste tecnologie, con la loro capacità di incidere sui diritti, tendano in ogni caso ad accentuare la condizione di concreto svantaggio in cui una persona si trova ad essere.

[210] Cfr. S. BYRNE-HABER, *Disability and AI-Bias, in Medium*, 11 luglio 2019 [bit.ly/3fTOBjQ].

[211] V. *infra* Cap. IV, par. 1.

CAPITOLO III

IL TENTATIVO DEL DIRITTO POSITIVO DI REGOLARE LE TRF

SOMMARIO: 1. Considerazioni introduttive: trovare rimedio ad una sostanziale anomia. – 2. La cornice complessiva offerta dalla normativa sul trattamento dei dati personali. – 3. Il "dato biometrico" alla prova delle TRF. – 4. La difficile ricerca di un solido fondamento giuridico per il trattamento dei dati. – 4.1. Un consenso al riconoscimento facciale sempre più consapevole. – 4.2. Il riconoscimento facciale in presenza di "interessi pubblici rilevanti". – 4.3. La necessità di una previsione legislativa e il rispetto del canone di proporzionalità nelle limitazioni ai diritti. – 5. Gli ulteriori principi a protezione dei dati. – 5.1. Limitazione delle finalità e uso secondario delle immagini. – 5.2. La minimizzazione dei dati e la ricerca della giusta misura. – 5.3. Conservazione delle immagini e problematiche connesse. – 6. I diritti conseguenti alla sottoposizione a riconoscimento facciale. – 6.1. Il diritto ad essere consapevoli e ricevere informazioni… – 6.2. (*segue*) …quale condizione per esercitare i diritti di autodeterminazione informativa. – 6.3. La difesa contro gli automatismi del riconoscimento facciale. – 6.4. Profilazione e assottigliamento del confine pubblico/privato. – 6.5. La "comprensibilità" delle TRF. – 7. Le "distorsioni" nel riconoscimento facciale (i c.d. *bias*). – 8. *Law in action*: le TRF portate di fronte ad un giudice. – 9. (*segue*) …e alcuni spunti sull'esperienza italiana: il caso S.A.R.I.

1. *Considerazioni introduttive: trovare rimedio ad una sostanziale anomia*

Una volta colto l'impatto delle TRF sui diritti fondamentali, occorre propriamente interrogarsi su quale sia la regolamentazione giuridica offerta a queste tecnologie di sorveglianza. Punto di partenza è la normativa attualmente vigente, mediante la quale, attraverso principi e regole immediatamente rilevanti, viene composto un primo inquadramento.

Il primo dato da osservare è che, né a livello europeo, né a livello

nazionale – ma la situazione è analoga anche in altri ordinamenti ove si compiono i primi passi, come gli Stati Uniti[1] – è stata adottata alcuna normativa che disciplini espressamente le TRF.

Assistiamo innanzitutto alla presenza di alcune normative settoriali che, a livello interno o di UE[2], concorrono a definire una cornice sulle condizioni di utilizzo e i possibili impieghi di queste tecnologie. Si pensi a quelle fonti che, nell'ambito delle misure per incrementare la sicurezza urbana, autorizzano le autonomie territoriali ad utilizzare sistemi di videosorveglianza[3], compreso l'uso di sistemi anche «tecnolo-

[1] Anche negli Stati Uniti, ove – come visto introduttivamente – le problematiche sollevate dalle TRF sono cospicue e forse più risalenti nel tempo, manca una legislazione espressamente dedicata a queste tecnologie, sebbene vi siano molteplici leggi federali che regolano la raccolta, l'uso e la conservazione delle informazioni sfruttate dalle TRF, o i controlli alle frontiere, o la raccolta e l'utilizzo dei dati personali da parte delle agenzie federali; cfr. *Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations*, cit., 7 ss.; U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, cit., 42. Singoli Stati hanno invece una propria disciplina sulla protezione della *privacy* ed alcuni disciplinano o proibiscono espressamente determinati usi delle TRF; sul punto v. sempre *Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations*, cit., 9 s.; U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, cit., 39; ed anche I. NESTEROVA, *Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world*, in *SHS web of conferences*, 74, 2020, 5 ss. Si segnala come lo Stato di Washington sia stato il primo – e finora pare l'unico – ad adottare una legislazione organica "*Concerning the use of facial recognition services*" da parte delle autorità pubbliche, comprese le forze di polizia, firmata dal Governatore il 31 marzo 2020, che produrrà effetti a partire del luglio 2021 [bit.ly/2Q5qc01]. Per un quadro delle decisioni circa possibili moratorie, v. i riferimenti *retro* nell'Introduzione.

[2] È il caso, ad esempio, della direttiva (UE) 2015/2366 del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, come recepita dal d.lgs. 15 dicembre 2017, n. 218, che introduce il sistema di "autenticazione forte del cliente", il quale prevede per alcune tipologie di pagamento l'autenticazione basata sull'uso di due o più elementi (art. 97), uno dei quali può essere biometrico, come ad esempio il riconoscimento facciale.

[3] Come il d.l. 23 febbraio 2009, n. 11, recante "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori", convertito con legge 23 aprile 2009, n. 38, che all'art. 6, cc. 7 e 8, prevede l'utilizzabilità, da parte dei Comuni, di sistemi di videosorveglianza in luoghi pubblici

gicamente avanzati, dotati di software di analisi video per il monitoraggio attivo»[4]. Parimenti, si consideri la disciplina relativa ai sistemi di videosorveglianza degli impianti sportivi a tutela dell'ordine e della sicurezza pubblica in occasione di eventi sportivi[5].

Riflettendo sulle interferenze e le limitazioni ai diritti fondamentali, si è visto anche come vi siano previsioni che, nella loro generalità, possono applicarsi estensivamente alle TRF, come nel caso della disciplina sull'acquisizione da parte delle forze di polizia dei rilievi fotodattiloscopici o dei dati biometrici, anche nelle sue declinazioni più settoriali[6].

Ciascuno di questi riferimenti normativi, tuttavia, deve trovare applicazione nel contesto di quella che è considerabile come la disciplina giuridica che, attualmente, è destinata ad informare più organicamente e complessivamente l'impiego delle TRF, ovvero la legislazione sulla tutela dei dati personali. Quest'ultima, proprio per la sua portata, è in

o aperti al pubblico per la tutela della sicurezza urbana, con possibilità di conservare i dati fino a sette giorni.

[4] Si veda il più recente d.l. 20 febbraio 2017, n. 14, convertito con modificazioni con la legge 18 aprile 2017, n. 48, che istituisce i c.d. "Patti per l'attuazione della sicurezza urbana", sottoscritti tra il prefetto ed il sindaco, attraverso cui individuare interventi sulla sicurezza urbana, per obiettivi, tra l'altro, quali prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria anche «attraverso l'installazione di sistemi di videosorveglianza» (art. 5, c. 2, lett. a). Nell'ambito di tali patti, oltre che degli accordi conclusi tra Stato e Regioni per la promozione della sicurezza integrata ai sensi dell'art. 3, possono essere individuati specifici obiettivi per l'incremento dei servizi di controllo del territorio e per la sua valorizzazione, comprensivi anche di progetti «per la messa in opera a carico di privati di sistemi di sorveglianza tecnologicamente avanzati, dotati di software di analisi video per il monitoraggio attivo con invio di allarmi automatici a centrali delle forze di polizia o di istituti di vigilanza privata convenzionati» (art. 7, c. 1-*bis*).

[5] V. art. 1-*quater*, c. 3, del d.l. 24 febbraio 2003, n. 28, e il d.m. 6 giugno 2005, relativo alle "Modalità per l'installazione di sistemi di videosorveglianza negli impianti sportivi di capienza superiore alle diecimila unità, in occasione di competizioni sportive riguardanti il gioco del calcio".

[6] V. *retro* Cap. II, par. 5. Anche il d.lgs. 25 luglio 1998, n. 286, prevede che lo straniero che richiede il permesso di soggiorno o che ne chiede il rinnovo è sottoposto a rilievi fotodattiloscopici (art. 5, cc. 2-*bis* e 4-*bis*). Più ampiamente, per ulteriori fondamenti legislativi a supporto delle attività di polizia che implicano trattamento di dati personali non occasionali, si v. il d.m. 24 maggio 2017, su cui v. *infra* nota 41.

grado – lo si vedrà – sia di intercettare alcune delle questioni più problematiche che queste tecnologie fanno emergere, sia di rilevare ai diversi fini delle limitazioni agli altri diritti fondamentali.

Dopo aver dato conto dei riferimenti normativi sulla protezione dei dati entro cui deve collocarsi l'impiego di queste tecnologie, i rispettivi regimi e ambiti di applicazione, l'analisi si snoderà nella disamina di quegli istituti e principi maggiormente rilevanti, per sottolinearne la relativa efficacia e i limiti che essi manifestano.

Così a partire dal concetto di dato biometrico, categoria di dati prodotta dal procedimento algoritmico di riconoscimento facciale. Di seguito, con la medesima logica, saranno analizzati quelli che la normativa in questione individua come i fondamenti di legittimità per la sottoposizione a riconoscimento facciale, ovvero il consenso dell'interessato e le condizioni previste in presenza di interessi pubblici rilevanti. A questo proposito occorrerà dare risalto alla autonoma necessità di disporre di previsioni legislative che si riferiscano a queste tecnologie e alla necessità che esse siano in grado di resistere al test di proporzionalità. Proseguendo, l'analisi si appunterà sui principi a presidio della protezione dei dati personali e sui diritti che propriamente la normativa in questione accorda agli interessati. Specifica attenzione deve essere destinata alle distorsioni (c.d. *bias*) in grado di falsare il procedimento di riconoscimento facciale e ai rimedi che è possibile approntare. Da ultimo, si verificherà come istituti e principi appena ricostruiti abbiano mostrato la propria tenuta "in azione", ovvero nel corso di un contenzioso giurisdizionale verificatosi nel Regno Unito sull'impiego di queste forme di sorveglianza da parte delle forze dell'ordine, dal quale sarà possibile ricavare significativi spunti sulle condizioni per l'utilizzo di queste tecnologie anche nell'esperienza italiana.

2. *La cornice complessiva offerta dalla normativa sulla protezione dei dati personali*

La normativa sulla protezione dei dati personali si articola tanto a livello internazionale e di UE, quanto nella disciplina di recepimento interno. Sotto il primo profilo occorre registrare una molteplicità di

strumenti a protezione della *privacy* e dei dati personali che interagiscono nel panorama internazionale[7]. Ai fini della presente analisi ci si concentrerà su quelli più rilevanti nella loro incidenza, adottati nell'ambito del Consiglio d'Europa. Si ha riguardo alla "Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale" (c.d. Convenzione 108) del 1981, ratificata in Italia con legge 21 febbraio 1989, n. 98, e alla conseguente Raccomandazione n. R(87) 15 del Comitato dei Ministri per "regolamentare l'utilizzo dei dati a carattere personale nel settore della polizia", del 17 settembre 1987. Tali documenti hanno stabilito per la prima volta un regime di protezione dei dati personali in molti degli Stati firmatari e hanno costituito il punto di partenza per lo sviluppo della disciplina comunitaria[8].

Molte delle ragioni che – come si vedrà – hanno spinto a riformare profondamente la disciplina dell'UE sul punto hanno indotto, in parallelo, il Comitato dei Ministri ad adottare il 18 maggio 2018 a Elsinore un protocollo di modifica (c.d. Convenzione 108+) che ha rinnovato profondamente la citata Convenzione[9]. Dal momento che tale pro-

[7] Si consideri, tra i principali, le "*Guidelines for the Regulation of Computerized Personal Data Files*" adottate dall'Assemblea generale delle NU con risoluzione 45/95 del 14 dicembre 1990, o la risoluzione 34/7 su "*The right to privacy in the digital age*" (A/HRC/RES/34/7) del 23 marzo 2017; le "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*" adottate dall'OCSE nel 1980, approvate in una nuova versione nel 2013; la "Risoluzione di Madrid" adottata nel 2009 dalla *International Conference of Data Protection and Privacy Commissioners*. Per una panoramica più approfondita sugli strumenti universali e regionali a protezione di questi diritti umani, cfr. C. PAULETTO, *Options towards a global standard for the protection of individuals with regard to the processing of personal data*, in *Computer Law & Security Review*, 40, 2021, in corso di pubblicazione.

[8] Cfr. L.A. BYGRAVE, *The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects*, in *Computer Law & Security Review*, 40, 2021, 7. Più ampiamente, v. anche C. CARLETTI, *Diritto alla riservatezza, protezione dei dati personali e spazio digitale nell'ordinamento internazionale*, cit., 282 ss.

[9] Il protocollo di modifica ha introdotto una serie di novità rilevanti cui si farà cenno più avanti, quali un rafforzamento nella protezione del diritto all'autonomia informazionale e della dignità a fronte dello sviluppo tecnologico, il consolidamento del principio di proporzionalità come requisito per il trattamento dei dati e l'ampliamento dei diritti a disposizione degli interessati, irrobustendo di converso le responsabilità del titolare del trattamento e gli obblighi di trasparenza. Più ampiamen-

tocollo è stato firmato dall'Italia ma non è stato ancora ratificato, nel proseguo si farà riferimento sia alla versione originaria della Convenzione, sia alle modifiche apportate.

La Convenzione 108, in sostanza, è uno strumento giuridico vincolante di portata universale e aperto all'adesione di nuove Parti. Essa è caratterizzata da una maggior flessibilità rispetto alla normativa vigente dell'UE, in quanto strutturata per principi e suscettibile di essere implementata con maggiore libertà dalle Parti, mediante la propria normativa nazionale o attraverso atti di *soft law* adottati a livello di Consiglio d'Europa[10]. Da una parte, la Convenzione 108 ha una portata più ristretta rispetto alla normativa UE, in quanto difetta, anche nella sua nuova formulazione, di numerose previsioni indicate da quest'ultima e della specificità con cui vengono previsti gli obblighi e i diritti conferiti; dall'altra, offre uno strumento di protezione più ampio, perché – come si vedrà – copre il trattamento dei dati in tutti i settori, pubblici e privati[11]. Uno "standard globale", quindi, meno ostico anche alle imprese e ai *competitors* di altri continenti[12].

Accanto alla normativa che si colloca nell'alveo del Consiglio

te, cfr. C. DE TERWANGN, *Council of Europe convention 108 +: A modernised international treaty for the protection of personal data*, in *International review of law, computers & technology*, 28, 2, 2014, in corso di pubblicazione. Per una elencazione più puntuale delle previsioni aggiunte e delle novità, v. G. GREENLEAF, *Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives*, 142 *Privacy Laws & Business International Report*, 14-17 agosto 2016; S.L. DUQUE DE CARVALHO, *Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108*, in *European data protection law review*, 5, 1, 2019, 55 ss., anche in paragone al GDPR.

[10] Si consideri quanto accaduto nell'ambito dei *big data* con le "*Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*", T-PD(2017)01, 23 gennaio 2017; sul punto, v. P. DE HERT, V. PAPAKONSTANTINOU, *Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should' to 'must' via* soft law *to address more than only individual harms*, in *Computer Law & Security Review*, 40, 2021, in corso di pubblicazione.

[11] V. art. 3 della Convenzione 108; cfr. S.L. DUQUE DE CARVALHO, *Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108*, cit., 55, anche per un elenco delle previsioni del GDPR eccedenti rispetto alla Convenzione 108+.

[12] Cfr. A. MANTELERO, *The future of data protection: Gold standard vs. global standard*, in *Computer Law & Security Review*, 40, 2021, in corso di pubblicazione, 4.

d'Europa troviamo pure la disciplina formulata dalle istituzioni dell'UE in attuazione dell'art. 8 TUE e dall'art. 16 TFUE. Il quadro vigente è costituito da quel "pacchetto protezione dati" adottato nel maggio 2016 che contempla il regolamento (UE) 2016/679, "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" (c.d. GDPR), e la direttiva (UE) 2016/680 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" (c.d. LED)[13].

Il GDPR offre il più avanzato punto di equilibrio tra le istanze dirette a promuovere la libera circolazione del dato, in un'ottica di scambio di libero mercato senza barriere, e la protezione del dato personale, come espressione di tutela delle persone fisiche[14].

Tale regolamento, innanzitutto, contiene una disciplina a carattere sovranazionale che, in ragione della fonte, non si limita a promuovere una armonizzazione del regime di protezione dei dati negli Stati membri, come la precedente direttiva 95/46/CE[15], ma si impone diretta-

[13] Ai due atti citati si aggiunge anche il regolamento (UE) 2018/1725, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

[14] Sottolinea questo aspetto S. SICA, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Wolters Kluver - Cedam, Milano, 2016, 2, che osserva questa tensione già nel titolo dell'atto. La tutela dei dati personali, poi, deve essere intesa come strumento che contribuisce alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche (cons. 2), ma anche «al servizio dell'uomo», da non considerare come «una prerogativa assoluta», ma «alla luce della sua funzione sociale» e contemperata «con altri diritti fondamentali, in ossequio al principio di proporzionalità» (cons. 4).

[15] Sottolinea questo passaggio F. PIZZETTI, *La protezione dei dati personali e le sfide dell'Intelligenza Artificiale*, in F. PIZZETTI ET AL., *Intelligenza artificiale, protezione dati personali e regolazione*, Giappichelli, Torino, 2018, 5 ss. V. anche L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo*

mente ad essi[16]. Si cerca così di andare incontro alle esigenze di "sovraterritorialità" che le nuove tecnologie impongono con la loro diffusione e sfruttamento, nell'insofferenza dei confini propriamente giuridici[17].

Pur ponendosi sotto molti aspetti in linea di continuità con la disciplina previgente – si pensi al rilievo del consenso personale e dell'informativa sul trattamento –, il nuovo regolamento mira a porre rimedio ai limiti manifestati dalla direttiva e alla frammentazione della protezione dei dati all'interno dell'UE che ne è scaturita[18].

La disciplina sulla protezione dei dati diviene quindi di fonte prevalentemente europea e solo limitatamente dei singoli Stati, la cui dimensione risulta economicamente, politicamente e giuridicamente

alla riservatezza e alla protezione dati personali, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, cit., 17 ss.

[16] V. art. 3 per la disciplina sull'ambito di applicazione territoriale del GDPR, che copre le ipotesi di trattamento in cui il titolare o il responsabile sono stabiliti nell'UE, oppure, a certe condizioni, in cui i dati personali sono riferiti a persone che si trovano nell'UE. Cfr. M.G. STANZIONE, *Genesi ed ambito di applicazione*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, cit., 27 ss. La questione del perimetro di applicazione è comunque controversa, come dimostra anche la sentenza CGUE in C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, del 24 settembre 2019, ove si stabilisce che il gestore di un motore di ricerca è tenuto a effettuare la deindicizzazione solo nelle versioni corrispondenti agli Stati membri; sul punto cfr. O. POLLICINO, *L' "autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *Federalismi.it*, 19, 2019, 1 ss., anche per ulteriori spunti giurisprudenziali.

[17] Di «questione eminentemente transnazionale, e come tale difficilmente ricomponibile ricorrendo alla tradizione giuridica singolo-nazionale», parla A. VENANZONI, *Intersezioni costituzionali – Internet e Intelligenze Artificiali tra ordine spontaneo, natura delle cose digitale e garanzia dei diritti fondamentali*, in *Forum di Quaderni Cost.*, 27 aprile 2018, 4. V. anche S. RODOTÀ, *Il diritto di avere diritti*, cit., 426.

[18] Sul punto si v. il cons. 9 del GDPR. Valorizza questo aspetto C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 22, 2018, 3. V. anche M.G. STANZIONE, *Genesi ed ambito di applicazione*, cit., 20; D. POLETTI, *Comprendere il Reg. UE 2016/679: un'introduzione*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, PUP, Pisa, 2018, 10.

inadeguata[19], imponendo un cambiamento nel modo di proteggere i dati personali rispetto a quanto avveniva venticinque anni fa[20].

Il quadro normativo, dunque, si compone oggi a livello UE dal GDPR, e a livello nazionale dal d.lgs. n. 196/2003, per come profondamente modificato dal d.lgs. n. 101/2018, che ha portato sostanzialmente all'adozione di un nuovo codice della *privacy*[21]. Del previgente d.lgs. n. 196/2003 sono state infatti abrogate le parti relative al trattamento dei dati in generale, che si sarebbero sovrapposte ai contenuti del regolamento, mentre sono state profondamente modificate le previsioni riferite ad ambiti legati alle peculiarità dell'ordinamento nazionale, come il diritto al lavoro, penale o amministrativo, cui si aggiungono le numerose disposizioni finali e di coordinamento[22]. Per questa ragione, nel resto della trattazione si farà prevalentemente riferimento al GDPR, salvo evidenziare ove occorra le specificazioni apportate dalla normativa nazionale. Centrali, poi, sono i numerosissimi atti adottati

[19] Si consideri come oggi la competizione si giochi tra *player* di diversi continenti: sullo scambio dei dati tra UE e USA, ad esempio, si vedano le importanti pronunce della Corte di giustizia adottate anche prima dell'adozione del GDPR, come nel caso *Schrems* del 2015 (cui ha fatto seguito *Schrems II* del 2020), o anche sulla portata di applicazione della normativa sulla protezione dei dati, come nel caso *Google Spain* del 2014 (cui ha fatto seguito ad esempio il sopra citato caso *Google LLC* del 2019), assieme alle ulteriori pronunce cui si farà riferimento più avanti nel testo; per una ricognizione della giurisprudenza rilevante, anche per i richiami bibliografici, v. O. POLLICINO, M. BASSINI, *Art. 8. Protezione dei dati di carattere personale*, cit., 141 ss.; L.P. VANONI, *L'applicazione del Bill of Rights europeo tra bilanciamento asimmetrico e paradosso federale: il caso della privacy digitale*, in *DPCE online*, 2, 2019, 1215 ss.

[20] G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in EAD. (a cura di), *La protezione dei dati personali in Italia*, cit., 1 ss.

[21] Per una ricostruzione nella successione di questi atti normativi, del percorso di adozione e dei contenuti del d.lgs. n. 101/2018, v. G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, cit., 3 ss., e S. SCAGLIARINI, *Dal "vecchio" al "nuovo" Codice della privacy*, in ID. (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali*, Giappichelli, Torino, 2019, spec. 9 s.

[22] Si pensi, per quanto qui rileva maggiormente, all'art. 22, c. 4, d.lgs. n. 101/2018, volto a stabilire l'ulteriore applicabilità dei provvedimenti del Garante dopo l'abrogazione della direttiva 95/46/CE, in quanto compatibili con il GDPR e il nuovo codice, come ad esempio i provvedimenti sui dati biometrici che si citeranno più avanti.

nell'esercizio della loro funzione paranormativa da parte sia dal Garante europeo e dal Gruppo di lavoro "Articolo 29", sia dal Garante della *privacy* italiano, che nel tempo hanno sì concorso a far perdere di centralità il richiamato codice, ma hanno anche favorito una concretizzazione dei precetti legislativo e una più effettiva tutela dei dati personali[23].

Tra le importanti novità introdotte e le molteplici chiavi di lettura adoperabili[24], interessa qui segnalare introduttivamente il passaggio da un approccio rimediale e riparatorio alla tutela dei dati personali, ad uno improntato ad anticipare la tutela ad un momento precedente al trattamento e prevenire così le possibili lesioni[25]. Questo passaggio si

[23] Cfr. A. SIMONCINI, *Il sistema delle fonti di disciplina del trattamento di dati personali*, in V. CUFFARO, L. RICCIUTO (a cura di), *Il trattamento dei dati personali*, II, Giappichelli, Torino, 1999, 35 ss., che osserva come il Garante, sebbene inizialmente sprovvisto di poteri normativi, li abbia acquisiti col tempo *de facto* e *de jure*.. Ai fini del presente discorso, oltre ai richiami che verranno svolti nel prosieguo, si pensi all'importanza delle "misure di garanzia" che il Garante della *privacy* dovrà adottare ai sensi dell'art. 2-*septies*, del d.lgs. n. 196/2003, le quali, in attuazione delle previsioni del GDPR relative ai dati "sensibili", tra cui rientrano – lo si vedrà – anche i dati biometrici elaborati dalle TRF, devono fissare le condizioni per il relativo trattamento.

[24] Per una prima panoramica delle novità introdotte dal GDPR, cfr. C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, cit. Il senso di queste modifiche è indicato in S. SCAGLIARINI, *Dal "vecchio" al "nuovo" Codice della privacy*, cit., 19, come il passaggio da una origine pretoria del diritto alla protezione dei dati, ad una prima regolazione fondata sulla visione proprietaria dei dati, in cui le autorizzazioni e i controlli preventivi del Garante avevano un peso rilevante, fino ad una legislazione che ha lasciato all'autorità pubblica il ruolo di soggetto regolatore ed ha valorizzato l'assunzione di responsabilità del singolo titolare del trattamento, riservando all'intervento del Garante un compito di controllo e di eventuale sanzione *a posteriori* nel caso di abusi nel margine di autovalutazione dei singoli.

[25] Più ampiamente sul punto, v. G. GIANNONE CODIGLIONE, Risk-based approach *e trattamento dei dati personali*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, cit., 55 ss.; A. MANTELERO, *La gestione del rischio*, cit., 473 ss.; F. PIZZETTI, *GDPR e Intelligenza artificiale. Codici di condotta, certificazioni, sigilli, marchi e altri poteri di soft law previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA*, *ivi*, 69 ss.; L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, cit., 34 ss.; G. SARTOR, F. LAGIOIA, *The impact of the General Data Pro-*

sostanzia, prima di tutto, in una valorizzazione del principio di "*accountability*", termine complesso che può essere inteso anche come "responsabilità". In base a tale principio scaturisce l'obbligo per il titolare del trattamento tanto di conformarsi alla normativa a protezione dei dati tramite procedure e misure tecniche e organizzative, quanto di dover essere in grado di dimostrare tale conformità[26]. Questo approccio assume forma, poi, in una serie di ulteriori istituti e principi che verranno presi in considerazione nel corso della trattazione e che proprio il titolare del trattamento ha la responsabilità di attuare e applicare[27].

Il secondo atto del "pacchetto" è costituito poi dalla LED, che si pone in termini di complementarietà rispetto al GDPR[28]. La disciplina della direttiva non risulta esattamente allineata e coincidente con il

tection Regulation (GDPR) on artificial intelligence, cit., 66 ss. Segnala D. POLETTI, *Comprendere il Reg. UE 2016/679: un'introduzione*, cit., 12, il passaggio dall'osservanza di specifiche misure di sicurezza (anche legislativamente previste) alla scelta e all'applicazione di quelle che risultino più adeguate in ogni specifico contesto; dall'adempimento di una dettagliata normativa ad un vero e proprio sistema di gestione del rischio; dalla responsabilità alla "responsabilizzazione"; dalla riparazione del danno alla prevenzione dello stesso.

[26] Art. 5, par. 2, del GDPR. In base a GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2010 sul principio di responsabilità*, WP 173, 13 luglio 2010, si tratta di un termine complesso traducibile come "*reinforced responsibility*" (responsabilità rafforzata), "*assurance*" (assicurazione), "*reliability*" (affidabilità), "*trustworthiness*" (attendibilità) e, in francese, "*obligation de rendre des comptes*" (obbligo di rendere conto), ecc. (22). Si aggiunge anche che l'architettura giuridica dei meccanismi di responsabilità prevedrebbe due livelli: il primo, costituito da un obbligo di base vincolante per tutti i titolari del trattamento, che comprenderebbe sia l'attuazione di misure e/o procedure, sia la conservazione delle relative prove; il secondo includerebbe sistemi di responsabilità di natura volontaria eccedenti le norme di legge minime (15). Tale dimostrazione può passare eventualmente tramite la certificazione di soggetti esterni (66 ss.).

[27] Quali l'individuazione della base giuridica e la verifica circa l'applicabilità del consenso come presupposto di legittimità (v. *infra* par. 4.1), le misure di sicurezza da adottare (v. *infra* par. 5.3), la valutazione preliminare dei rischi (v. *infra* Cap. V, par. 2), i principi di *privacy by design* e *by default* (v. *infra* Cap. V, par. 5).

[28] A. RICCI, *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati. Riflessioni sul d.lgs. 18 maggio 2018, n. 51, di attuazione della dir. 2016/680/UE*, in *Le Nuove leggi civili commentate*, 3, 2019, 565, 571 s.

GDPR, dal momento che la disciplina sulla protezione dei dati personali ai fini della prevenzione e repressione dei reati comporta inevitabilmente un bilanciamento più complesso nel quale, assieme all'interesse del singolo alla tutela dei dati personali, occorre tener conto delle esigenze di natura pubblicistica e sociale legate alla tutela dell'ordine pubblico e alla cooperazione informativa tra le autorità di contrasto[29]. In questo senso, la stessa scelta di ricorrere ad una direttiva riflette questa pluralità di istanze, rimettendo agli Stati un significativo margine di discrezionalità per la relativa attuazione[30].

Le diversità presenti, inoltre, sono il portato dell'originale struttura a pilastri che caratterizzava l'UE prima dell'entrata in vigore del Trattato di Lisbona, la quale ha determinato nel tempo una proliferazione di strumenti giuridici in materia di cooperazione giudiziaria e di polizia in materia penale, con una conseguente frammentazione del quadro normativo, dando origine ad una serie di atti non sempre coordi-

[29] Su questo aspetto, cfr. A. RICCI, *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati*, cit., 572 ss.; G. RUGANI, *La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della Direttiva (Ue) 2016/680: frammentazione ed incertezze applicative*, in *Freedom, Security & Justice: European Legal Studies*, 1, 2019, 75 s.; P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, cit., 319, a proposito della "qualità" e "sicurezza" dei dati, in modo da evitare il rischio che a circolare siano informazioni della cui veridicità e affidabilità si possa dubitare. Sottolinea come si vada a toccare così il "nucleo della sovranità statale", P. MILAZZO, *La Direttiva UE 2016/680 e la protezione dei dati personali nell'ambito della sicurezza pubblica e della giustizia penale*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, cit., 723.

[30] T. MARQUENIE, *The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework*, in *Computer Law & Security Review*, 33, 3, 2017, 328 s. Anche la presenza di numerose eccezioni rimesse agli Stati membri e clausole di apertura concorrono in questo senso, come rilevato in S. CONTI, G. PERUGINELLI, *L'impatto del regolamento europeo in materia di protezione dei dati personali sull'attività giurisdizionale*, in *Ciberspazio e Diritto*, 1-2, 2018, 137. Si considerino, ad esempio, la mancanza di indicazioni su come intendere criteri generali al pari di "necessità", "proporzionalità", "appropriatezza", oppure le deroghe o restrizioni ai diritti dell'interessato, o lo stesso concetto di "autorità competente" su cui v. *infra* nota 33.

nati tra di loro nello stabilire la disciplina e il livello di protezione effettivo dei dati personali, a discapito tanto della tutela del singolo, quanto della cooperazione tra autorità pubbliche[31]. A tutt'oggi la complessità del panorama normativo non può dirsi interamente superata[32], date le incertezze derivanti dal raccordo con il GDPR[33], ma an-

[31] All'origine della disciplina sulla protezione dei dati nel settore di polizia si collocano le già menzionate Convenzione 108 e la Raccomandazione n. R(87) 15. Dal momento che la successiva direttiva 95/46/CE non si applicava ai trattamenti nel settore della cooperazione giudiziaria e di polizia, si è assistito alla proliferazione di atti normativi al di fuori della cornice dell'UE, che peraltro continuavano a fare riferimento ai due atti sopra citati, quali la "Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985", del 19 giugno 1990, ratificata con legge n. 388/1993, che ha istituito il Sistema d'Informazione Schengen (SIS) (art. 117, par. 1) (v. *infra* Cap. IV, par. 2); la Convenzione istitutiva dell'Europol, del 26 luglio 1995 (art. 14), l'istituzione dell'Unità di cooperazione giudiziaria dell'Unione Europea (Eurojust), con decisione 2002/187/GAI del Consiglio (art. 14, par. 2); il Trattato di Prüm, riguardante l'approfondimento della cooperazione transfrontaliera, in particolare al fine di lottare contro il terrorismo, la criminalità transfrontaliera e la migrazione illegale, stipulato il 27 maggio 2005 (art. 34, par. 1), poi incorporato nel diritto UE con la Decisione 2008/615/GAI (v. *infra* Cap. IV, par. 1). Tali riferimenti contribuivano a rendere poco chiaro e coerente il quadro normativo complessivo, con le conseguenze sottolineate in P. DE HERT, V. PAPAKONSTANTINOU, *The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area*, *Study for the LIBE Committee*, PE 510.001, 2014, 10; H. HIJMANS, A. SCIROCCO, *Shortcomings in EU data protection in the third and the Second Pillars. Can the Lisbon Treaty be expected to help?*, in *Common Market Law Review*, 46, 5, 2009, 1496. L'ultima tappa prima dell'entrata in vigore della LED è segnata dalla decisione quadro 2008/977/GAI, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, la quale tuttavia, al cons. 39 e all'art. 28, regolava il rapporto con gli altri atti dell'UE adottati in precedenza, come quelli richiamati, stabilendo come questi ultimi prevalessero qualora «siano state introdotte condizioni specifiche relative all'utilizzo di tali dati da parte dello Stato membro ricevente». In questo modo, anche la decisione quadro 2008/977/GAI non ha certo contribuito a uniformare le regole progressivamente stratificatesi e dare loro coerenza; G. RUGANI, *La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della Direttiva (Ue) 2016/680: frammentazione ed incertezze applicative*, cit., 79. Più ampiamente, v. anche P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, cit., 313 ss.; P. MILAZZO, *La Direttiva UE 2016/680 e la protezione dei dati personali nell'ambito della sicurezza pubblica e della giustizia penale*, cit., 709 ss.

[32] Come rilevano, tra gli altri, T. MARQUENIE, *The Police and Criminal Justice Au-*

che la circostanza che la direttiva lascia comunque impregiudicate le disposizioni specifiche per la protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia adottate in precedenza[34]. In aggiunta, sono state successivamente adottate ulteriori fonti che si affiancano a quelle della LED[35].

thorities Directive: Data protection standards and impact on the legal framework, cit., 328; G. RUGANI, *La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della Direttiva (Ue) 2016/680: frammentazione ed incertezze applicative*, cit., 84 ss.,

[33] Il parere del Gruppo di lavoro "Articolo 29" sulla bozza di direttiva, ad esempio, osserva come il GDPR ponga garanzie di protezione più elevate e imponga obblighi più stringenti sul titolare del trattamento rispetto alla LED; cfr. GRUPPO DI LAVORO ARTICOLO 29, *Parere 03/2015 sulla proposta di direttiva concernente la tutela 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, e la libera circolazione di tali dati*, WP233, 1 dicembre 2015, 4. Sussistono altresì problematiche più specifiche. Quanto all'ambito di applicazione, si osserva come la nozione di "autorità competente" all'art. 3, par. 1, n. 7, comprensiva di «qualsiasi autorità pubblica competente» e «qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica», contenga un riferimento (alla "salvaguardia contro e prevenzione di minacce alla sicurezza pubblica") che determina «un diverso grado di protezione dipendente dalla sua attuazione da parte degli Stati membri» (*ibidem*). Riferisce poi M.M. CARUANA, *The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement*, in *International Review of Law, Computers & Technology*, 33, 3, 2017, 249 ss., come tale nozione sia talmente ampia da comprendere non solo le autorità di contrasto, ma anche altri soggetti, quali le compagnie di sicurezza private, che in alcuni Stati membri non sono considerate autorità di contrasto, e dunque sono soggetti al GDPR. Sottolinea P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, cit., 333 s., come la LED si applichi per le attività a seguito di *notitia criminis*, in vista di prevenzione di reati anche in assenza di previa notizia di un fatto penalmente rilevante, e per l'esecuzione di sanzioni penali; al di fuori di questi casi trova invece applicazione il GDPR (art. 9).

[34] Così in base all'art. 60 LED.

[35] Oltre al già citato regolamento (UE) 2018/1725, anche il regolamento (UE) 2016/794, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol), che dedica gli artt. 28-46 alle "Garanzie in materia di protezione dei dati"; il regolamento (UE) 2018/1727, del 14 no-

Nonostante ciò, a fronte dei limiti manifestati dalla precedente decisione quadro 2008/977/GAI, ora abrogata, che non era riuscita a realizzare un sufficiente grado di armonizzazione[36], la LED si fa portatrice di novità notevoli ai fini del presente discorso[37], non da ultimo la sua applicabilità tanto agli scambi transfrontalieri di dati[38], quanto ai trattamenti effettuati all'interno dei confini nazionali[39].

A livello interno, nel settore di polizia, il quadro normativo si completa con il d.lgs. 18 maggio 2018, n. 51, attuativo della LED, che recepisce pressoché integralmente la direttiva riproducendone i contenuti[40]. In analogia al GDPR, anche in questo caso sarà possibile fare prevalentemente riferimento alla normativa dell'UE, salvo considerare le norme attuative più significative introdotte dal legislatore italiano. Sul punto, tuttavia, si segnala un'ulteriore complicazione dovuta alla circostanza che risulta attualmente in vigore, seppur in via transitoria, la normativa attuativa di rango regolamentare di cui al d.P.R. 15 gennaio 2018, n. 15, e al decreto del Ministero dell'interno 24 maggio

vembre 2018, che istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust), che dedica gli artt. 26-46 al "Trattamento delle informazioni".

[36] Più ampiamente, cfr. P. DE HERT, V. PAPAKONSTANTINOU, *The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area*, cit., 7 ss.

[37] La nuova direttiva eleva gli standard di protezione dei dati, introduce più forti garanzie contro le lesioni dei diritti, fornisce maggiori informazioni ai titolari dei dati sui propri diritti, introduce meccanismi di controllo più significativi, dispone che le limitazioni ai diritti o le eccezioni rispetto alle regole poste siano giustificate solamente nel rispetto dei requisiti di necessità e proporzionalità; cfr. T. MARQUENIE, *The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework*, cit., 328.

[38] A differenza di quanto accadeva con la decisione quadro 2008/977/GAI (art. 1, par. 2), il quale originava una difficoltà nello stabilire quando i dati venivano trattati esclusivamente a livello interno e quando si verificava uno scambio tra Stati, e conseguentemente quando dovessero essere istituiti *database* separati per tenere tali dati ben distinti; cfr. P. DE HERT, V. PAPAKONSTANTINOU, *The new police and criminal justice data protection directive: A first analysis*, in *New journal of European criminal law*, 7, 1, 2016, 7 ss.

[39] V. art. 2 e cons. 12 LED. Aspetto enfatizzato, ad esempio, da A. RICCI, *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati*, cit., 571.

[40] *Ivi*, 576 ss.

2017, entrambi non pienamente allineati con la LED e il d.lgs. n. 51/2018[41].

Sebbene le finalità del trattamento considerate dalla LED siano solo quelle della prevenzione e repressione dei reati, numerose sue previ-

[41] L'art. 57 del d.lgs. n. 196/2003 demandava ad un d.P.R. l'adozione della normativa attuativa sul trattamento dei dati a fini di polizia di cui all'art. 53 dello stesso d.lgs. n. 196/2003, per come modificato nel frattempo dal d.l n. 7/2015, convertito dalla legge n. 43/2015. Conseguentemente, è stato adottato il d.P.R. 15 gennaio 2018, n. 15. Tale art. 57 è stato poi abrogato dal d.lgs. n. 51/2018, in attuazione della LED. L'art. 49, c. 3, del d.lgs. n. 51/2018, tuttavia, ha previsto che, in via transitoria, il citato d.P.R. rimanga in vigore fino all'adozione di diversa disciplina attuativa del d.lgs. n. 51/2018 stesso. La disciplina nel citato d.P.R., tuttavia, è stata formulata precedentemente all'adozione del d.lgs. n. 51/2018 e replica ancora numerose previsioni originarie del Codice della privacy. Pertanto, tale d.P.R. dovrà considerarsi abrogato nella misura in cui non sia più compatibile con il d.lgs. n. 51/2018, profilando un'operazione ermeneutica nient'affatto pacifica. Si pensi, quanto all'oggetto e all'ambito di applicazione, al fatto che l'art. 1, c. 2, del d.lgs. n. 51/2018 riprenda le disposizioni all'art. 1, par. 1, e all'art. 3, par. 1, n. 7 della LED, replicando le incertezze riportate sopra in nota 33 a proposito dell'ampiezza con cui vengono identificate le "autorità competenti", mentre l'art. 3 del d.P.R. n. 15/2018 riporti ancora le previsioni all'art. 53, per come modificato dal d.l n. 7/2015, riferendosi in termini più restrittivi ai trattamenti che sono «*direttamente* correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati» (enfasi aggiunta).

Il d.m. 24 maggio 2017, che al pari del d.P.R. citato sopra rimane ancora transitoriamente in vigore, è stato invece adottato in attuazione dell'allora vigente art. 53, c. 3, del Codice, che demandava ad un regolamento il compito di individuare i «trattamenti non occasionali» effettuati «dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento», esenti dal rispetto di numerose previsioni del Codice stesso che ora sono state abrogate perché sostituite dal GDPR e dalla LED, secondo il regime di cui si dirà più avanti: si tratta delle previsioni allora vigenti relative, ad esempio, al diritto di accesso, rettifica e integrazione dell'interessato (artt. 9 e 10), l'informativa da rendere (art. 13), le misure da assumere a seguito di cessazione dei trattamento (art. 16), il limite dello svolgimento del trattamento per fini istituzionali (art. 18), persino i principi applicabili al trattamento di dati sensibili (art. 20 e 22), nonché la disciplina sui trasferimento dei dati all'estero (artt. 42-25); la possibilità di operare tali deroghe dovrà essere vagliata alla luce del nuovo quadro normativo e alla conferma o meno di tali ipotesi derogatorie.

sioni ricalcano o riprendono quelle contenute nel GDPR. Ai due regimi, dunque, si potrà fare richiamo congiuntamente, pur tenendo in debito conto le rispettive differenze.

Nel prosieguo dell'analisi, infine, occorrerà inevitabilmente adoperare una prospettiva tipicamente "multilivello"[42], con la quale verranno operati dei frequenti riferimenti incrociati alla tutela dei dati personali apprestata non solo a livello interno, ma soprattutto a livello di UE e di Consiglio d'Europa, compresi gli indirizzi giurisprudenziali elaborati da CGUE e Corte EDU. Occorrerà ovviamente tener presente, da una parte, la differente efficacia vincolante delle norme appartenenti ai due ordinamenti, l'una in termini di *primauté* sul diritto interno, l'altra come limite al legislatore in base all'art. 117, c. 1 Cost.[43]; dall'altra, non si trascurerà l'osmosi tra i due sistemi determinata dall'art. 52, par. 3 della CDFUE, in forza del quale la CEDU opera come parametro di interpretazione per i c.d. diritti corrispondenti della CDFUE[44].

[42] Sul punto, per un inquadramento sistematico sulla tutela multilivello dei diritti fondamentali, da intendersi come complesso di istituti attraverso cui si articolano le competenze e le relazioni tra le istanze giurisdizionali degli ordinamenti nazionali e sovranazionali preposte alla tutela di tali diritti, basti rinviare ad A. CARDONE, *La tutela multilivello dei diritti fondamentali*, Giuffrè, Milano, 2012.

[43] *Ex multis*, C.cost., sent. nn. 348 e 349/2007, nn. 301 e 317/2009, nn. 120 e 240/2018, n. 25/2019, n. 35/2021.

[44] La Corte EDU – come già riferito *retro* in Cap. II, par. 4 – ha infatti ricondotto la protezione dei dati personali ad un aspetto della tutela della vita privata all'art. 8 della CEDU, il quale, in base alle Spiegazioni alla CDFUE, trova corrispondenza nell'art. 7 di quest'ultima; cfr. GUUE, *Spiegazioni relative alla Carta dei diritti fondamentali*, C303/02, 14 dicembre 2007. Più approfonditamente, v. anche O. POLLICINO, M. BASSINI, *Art. 8. Protezione dei dati di carattere personale*, cit., 135 s., e S. CALZOLAIO, *Protezione dei dati personali*, cit., 618. Sui richiami alla CDFUE da parte della Corte EDU, per rendere la CDFUE uno "strumento vivente", cfr. G. GAJA, *The Charter of Fundamental Rights in the Context of International Instruments for the Protection of Human Rights*, in *European Papers*, 1, 3, 2016, 792 ss. Sull'influenza della CEDU nell'interpretazione della CDFUE, v. anche L.S. ROSSI, *I rapporti fra la Carta dei diritti fondamentali e la CEDU nella giurisprudenza delle rispettive Corti*, in *AISDUE*, 30 dicembre 2020, spec. 44. Più in generale, sui rapporti tra CEDU e CDFUE, v. anche N. LAZZERINI, *La Carta dei diritti fondamentali dell'Unione europea. I limiti di applicazione*, FrancoAngeli, Milano, 2018, 64 ss.

3. *Il "dato biometrico" alla prova delle TRF*

Il primo aspetto da inquadrare nello stretto legame tra normativa sulla protezione dei dati e TRF, nella prospettiva sopra esposta, consiste nel chiarire preliminarmente quali siano e come venga definito il regime giuridico dei dati che rilevano ai fini del riconoscimento facciale, ossia i *dati biometrici*.

Usando una immagine, si potrebbe sostenere che i dati biometrici rappresentino una "forma di digitalizzazione del corpo umano"[45]. Si è già detto di come, nelle pratiche contemporanee di sorveglianza, le persone divengano fonti di informazione nei loro comportamenti, abitudini, preferenze, e tendano quindi ad essere "smaterializzate" in flussi di dati[46]. Nel dato biometrico, però, è il corpo stesso, o meglio le sue singole parti, a divenire direttamente fonti di informazioni digitali tramite le quali riuscire ad identificare le singole persone[47]. Il volto di una persona, le impronte digitali, il DNA, la forma dell'iride, la struttura vascolare della retina, la geometria e la struttura venosa della mano, la voce, ma anche il comportamento; sono come una sorta di "codici a barre" che emettono segnali con i quali gli individui vengono distinti gli uni dagli altri[48].

Questa identificazione è resa possibili perché i dati biometrici che così si possono ricavare presentano alcune caratteristiche essenziali, che variano in base alle caratteristiche prese in considerazione[49]: universalità, in quanto tutte le persone hanno gli stessi "elementi" fisici;

[45] I. VAN DER PLOEG, *Biometric identification technologies: ethical implications of the informatization of the body. Biometric Technology & Ethics, BITE Policy Paper no.1*, 2005.

[46] Cfr. *retro* Cap. II, parr. 2 e 4.

[47] D. LYON, *La società sorvegliata*, cit., 95 s. Più ampiamente, v. A.K. JAIN, A.A. ROSS, *Introduction to Biometrics*, in A.K. JAIN, P. FLYNN, A.A. ROSS (a cura di), *Handbook of Biometrics*, Springer, New York, 2008, 1 ss. Sullo sviluppo delle tecnologie biometriche, a partire dal XIX° secolo, v. J. PUGLIESE, *Biometrics. Bodies, Technologies, Biopolitics*, Routledge, New York-Oxon, 2010, 25 ss.

[48] Cfr. S. AMATO, *Ai confini del corpo*, in S. AMATO, F. CRISTOFARI, S. RACITI, *Biometria: i codici a barre del corpo*, Giappichelli, Torino, 2013, 5 ss.

[49] COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, cit., 6.

distinguibilità, in quanto tali dati si basano su caratteristiche biometriche uniche; permanenza, in quanto tali caratteristiche si mantengono quasi inalterate nel corso della vita di una persona; collezionabilità, in quanto le informazioni così raccolte possono essere conservate, utilizzate e riutilizzate.

Stabilire una definizione giuridica univoca di dato biometrico rilevante ai fini delle TRF risulta alquanto problematico, dal momento che il progresso scientifico e l'evoluzione della tecnologia ampliano costantemente la possibilità di acquisire e elaborare questo tipo di dati, impedendo di fornire un inquadramento statico e definitivo[50].

La direttiva 95/46/CE e la Convenzione 108 non riconoscevano la specificità dei dati biometrici, ma facevano solamente un riferimento generale alla categoria dei "dati personali". Sulla scorta delle sollecitazioni a elaborare una definizione a livello internazionale[51], il GDPR, la LED e la Convenzione 108+ introducono una disciplina che, da una parte, è collegata ad una specifica definizione di dati biometrici e, dall'altra, ricollegano ad essi precise garanzie.

Il trattamento delle immagini facciali è di per sé coperto dalla tutela della vita privata all'art. 8 della CEDU[52]. In base alla più recente normativa, però, le immagini sono riconducibili nell'ambito della nuova e ampia nozione di "dato personale"[53], nella misura in cui, come so-

[50] Come sottolineato anche in A. IANNUZZI, F. FILOSA, *Il trattamento dei dati genetici e biometrici*, in *Dirittifondamentali.it*, 2, 2019, 2.

[51] Si consideri la risoluzione 1797 (2011) dell'Assemblea Parlamentare del Consiglio d'Europa *The need for a global consideration of the human rights implications of biometrics*, ove si osservava che «at the European level, the existing legal framework remains vague, as there is no generally accepted definition of "biometric data"» (3).

[52] Cfr. Corte EDU, *von Hannover v Germany*, 24 giugno 2004, p. 76 ss.; *Bogomolova v Russia*, 20 giugno 2017, p. 52.

[53] Viene qualificata "dato personale" «qualsiasi informazione riguardante una persona fisica identificata o identificabile»; si considera identificabile «la persona fisica che può essere identificata, *direttamente* o *indirettamente*, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale» (art. 4, par. 1, n. 1, del GDPR; art. 3, par. 1, n. 1, della LED; enfasi aggiunta). Sottolinea particolarmente l'ampiezza e l'elasticità di questa nozione, C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul*

litamente accade nelle comuni fotografie, non bastino di per sé a identificare il soggetto ritratto se sconosciuto, ovvero a ricollegarlo alle sue generalità[54].

I "dati biometrici", invece, vengono espressamente qualificati come quei «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»[55]. Le semplici videoriprese o fotografie, dunque, rientrano in questa categoria nella misura in cui ricorrano tali condizioni relative a: la natura dei dati (*i.e.* la riproduzione delle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica); mezzi e modalità del trattamento (*i.e.* la loro sottoposizione ad un trattamento tecnico specifico); finalità del trattamento (*i.e.* la possibilità di identificare in modo univoco una persona fisica)[56]. La riconducibilità dei dati a tali caratteristiche ai fini dell'identificazione, inoltre, può scontare anche un certo margine di probabilità[57]. Entro questi parametri, dunque, occor-

contesto normativo nazionale, cit., 15 ss. Si legge nei considerando, infatti, che «per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici» (cons. 26 GDPR; cons. 21 LED). Di «funzione di onnicomprensività» e di «capacità di attrazione di nuove situazioni non previste né prevedibili *ex ante* dal legislatore» parla S. SICA, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, cit., 5.

[54] Considerando 51 al GDPR. Cfr. anche COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, 2.0, 29 gennaio 2020, 7. Si veda anche CGUE, C-212/13, *Rynes c. Urad*, dell'11 dicembre 2014, in cui la Corte ha qualificato come «trattamento» concernente – per l'appunto – «dati personali» l'utilizzo di un sistema di videosorveglianza, con registrazione continua delle immagini, installato davanti ad una abitazione familiare a scopo di sicurezza dei proprietari (p. 25).

[55] Art. 4, par. 1, n. 14 GDPR; art. 3, par. 1, n. 13 LED.

[56] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 19 s.

[57] Il Gruppo di lavoro "Articolo 29" esplicita tale definizione riferendosi ai dati biometrici come «proprietà biologiche, aspetti comportamentali, caratteristiche fisio-

re applicare il regime delle categorie "particolari" di dati, chiamati comunemente "dati sensibili", sottoposti a regole specifiche rispetto agli altri dati personali[58].

Quanto detto, dunque, impone di distinguere tra le diverse finalità perseguibili tramite riconoscimento facciale. Mentre è pacifico che il regime sui dati biometrici trovi applicazione se l'obiettivo è l'identificazione di un soggetto tramite una comparazione uno-a-molti, qualche dubbio si potrebbe nutrire per l'ipotesi della verifica o autenticazione uno-a-uno. Il Comitato europeo per la protezione dei dati ha stabilito espressamente, tuttavia, che se le generalità di un soggetto non sono conosciute, ma il sistema di riconoscimento facciale effettua una conservazione dei dati anche solo come modello di riferimento, allo scopo, ad esempio, di tracciare l'interessato, siamo comunque in presenza di un trattamento di dati biometrici[59]. Ne consegue che tali regole si applicano sia se la verificazione avviene nei confronti di una persona conosciuta e ben definita, come ad esempio in un controllo per verificare l'identità di un soggetto a partire dalla fotografia presente su un documento, sia che il titolare non abbia comunque modo di risalire all'identità del soggetto, purché si conservi il *template* biometrico. In questo caso, dunque, più che di "identificazione" in senso stretto si potrebbe parlare di "rilevamento"[60].

logiche, tratti biologici o azioni ripetibili laddove tali caratteristiche e/o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità»; cfr. GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, cit., 2; ma v. già ID., *Parere 4/2007 sul concetto di dati personali*, cit., 4.

[58] Art. 9, par. 1 GDPR; art. 10 LED.

[59] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 20.

[60] In questo senso la "identificazione" non starebbe a rappresentare quella attività complessa ricomprendente (i) l'attribuzione ad un soggetto i propri dati identificativi, intesi come coordinate giuridiche ritenute necessarie e sufficienti dall'ordinamento per distinguerlo rispetto agli altri; (ii) l'autenticazione, intesa come corretto accertamento della corrispondenza dei dati attribuiti ai caratteri somatici peculiari del soggetto; (iii) il riconoscimento; cfr. L. TRUCCO, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, cit., 4 s. Nel caso descritto nel testo, il processo si fermerebbe ancor prima della autenticazione e, paradossalmente, non presupporrebbe necessariamente neppure la fase di attribuzione.

Viceversa, come chiarito dal Garante della *privacy* italiano, se si utilizzano solamente algoritmi di "*face detection*" e non di "*face recognition*", ossia di mero rilevamento del volto e non di identificazione della persona, senza che avvenga alcuna conservazione del *template* biometrico, allora non si rientra nell'ambito di applicazione delle regole sui dati biometrici, ma solo dei dati personali[61].

Se lo scopo, poi, è quello di operare categorizzazioni, ossia distinguere tra categorie di persone a partire da un aspetto specifico, senza però identificare l'interessato e cancellando subito le istanze biometriche costituite dai dati acquisiti e i modelli elaborati, allora in questo caso non si ricadrebbe nel regime dei dati biometrici, ma si rientrerebbe comunque all'interno delle categorie "particolari" di dati, nella misura in cui questi ultimi sono suscettibili di rivelare l'aspetto per il quale le persone vengono categorizzate, ossia l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona[62].

È in ragione della delicatezza delle operazioni in questione che il

[61] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria*, 21 dicembre 2017, con cui il Garante ha consentito la prosecuzione del trattamento dei dati da parte di un sistema di tipo "*digital signage*", che tramite una webcam si limita a effettuare la raccolta di dati audience per personalizzare l'offerta pubblicitaria e realizzare analisi di tipo statistico, operano una raccolta di dati a partire da tecniche di "*face detection*" che valutano l'età, il sesso, la risposta emozionale dello spettatore; visto che il sistema memorizza tali dati solo per una frazione di secondo, per poi sovrascriverli, e che non vi è modo di identificare lo spettatore, il Garante ha ritenuto sufficiente predisporre una informativa in forma semplificata, essendo impossibile acquisire il consenso. Ulteriormente, v. ID., *Verifica preliminare. Sistema di rilevazione delle immagini dotato di un software che permette il riconoscimento della persona (morfologia del volto)*, n. 155 del 15 marzo 2018, 2.2, ove si chiarisce che «nel caso del riconoscimento facciale, il presupposto perché il trattamento delle immagini possa essere qualificato come trattamento biometrico è che i confronti finalizzati al riconoscimento dell´individuo (verifica dell´identità, nel caso in esame) siano automatizzati mediante l´ausilio di appositi strumenti software o hardware (che non sussistono nel caso di specie».

[62] Art. 9, par. 1, del GDPR; art. 10 della LED. Sul punto, *mutatis mutandis*, si vedano le considerazioni contenute nell'*Explanatory Report* della Convenzione 108+ (punti 59 ss.).

d.lgs. n. 196/2003 incarica il Garante della *privacy* di adottare specifiche "misure di garanzia" per il trattamento dei dati biometrici, attraverso cui fissare le condizioni per il relativo trattamento, fra cui «le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, le misure di minimizzazione, le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a garantire i diritti degli interessati», con esplicito riferimento ai «dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati»[63].

Se le coordinate appena ricostruite potrebbero apparire piuttosto lineari nell'offrire un inquadramento giuridico del fenomeno, il caso delle TRF è paradigmatico delle difficoltà di questa normativa a regolare tecnologie all'avanguardia e in continua evoluzione come quelle che sfruttano IA.

Si pensi innanzitutto alla nozione fornita di "*dato biometrico*", che si espone a critiche in quanto troppo rigida. La costruzione di enormi *database* di immagini, infatti, non implica l'applicazione del regime sui dati biometrici, sebbene una vasta disponibilità di immagini, grazie anche – come visto in precedenza – all'ampia diffusione di TRF a basso costo e allo sviluppo di tecniche di *big data analytics* sempre più raffinate, consenta molto facilmente di operare una identificazione a partire da semplici fotografie digitali[64]. Si tratta di quel fenomeno che – più in generale – investe la stessa nozione di dato personale e ne assottiglia la distinzione rispetto al dato non personale, rendendo sfumata l'applicabilità della disciplina sulla protezione dei dati[65]. Anche per questi motivi la Corte di giustizia tende ad offrire una interpretazione

[63] Art. 2-*septies* del d.lgs. n. 196/2003. Attualmente non risulta che tali misure di sicurezza siano state adottate.

[64] E.J. KINDT, *Having yes, using no? About the new legal regime for biometric data*, in *The computer law and security report*, 34, 3, 2018, 530.

[65] Sul problema della *de-identification* del dato alla luce delle *big data analytics*, cfr. G. DE GREGORIO, R. TORINO, *Privacy, protezione dei dati personali e big data*, in E. TOSI (a cura di), *Privacy digitale*, cit., 472 ss. Sul punto, v. anche S. CALZOLAIO, *Protezione dei dati personali*, cit., 605 ss. Sulle tecniche di pseudonimizzazione e di anonimizzazione fini di sicurezza dei dati, ma anche a garanzia contro la de-identificazione, v. *infra* par. 5.3.

estensiva di dato personale[66], sebbene le tecnologie algoritmiche riescano continuamente a forzare le qualifiche formali impiegate dal diritto[67].

Già nel 2004 l'allora Presidente del Gruppo di lavoro "Articolo 29", Stefano Rodotà, metteva in guardia dal rischio che la videosorveglianza, grazie allo sviluppo di nuovi software, potesse tradursi «avventatamente in una sorveglianza dinamico-preventiva»[68]. Le TRF riescono oggi a ricavare le emozioni, i tratti caratteriali e gli aspetti della personalità a partire da una immagine facciale, contribuendo a stabilire profili personali, mappare le preferenze e ricostruire le abitudini di un individuo. La distinzione tra dato biometrico e non, quindi, tende a recedere innanzi ai modi con cui – secondo quanto chiarito[69] – i sistemi di IA sono in grado di "pensare", o meglio di originare automaticamente inferenze statistiche su una mole enorme di dati e ad una velocità quasi istantanea, con risultati non equiparabili – ma non per questo migliori – rispetto a quelli della mente umana.

Le TRF, con la loro capacità di captazione, pongono in crisi anche le nozioni di soggetto "*interessato*", i cui dati sono sottoposti a "*trat-*

[66] Si pensi a CGUE, C-582/14, *Breyer c. Bundesrepublik Deutschland*, 19 ottobre 2016, con cui è stata riconosciuta la qualifica di dato personale persino agli indirizzi IP dinamici registrati dal fornitore di servizi di *media online* in occasione della consultazione di siti internet pubblici; un dato che, a differenza degli indirizzi IP statici, non sarebbe di per sé immediatamente riconducibile alla persona che ha consultato il sito, in quanto provvisorio, assegnato ad ogni connessione e sostituito in caso di accessi successivi. Tuttavia, il fatto che il fornitore di *media* possa ottenere, a determinate condizioni, ulteriori informazioni a disposizione anche di altri soggetti, come il fornitore di accesso a internet, le quali consentono "indirettamente" di identificare l'utente che ha consultato detto sito internet, vale a qualificare tale dato come personale.

[67] Le tecniche di profilazione e di predizione hanno raggiunto un livello di efficienza tale che anche da dati meramente neutrali si possono ricavare dati pienamente "sensibili"; cfr. M. KOSINSKI, D. STILLWELL, T. GRAEPEL, *Private traits and attributes are predictable from digital records of human behavior*, in *PNAS*, 110, 15, 9 aprile 2013, 5802 ss., che dimostrano come siano sufficienti meno di 70 "*like*" di Facebook per determinare il colore della pelle dell'utente (con il 95% di precisione), l'orientamento sessuale (con l'88% di precisione), l'afferenza al partito politico (con il 95% di precisione).

[68] GRUPPO DI LAVORO ARTICOLO 29, *Parere 4/2004 relativo al trattamento dei dati personali mediante videosorveglianza*, WP89, 11 febbraio 2004, 4.

[69] V. *retro* Cap. II, par. 3.1.

tamento"[70]. Grazie alla crescente diffusione di queste tecnologie, infatti, il dato viene fatto continuamente oggetto di raccolta, trasformazione, circolazione. L'immagine di un volto può essere acquisita da un dispositivo, inserita in un *database*, conservata e resa disponibile per un numero indefinito di successivi riutilizzi, così che qualsiasi persona fisica, in qualunque momento, può diventare potenzialmente oggetto di trattamento e, perciò, interessata alla tutela dei propri dati, rendendo sempre più difficile ottenere tutela in base alla normativa in questione[71].

Ancora, questa disciplina è congegnata per proteggere il singolo interessato, ma non il *gruppo*, il quale non è riconosciuto come titolare del diritto alla protezione dei dati[72]. Eppure, come si vedrà meglio parlando delle tecniche di profilazione, i dati estratti con le TRF possono essere rielaborati tramite *big data analytics*, non trattando più il dato del singolo individuo, ma lavorando su *cluster* di dati in forma aggregata, allo scopo di ricavare categorie di persone non tanto a partire da elementi strutturali (come sesso, lingua, religione), quanto, con una "geometria variabile", partendo da preferenze di consumo, relazioni personali, stili di vita, o tempo trascorso *online*. Anche da questo punto di vista, sebbene questa dimensione di gruppo non sia del tutto estranea[73], la portata precettiva della normativa in questione rischia di dimostrarsi troppo limitata, tanto che le autorità di controllo hanno espresso precise preoccupazioni al riguardo[74].

[70] Art. 1, par. 1, del GDPR.

[71] Come rilevato in generale da F. PIZZETTI, *La protezione dei dati personali e le sfide dell'Intelligenza Artificiale*, cit., 40 ss.

[72] Più ampiamente, v. A. MANTELERO, *Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection*, in *Computer Law & Security Review*, 32, 2, 2016, 238 ss.; L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy: New Challenges of Data Technologies*, Springer, Dordrecht, 2017.

[73] Come chiarito in GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 6 febbraio 2018, 8, la profilazione consiste «nella raccolta di informazioni su una persona (o un gruppo di persone) e nella valutazione delle loro caratteristiche o dei loro modelli di comportamento al fine di includerli in una determinata categoria o gruppo, in particolare per analizzare e/o fare previsioni, ad esempio, in merito a: capacità di eseguire un compito; interessi, o comportamento probabile». V. *infra* par. 6.4.

[74] Cfr. 40TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY

In generale, dunque, si può osservare già fin dalle prime battute come la disciplina in questione, pur con tutte le sue novità rispetto al passato, offra un crinale piuttosto stretto su cui muoversi, esposta com'è al rischio che le TRF sfuggano alla sua regolazione; una condizione destinata a ripercuotersi nel regime in cui essa si specifica.

4. *La difficile ricerca di un solido fondamento giuridico per il trattamento dei dati*

4.1. *Un consenso al riconoscimento facciale sempre più inconsapevole*

Principio cardine per la tutela dei dati personali è che il trattamento avvenga in maniera "*lecita*"[75]. La normativa individua una serie di condizioni di liceità che offrono la sintesi del bilanciamento tra gli interessi in gioco che ruotano attorno ai dati personali[76]. Per stabilire le condizioni di liceità del trattamento applicabili alle TRF occorre tenere innanzitutto in considerazione la distinzione operata sopra tra dati biometrici e non.

Come anticipato, le ipotesi in cui le TRF trattino dati qualificati come non biometrici sono limitate alle sole autenticazioni anonime, in cui il sistema non identifica il soggetto e neppure ne conserva i *template* biometrici. In questi casi troverebbero applicazione i requisiti generali di liceità posti generalmente per il trattamento dei meri dati perso-

COMMISSIONERS, *Declaration on Ethics and Data Protection in Artifical Intelligence,* Bruxelles, 23 ottobre 2018, 3, ove, in generale con riguardo alle nuove tecnologie, si legge che il principio di correttezza debba essere perseguito anche «taking into consideration not only the impact that the use of artificial intelligence may have on the individual, but also the collective impact on groups and on society at large».

[75] Art. 5, par. 1, lett. a, del GDPR; art. 4, par. 1, lett. a, della LED. Principio disposto anche dall'art. 5, par. 1, lett. a, della Convenzione 108.

[76] Un bilanciamento che, ad esempio, contempera la tutela della *privacy* e del dato personale con i diritti di libertà di manifestazione del pensiero, di espressione e di informazione, nonché la libertà di impresa e, funzionalmente, di libera circolazione dei dati; cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, cit., 111 s.

nali[77]. Nella maggior parte dei casi, invece, si applicano le regole sui dati biometrici, rientranti nella categoria dei dati "particolari" assistiti da maggiori cautele.

Allorché si tratti di perseguire interessi non di natura pubblicistica, come accade, ad esempio, nelle attività commerciali delle imprese private, si rientra nell'ambito delle regole poste dal GDPR, il quale, in linea con la Convenzione 108, impone come regola un divieto generale di trattamento di dati biometrici, salvo ricadere nelle ipotesi eccezionali successivamente elencate[78]. Ai fini del presente discorso, la situazione che assume maggior

[77] Nel GDPR il più calzante dei requisiti rispetto alle tecnologie in parola è che l'interessato abbia prestato il proprio consenso al trattamento, o che il trattamento sia necessario «per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri» (art. 6, par. 1, lett. a, e). Nella seconda ipotesi, in attuazione, v. l'art. 2-*ter*, d.lgs. n. 196/2003. A commento, v. M. MIDIRI, S. PIVA, *L'interesse pubblico come base giuridica e come finalità del trattamento dei dati personali*, in S. SCAGLIARINI (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali*, cit., 26 ss.

Ancor più residuali sono le ipotesi in cui troverebbero applicazione le regole della LED all'art. 8, par. 2, ovvero, da una parte, la "necessità" del trattamento ai fini della prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali e, dall'altra, la disciplina da parte del diritto dell'UE o degli Stati. Il successivo par. 2 demanda al diritto degli Stati il compito di disciplinare il trattamento specificando «quanto meno gli obiettivi del trattamento, i dati personali da trattare e le finalità del trattamento». Conseguentemente l'art. 5, c. 2, del d.lgs. n. 51/2018, incarica un regolamento, da adottare ai sensi dell'art. 17, c. 1, della legge 23 agosto 1988, n. 400, di individuare i termini, ove non già altrove stabiliti, e le modalità di conservazione dei dati, i soggetti legittimati ad accedervi, le condizioni di accesso, le modalità di consultazione, nonché le modalità e le condizioni per l'esercizio dei diritti di informazione, accesso, e gli accertamenti che possono essere richiesti al Garante.

[78] L'art. 9, par. 2, stabilisce che il trattamento è lecito, fra l'altro, per assolvere obblighi o esercitare diritti in ambito lavorativo e previdenziale (b); qualora sia necessario tutelare un interesse vitale quando non sia possibile prestare il consenso (c); per il raggiungimento delle finalità di legittime attività di fondazioni, associazioni o altri organismi senza scopo di lucro (d); qualora i dati personali particolari siano resi manifestamente pubblici dall'interessato (e); per lo svolgimento di attività difensive ed investigative (e); per un interesse pubblico rilevante nel settore della sanità pubblica (i); per scopi di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (J), salvo le possibili deroghe e adeguamenti introdotti dagli Stati membri (art. 89, par. 2). Per la relativa casistica applicativa v. G. DRUETTA, 9. *Trattamento di categorie particolari di dati personali*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Wolkers Kluwer, Milano, 2018, 93 ss.

rilievo è la necessità di ottenere un "*consenso esplicito*" al trattamento automatizzato delle proprie immagini in relazione ad una o più finalità definite[79]. Il termine "esplicito" si riferisce al modo in cui il consenso è espresso dall'interessato e significa che l'interessato debba fornire una dichiarazione esplicita di consenso, a fronte di circostanze nelle quali emergono gravi rischi per la protezione dei dati e, quindi, si ritiene necessario elevare il livello di controllo individuale su di essi[80]. A riprova di questa stretta, l'interessato può revocare il proprio consenso in qualsiasi momento con la stessa facilità con cui è stato accordato[81].

Per comprendere la "sensibilità" di questo requisito, si consideri la reazione suscitata dal servizio introdotto da Facebook nel 2010, che consentiva alla piattaforma, sfruttando appunto tecniche di riconoscimento facciale, di suggerire automaticamente ad un utente che pubblicava le immagini sul *social network* di "taggare" – ovvero associare con le relative generalità e tutte le informazioni pubblicate nel rispettivo profilo personale – le persone in esse ritratte, qualora queste fossero già state identificate dall'utente stesso. Benché questa forma di identificazione consistesse in un mero suggerimento offerto dal sistema a seguito della condivisione delle immagini[82], tale innovazione è stata cen-

A proposito delle categorie speciali di dati, la Convenzione 108 impone un generale divieto di trattamento, «a meno che il diritto interno preveda delle garanzie appropriate» (art. 6).

[79] Art. 9, par. 2, lett. a, del GDPR. La Convenzione 108+ stabilisce, nella nuova versione dell'art. 6, che per il trattamento dei dati biometrici occorrono appropriate misure di salvaguardia stabilite dalla legge, che mettano al riparo dai rischi nei confronti degli interessi, diritti e libertà fondamentali del titolare dei dati, specialmente contro le discriminazioni. L'*Explanatory Report* esemplifica tali misure, citando, per l'appunto, il consenso esplicito, una legge che stabilisca lo scopo e i mezzi del trattamento, comprese le eccezioni al divieto di trattamento, le misure conseguenti ad una analisi del rischio, misure tecniche e organizzative (p. 56).

[80] GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, 10 aprile 2018, 20.

[81] Così in base all'art. 7, par. 3, del GDPR.

[82] Ciò non toglie che, in ipotesi estreme, anche solo il mero suggerimento possa avere conseguenze pericolose, come avviene nei regimi totalitari ove si torturano i dissidenti per avere accesso ai loro profili Facebook; cfr. A. BLOMFIELD, *Syria 'tortures activists to access their Facebook pages'*, in *The Telegraph*, 9 maggio 2011 [bit.ly/3mrIjJo].

surata nell'agosto 2011 dal Commissario per la protezione dei dati e la libertà di informazione di Amburgo, sul presupposto che violasse la direttiva 95/46/CE e la legislazione tedesca attuativa, a causa della mancanza della richiesta di un consenso esplicito preventivo degli utenti per l'attivazione di questa opzione, invece che della sola possibilità di disabilitarla *ex post*[83]. Sulla scorta di questa iniziativa, l'*Irish Office of the Data Protection Commissioner* ha sottoposto Facebook ad una procedura di *audit*, formulando una serie di raccomandazioni alcune delle quali riguardanti il riconoscimento facciale e la necessità di richiedere il consenso esplicito[84]. In risposta, Facebook ha adottato una serie di misure, fra le quali consentire agli utenti di cancellare i *template* biometrici raccolti in precedenza, ed ha sospeso tale servizio in ambito europeo[85].

Nonostante gli accorgimenti tesi a rafforzare il controllo sui propri dati, occorre tuttavia chiarire come il regime così previso non paia affatto idoneo a qualificare il consenso come una base giuridica sufficiente ed efficace a fronte della capacità invasiva delle TRF sui diritti fondamentali in gioco, quando queste vengono impiegate a fini di verificazione, ma soprattutto di identificazione e categorizzazione.

I maggiori problemi circa il consenso personale sorgono per i *sistemi passivi* di riconoscimento facciale, ove la raccolta dei dati può prescindere dalla percezione o consapevolezza dell'interessato. Ad esempio, l'ingresso in una zona videosorvegliata non può integrare *sic et simpliciter* una dichiarazione o una chiara azione affermativa equivalente ad un consenso esplicito[86]. Ne consegue come i dispositivi di ri-

[83] Cfr. Y. WELINDER, *Face Recognition Privacy in Social Networks under German Law*, in *Communications Law Bulletin*, 31, 1, 2012, 5 ss.

[84] Cfr. DATA PROTECTION COMMISSIONER, *Facebook Ireland Ltd. Report of Audit*, 21 dicembre 2011,14. Sul punto si è espresso di lì a poco anche il Gruppo "Articolo 29" nel medesimo senso; cfr ARTICLE 29 WORKING PARTY, *Opinion 02/2012 on facial recognition in online and mobile services*, WP 192, 22 marzo 2012, p. 4.5.

[85] Cfr. [bit.ly/3t2CzZo].

[86] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 15. Il mero ingresso può costituire espressione di un consenso esplicito se vengono rispettate le condizioni indicate all'art. 9, come anche specificate in GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, cit., 20 ss.

levamento debbano poter essere attivati intenzionalmente dall'interessato[87], o che le aree dove viene impiegato un sistema di TRF debbano essere tenute ben separate dalle altre[88], e ancora che debbano essere offerte vie alternative per l'accesso ai rispettivi luoghi; sebbene nei fatti ciò sia tecnicamente e organizzativamente difficile da garantire[89]. In assenza di queste condizioni, o qualora le alternative fossero troppo onerose per l'interessato, occorrerebbe riflettere sull'opportunità di impiegare tali sistemi[90].

Una delle vicende più recenti che hanno attirato maggiori preoccupazioni e suscitato consapevolezza per la capacità intrusiva di queste tecnologie è quella legata all'uso di TRF nell'area di "King's Cross" al centro di Londra[91]. Nell'agosto del 2019 ne è scaturita una indagine da parte dell'*Information Commissioner's Office* del Regno Unito[92], in ragione dell'enorme volume di persone sottoposte a sorveglianza tra il maggio 2016 e il maggio 2018, senza alcun consenso da parte loro.

Tuttavia, anche nei *sistemi interattivi*, ove dovrebbe esservi una partecipazione consapevole dell'interessato durante la raccolta del dato biometrico, possono sorgere questioni sulla bontà del consenso prestato. Quest'ultimo deve sempre intendersi come una «intenzione libe-

[87] Come dovrebbe avvenire nei controlli all'accesso di edifici, offrendo a coloro che non abbiano prestato il consenso esplicito la possibilità di usufruire di vie di accesso alternative; cfr. COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 20.

[88] Evitando così che vengano acquisite le immagini anche di coloro che non abbiano prestato il proprio consenso, come avviene ad esempio presso i terminali aeroportuali; *ivi*, 20.

[89] Con riguardo al "*Customs and Border Protection Biometric Exit Program*" in vigore negli aeroporti degli Stati Uniti, cfr. A. FUNK, *I Opted Out of Facial Recognition at the Airport–It Wasn't Easy*, in *Wired*, 2 luglio 2019 [bit.ly/3dH29N5]. In Europa, v. CNIL, *Reconnaissance faciale dans les aéroports: quels enjeux et quels grands principes à respecter ?*, 9 ottobre 2020.

[90] CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on Facial Recognition*, cit., 7.

[91] Cfr. D. SEBBAGH, *Facial recognition technology scrapped at King's Cross site*, in *The Guardian*, 2 settembre 2019 [bit.ly/3sUkRqK].

[92] ICO, *Statement: Live facial recognition technology in King's Cross*, 15 agosto 2019 [bit.ly/31TP2m5].

ra, specifica, informata e inequivocabile» di accettazione[93], con una valutazione da operare caso per caso.

Si pensi, ad esempio, alla condizione dei lavoratori dipendenti cui venga richiesto di sottoporsi a videosorveglianza tramite TRF[94]. Al di là dei divieti specifici previsti dalla legislazione italiana[95], i lavoratori

[93] Art. 4, par. 1, n. 11, del GDPR. Per ulteriori specificazioni, v. GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, cit., 6 ss. In base alla Convenzione 108+, la nuova versione dell'art. 5, par. 2, chiede ora un consenso "libero, specifico, informato e non ambiguo".

[94] Si consideri che tra le eccezioni al divieto di trattamento dei dati sensibili previste dal GDPR vi è anche la necessità di «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» (art. 9, par. 2, lett. b). L'art. 88 del GDPR, inoltre, rimette alla legge o alla contrattazione collettiva la possibilità di stabilire «norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro», per le finalità indicate dal regolamento. Ha fatto seguito il nuovo art. 111 del d.lgs. n. 196/2003, che in attuazione favorisce l'adozione di «regole deontologiche». Più in generale, anche per un richiamo alle autorizzazioni generali del Garante italiano ancora in vigore, v. A. MARESCA, S. CIUCCIOVINO, I. ALVINO, *Regolamento UE 2016/679 e rapporto di lavoro*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, cit., 311 ss.; C. DEL FEDERICO, *Il trattamento dei dati nell'ambito dei rapporti di lavoro*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, cit., 895 ss.; M.C. DEGOLI, *I trattamenti in ambito lavorativo*, in S. SCAGLIARINI (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali*, cit., 243 ss. In aggiunta, la disciplina sul trattamento dei dati dei lavoratori va letta in combinato disposto con le recenti modifiche sui sistemi di controllo di cui allo Statuto dei lavoratori, come novellato dal d.lgs. n. 151/2015 e poi integrato dal d.lgs. n. 185/2016, che prevede adesso, più in generale, che le informazioni raccolte ai fini di controllo, come le videoregistrazioni, «sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli» e nel rispetto del Codice della privacy (art. 4, c. 3); sui risvolti nella tutela dei dati personali, v. anche L. CALIFANO, *Tecnologie di controllo del lavoro, diritto alla riservatezza e orientamenti del Garante per la protezione dei dati personali*, in P. TULLINI (a cura di), *Controlli a distanza e tutela dei dati del lavoratore*, cit., 165 ss.

[95] V. *retro* Cap. II, par. 8.

subordinati, trovandosi in una posizione di debolezza nei confronti del datore di lavoro, si ritiene possano manifestare il loro consenso liberamente soltanto in casi eccezionali, quando non subiranno alcuna ripercussione negativa per il fatto che esprimano un eventuale rifiuto[96].

In una situazione di soggezione per certi versi analoga si trovano anche i minori[97], per i quali vi è una disciplina specifica quanto al consenso in relazione ai servizi della società dell'informazione[98], ma soprattutto per il trattamento dei dati sensibili nell'ambito dell'istruzione[99]. Si pensi infatti alla condizione dei minori che frequentano istituti scolastici, come insegna la vicenda della sperimentazione di TRF a scopo di controlli di sicurezza all'interno di alcune scuole superiori francesi. Il suo epilogo – oltre che segnato dalla censura da parte della CNIL, come si vedrà a breve[100] – è stato un contezioso giurisdizionale in esito al quale il *Tribunal administratif de Marseille*, con sentenza del 27 febbraio 2020, ha annullato la deliberazione del Consiglio della *Provence-Alpes-Côte d'Azur* che aveva autorizzato tale sperimentazione, sul presupposto che non sia sufficiente firmare un modulo per aver consapevolezza della portata di tali tecnologie, o

[96] GRUPPO DI LAVORO ARTICOLO 29, *Parere 2/2017 sul trattamento dei dati sul lavoro*, WP 249, 8 giugno 2017, 26.

[97] V. *retro* Cap. II, par. 8.

[98] In base all'art. 8 del GDPR, nelle ipotesi in cui il trattamento di basa sul consenso per quanto riguarda l'offerta diretta di servizi della società dell'informazione, occorre che il minore abbia almeno 16 anni; al di sotto di questa età, occorre che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale. L'art. 2-*quinquies* del d.lgs. n. 196/2003, secondo quanto consentito dal regolamento, ha abbassato tale soglia a 14 anni. Più in generale sul punto, v. A. ASTONE, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, GFL, Milano, 2019, 25 ss.; F. SCIA, *Diritti dei minori e responsabilità dei genitori nell'era digitale*, ESI, Napoli, 2020, 23 ss.

[99] Aspetto per il quale si rinvia, anche in ragione delle specifiche previsioni all'art. 96 del d.lgs. n. 196/2003 (Trattamento di dati relativi a studenti), a C. DEL FEDERICO, *Il trattamento dei dati personali relativi all'istruzione*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, cit., 873 ss. Nell'ambito dell'istruzione, peraltro, potrebbe invocarsi anche il differente fondamento giuridico dell'"interesse pubblico rilevante", come si vedrà a breve.

[100] V. *infra* par. 4.3.

che il consenso così prestato sia effettivamente libero e consapevole[101]. Ad analoghe conclusioni è giunta l'Autorità di protezione dei dati svedese in un caso molto simile[102].

Più in generale, tuttavia, l'impatto delle TRF è tale da porre in crisi il principio del "*notice and consent*" tradizionalmente alla base della protezione dei dati personali[103].

Come detto introduttivamente, queste forme innovative di sorveglianza sono talmente ubiquitarie e integrate – basti pensare a quanto avviene in ambienti come le *smart cities* – da poter catturare sistematicamente le immagini senza la piena consapevolezza degli interessati.

In termini di effettività, inoltre, queste tecnologie radicalizzano alcuni limiti ben noti del meccanismo del consenso. Innanzitutto, cresce esponenzialmente il pericolo che il consenso a sottoporsi ad un trattamento venga reso come un automatismo[104]. È difficile, in generale, che

[101] Cfr. Tribunal administratif de Marseille, sent. 27 febbraio 2020, n. 1901249, ove si legge: «*ce consentement serait recueilli par la seule signature d'un formulaire, alors que le public visé se trouve dans une relation d'autorité à l'égard des responsables des établissements publics d'enseignement concernés, la région ne justifie pas avoir prévue des garanties suffisantes afin d'obtenir des lycéens ou de leurs représentants légaux qu'ils donnent leur consentement à la collecte de leurs données personnelles de manière libre et éclairée*» (p. 12). Suscita perplessità il fatto che si sia scelta come base giuridica il consenso esplicito all'art. 9, par. 2, lett. a, del GDOR, e non le condizioni per i motivi di interesse pubblico rilevante alla successiva lett. g, su cui v. *infra* il prossimo par.

[102] Cfr. SWEDISH DATA PROTECTION AUTHORITY (*Integritetsskydds myndigheten*), *Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students*, DI-2019-2221, 20 agosto 2019, con riguardo all'utilizzo di queste tecnologie presso la "Skellefteå Municipality, Secondary Education Board".

[103] L. MITROU, *Data Protection, Artificial Intelligence and Cognitive Services. Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?*, in *SSRN*, dicembre 2018, 36 s.; V. MAYER-SCHÖNBERGER, Y. PADOVA, *Regime Change? Enabling Big Data through Europe's New Data Protection Regulation*, in *The Columbia Science & Technology Law Review*, 17, 2016, 332; C. MUNDIE, *Privacy Pragmatism: Focus on Data Use, Not on Data Collection*, in *Foreign Affairs*, 94, 2, 2014, 28 ss.; A. MANTELERO, *The Future of Consumer Data Protection in the E.U. Rethinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics*, in *Computer Law and Security Review*, 30, 2014, 643 ss.

[104] M.L. JONES, E. KAUFMAN, E. EDENBERG, *AI and the Ethics of Automating Consent*, in *IEEE Security & Privacy*, 16, 3, 2018, 64 ss.

le persone leggano attentamente e valutino razionalmente l'informativa sul consenso per poi decidere in piena consapevolezza sulle conseguenze circa la *privacy* e i propri dati personali[105]. Spesso l'informativa è formulata in termini troppo complessi, tramite un linguaggio giuridico non sempre accessibile alla generalità degli utenti o dei consumatori[106]. Tanto più ciò accade quando i dati sono destinati ad essere processati con tecnologie avanzate, il cui funzionamento può risultare il più delle volte incomprensibile agli interessati. Questa difficoltà di comprensione, tuttavia, non è riservata solamente al comune cittadino, ma può essere connaturata alle specificità delle tecnologiche impiegate, come avviene nel caso di *big data analytics* e *machine learning* che – come visto[107] – non impiegano procedimenti logici, ma inferenze statistiche difficilmente ricostruibili dagli stessi programmatori. Sono tutti fattori che incrementano l'asimmetria nel potere informativo dei soggetti coinvolti nei processi di trattamento dei dati e di riconoscimento facciale, a discapito di un effettivo bilanciamento con la propria libertà di autodeterminazione[108].

Un approccio imperniato prevalentemente sul consenso, inoltre, valorizza sì l'autodeterminazione personale e la libertà di scelta consapevole, ma al fondo disvela una concezione di tutela della *privacy* e dei dati personali che rischia di sovraccaricare ideologicamente le nozioni di "controllo" o "autonomia", trascurando il contesto concreto entro cui il consenso viene prestato o l'assenza di alternative effettive. La conseguenza è che si abbandonano ai rapporti di forza – non da ultimo, economici – situazioni che invece dovrebbero ricevere maggiore

[105] E. CAROLAN, *The continuing problems with online consent under the EU's emerging data protection principles*, in *Computer Law & Security Review*, 32, 3, 2016, 462 ss.; M. BUTTERWORTH, *The ICO and artificial intelligence: The role of fairness in the GDPR framework*, in *Computer Law and Security Review,* 34, 2018, 262. Di "consenso consapevolmente disinformato" parla C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Dir. pubb. comp. eur.*, f.s., 2019, 107 ss.

[106] J.R. REIDENBERG ET AL., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, in *I/S: A Journal of Law and Policy for the Information Society*, 11, 2, 2015, 485 ss.

[107] V. *retro* Cap. I, par 3.2.

[108] L. MITROU, *Data Protection, Artificial Intelligence and Cognitive Services. Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?*, cit., 41.

tutela a livello giuridico[109]. Una riprova esasperata di queste situazioni si ha nella pratica di collezionare immagini di volti di persone vulnerabili o in posizioni economiche e sociali di svantaggio allo scopo di migliorare i meccanismi di riconoscimento facciale[110].

Da qui le proposte di regolazione – fiorite soprattutto negli Stati Uniti, ove manca una legislazione sui dati personali analoga a quella europea – non incentrate solamente sul meccanismo del consenso, ma dirette, ad esempio, a regolare con legge ed *ex post* i possibili usi e abusi dei dati personali, permettendo o vietando non solo quelli – allo stato – illegittimi, ma anche eticamente inaccettabili[111], oppure rafforzando il potere di controllo e di sfruttamento economico dei dati da parte dei titolari[112]. Si tratta comunque di tentativi che testimoniano la necessità di un cambiamento di paradigma e l'esigenza di trovare un «fondamento legittimo previsto dalla legge» – per usare la terminolo-

[109] Cfr. J.E. COHEN, *Examined Lives: Informational Privacy and the Subject as Object*, in *Stanford Law Review*, 52, 5, 2000, 1399 ss., a proposito di quell'approccio che viene definito "*privacy-as-choice*". Ma v. anche le considerazioni di S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, cit., 599, secondo cui «il diritto all'autodeterminazione informativa [...] non è ricostruibile in una dimensione puramente negoziale. E i limiti al potere negoziale dell'interessato, che possono configurare anche situazioni di indisponibilità, ben si spiegano con il fatto che qui ci troviamo propriamente in un quadro complessivo di definizione e tutela di liberta fondamentali della persona». Ulteriori considerazioni in ID., *Tecnologie e diritti*, cit., 82. Si osserva in S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Rivista di Diritto Civile*, 6, 2001, 632 s., come però occorra rifuggire da visioni estremistiche che negano del tutto la valenza economica e alla possibile circolazione contrattuale dell'informazione.

[110] I.A. HAMILTON, *Google suspended facial recognition research for the Pixel 4 smartphone after reportedly targeting homeless black people*, in *Business Insider*, 17 ottobre 2019 [bit.ly/3rXCBQA].

[111] Cfr. C. MUNDIE, *Privacy Pragmatism: Focus on Data Use, Not on Data Collection*, cit., 28 ss.; V. MAYER-SCHÖNBERGER, Y. PADOVA, *Regime Change? Enabling Big Data through Europe's New Data Protection Regulation*, cit., 332.

[112] Si pensi, ad esempio, alla strategia "*sharing the wealth*" proposta in O. TENE, J. POLONETSKY, *Big Data for All: Privacy and User Control in the Age of Analytics*, in *Northwestern Journal of Technology and Intellectual Property*, 11, 5, 2013, 239 ss., che consiste nel consentire ai singoli di accedere ai propri dati, in analogia al nuovo diritto alla portabilità all'art. 20 del GDPR, e fruttare applicazioni che permettano di analizzare i propri dati e trarre conclusioni utili.

gia dell'art. 8 della CDFUE – che sia diverso dal mero consenso, sempre più inefficace al cospetto di tecnologie come quelle di riconoscimento facciale[113].

4.2. *Il riconoscimento facciale in presenza di "interessi pubblici rilevanti"*

Diversa è la disciplina che si applica alle TRF quando il trattamento dei dati biometrici avviene per scopi di *interesse pubblico*. Vi sono situazioni in cui queste tecnologie vengono impiegate, ad esempio, per l'identificazione entro spazi pubblici o per il perseguimento di reati in cui occorrere necessariamente prescindere dal consenso. Quest'ultimo, inoltre, non potrebbe il più delle volte essere legittimamente invocato in ragione dello squilibrio fra privati e autorità pubbliche[114].

Si tratta di utilizzi consentiti dal GDPR, a patto che il trattamento rispetti una serie condizioni: quanto alla finalità, che esso sia «necessario per motivi di interesse pubblico rilevante» e che sia «proporzionato alla finalità perseguita»; quanto al fondamento giuridico, che esso sia individuato sulla base «del diritto» dell'UE o degli Stati; quanto alle garanzie offerte, che esso debba «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»[115].

[113] Sull'insufficienza del meccanismo del consenso a livello europeo, v. A. MANTELERO, *The Future of Consumer Data Protection in the E.U. Rethinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics*, cit., 643 ss., per una valorizzazione del ruolo di controllo dei Garanti, dell'analisi di impatto obbligatoria, della trasparenza e del design dei sistemi, del divieto di re-identificazione dei dati resi anonimi, di revoca del consenso.

[114] CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on Facial Recognition*, cit., 6.

[115] Così l'art. 9, lett. 2, par. g, del GDPR. In attuazione, l'art. 2-*sexies*, d.lgs. n. 196/2003, specifica che il fondamento giuridico a livello nazionale sia offerto da disposizioni di legge o di regolamento, ove previsto a livello legislativo, le quali specifichino «i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato» (c. 1). Vengono espressamente considerati "motivi di interesse pubblico rilevante" (c. 2) trattamenti – per quanto qui rileva maggiormente – nelle materie di: cittadinanza, immigrazione, asilo, condizione

In termini parzialmente analoghi viene disposto anche dalla LED, con riferimento alle specifiche finalità di prevenzione e repressione di reati[116]. In questo caso, in linea con la giurisprudenza della Corte di giustizia[117], si autorizza il trattamento di dati biometrici purché ciò sia «strettamente necessario», da intendersi come presenza di giustificazioni precise e particolarmente solide per il trattamento di tali dati[118]; che sia «autorizzato dal diritto» dell'UE o degli Stati; che sia «soggetto a garanzie adeguate per i diritti e le libertà dell'interessato»[119]. Sebbene, sul punto, il GDPR parli di mera «necessità» e non di «stretta necessità», e che ai sensi della LED il consenso non possa costituire una base giuridica per il trattamento[120], la direttiva pone comunque requisiti meno stringenti[121]. Si pensi che la LED fa riferimento ad una generica "adeguatezza" delle garanzie da disporre a tutela dell'interessato; ma, soprattutto, che la direttiva rimette alla disciplina attuativa degli

dello straniero e del profugo, stato di rifugiato (lett. e); attività di controllo e ispettive (lett. l); attività sanzionatorie e di tutela in sede amministrativa o giudiziaria (lett. q). Il trattamento dei dati biometrici deve avvenire comunque nel rispetto delle misure di garanzia disposte dal Garante (c. 3).

[116] Così l'art. 10 della LED.

[117] Cfr. CGUE, C-293-12 e C-594/12, *Digital Rights Ireland v. Minister for Communications e.a.*, 8 aprile 2014, p. 52; CGUE, C-362/14, *Maximillian Schrems*, cit., p. 92.

[118] Così GRUPPO DI LAVORO ARTICOLO 29, *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, WP 258, 29 novembre 2017, 7 s.

[119] Esemplificativamente il cons. 37 indica: la possibilità di raccogliere tali dati unicamente in connessione con altri dati relativi alla persona fisica interessata, la possibilità di provvedere adeguatamente alla sicurezza dei dati raccolti, norme più severe riguardo all'accesso ai dati da parte del personale dell'autorità competente e il divieto di trasmissione di tali dati. In aggiunta, è possibile prevedere ulteriori misure, come la limitazione a determinate categorie di reato o, in caso di misure preventive, una certa urgenza (ad esempio pericolo imminente con conseguenze probabilmente gravi per l'interesse vitale di molte persone), oppure l'autorizzazione preliminare di un giudice; cfr. GRUPPO DI LAVORO ARTICOLO 29, *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, cit., 8. L'art. 7 del d.lgs. n. 51/2018 si limita per lo più a ribadire i contenuti della direttiva.

[120] Aspetti sottolineati *ivi*, 7 ss.

[121]. Anche la Raccomandazione n. R(87) 15, al principio 2.4, parla di "assoluta necessità" del trattamento.

Stati membri, e quindi potenzialmente alle forze dell'ordine, un ampio margine di azione[122].

A riprova di questa ampiezza e delle incertezze che possono derivare a livello nazionale, inoltre, basti pensare che il d.P.R. n. 15/2018, attuativo del d.lgs. n. 51/2018, prevede molto genericamente che il trattamento di dati "sensibili", fra cui quelli biometrici, è consentito «quando è necessario per le esigenze di un'attività informativa, di sicurezza o di indagine di polizia giudiziaria o di tutela dell'ordine e della sicurezza ad integrazione di altri dati personali»[123]. Disposizioni simili necessitano di una interpretazione restrittiva per essere raccordate con le previsioni europee citate sopra.

Di contro, la normativa attuativa italiana circonda il trattamento dei dati personali per finalità di polizia di alcune cautele allorché si abbia riguardo a sistemi di sorveglianza e di ripresa video o fotografica, pur differenti rispetto alle TRF. Tale disciplina, sebbene non in linea con le novità arrecate dalla LED, limita l'impiego di tali sistemi, nel primo caso, ove «necessario» per le finalità sopra indicate e ove «non comporti un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali delle persone interessate», dovendosi registrare «esclusivamente le immagini indispensabili»; nel secondo caso, le riprese sono consentite, in termini piuttosto ampi, per finalità di sicurezza pubblica, prevenzione e repressione di reati[124].

La LED, inoltre, accompagna la definizione dei requisiti citati con la necessità, più in generale, di operare una distinzione tra le categorie di interessati al trattamento in relazione alla qualifica acquisita durante il procedimento penale[125], in accordo anche con gli indirizzi formulati

[122] T. MARQUENIE, *The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework*, cit., 332.

[123] Art. 11, c. 2, del d.P.R. n. 15/2018.

[124] Rispettivamente, art. 22 e art. 23 d.P.R. n. 15/2018. Quest'ultimo indica che le riprese sono consentite ove necessario per documentare: una specifica attività preventiva o repressiva di fatti di reato, situazioni dalle quali possano derivare minacce per l'ordine e la sicurezza pubblica o un pericolo per la vita e l'incolumità dell'operatore, o specifiche attività poste in essere durante il servizio che siano espressione di poteri autoritativi degli organi, uffici e comandi di polizia» (c. 2).

[125] A questo proposito, l'art. 6 della LED stabilisce che gli Stati membri dispongano che il titolare del trattamento, «se del caso e nella misura del possibile», operi

dalla Corte di giustizia[126]. A questa distinzione enunciata in termini di massima, tuttavia, non fa seguito una disciplina propriamente modellata su di essa, con la conseguenza che non vi sono condizioni da rispettare per il trattamento dei dati in relazione ai diversi soggetti, i quali si trovano ad essere trattati indistintamente allo stesso modo[127].

La normativa applicabile alle TRF in presenza di "interessi pubblici rilevanti" presenta, infine, un aspetto di immediato interesse anche per quanto detto a proposito della tutela dell'anonimato nello spazio pubblico[128]. Si tratta, in particolare, del riferimento alla possibilità di prescindere dalla previsione legislativa a disciplina del trattamento per fini di polizia, nel caso in cui questo avvenga perché i dati sono stati «resi manifestamente pubblici dall'interessato»[129]. Come messo in luce

una chiara distinzione tra i dati personali delle diverse categorie di interessati, quali: le persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato; le persone condannate per un reato; le vittime di reato; le altre parti rispetto a un reato (testimoni, informati sui fatti, le persone collegate ai soggetti citati sopra). Osserva P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, cit., 338, come questa distinzione sia espressione della garanzia di evitare una conservazione indifferenziata di informazioni ed un trattamento generalizzato in ambito penalistico, i quali sarebbero in contrasto con i principi di necessità, pertinenza e proporzionalità, oltre che a detrimento della presunzione di non colpevolezza.

[126] In varie occasioni la CGUE ha avuto modo di ribadire come occorra effettuare una distinzione tra le categorie di dati oggetto di conservazione, e più in generale di trattamento, a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate; cfr. C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 63; CGUE, C-362/14, *Maximillian Schrems* cit., p. 93. Con riguardo all'accesso ai dati delle comunicazioni, sulla necessaria «differenziazione, limitazione o eccezione in funzione dell'obiettivo perseguito», v. CGUE, C-203/15 e C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* e *Secretary of State for the Home Department v. Tom Watson e a.*, 21 dicembre 2016, p. 105.

[127] Di eccessiva cautela dovuta al carattere meramente eventuale di questa distinzione e alla rimessione alla volontà degli Stati parla T. MARQUENIE, *The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework*, cit., 331. Osserva P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, cit., 339, inoltre, come sarebbe stato necessario definire una disciplina differenziata quanto ai soggetti non sospettati, limiti alle condizioni di raccolta, tempi di conservazione, soggetti legittimati all'accesso e finalità di utilizzo.

[128] V. *retro* Cap. II, par. 6.

[129] Art. 10, par. 1, lett. c, della LED.

in più occasioni anche dalla Corte EDU, se le attività svolte in pubblico implicano un contemperamento nella pretesa di tutela della *privacy*, la raccolta e la conservazione di dati di persone sottoposte a sorveglianza costituisce comunque un'ingerenza nella loro vita privata, anche se raccolti in luoghi pubblici, qualora essa avvenga, ad esempio, in maniera sistematica o vi sia una registrazione permanente dei dati[130]. Una videoripresa che avvenga in un luogo pubblico, quindi, potrebbe rientrare in tale ipotesi solamente in seguito ad una valutazione attenta, dalla quale emerga che «l'interessato abbia volontariamente rinunciato alla protezione speciale per i dati sensibili rendendoli disponibili al pubblico, autorità comprese»[131]. Il fatto di camminare per strada, dunque, non legittima di per sé le forze di polizia a raccogliere le immagini dei passanti. Considerazioni in parte analoghe, però, valgono anche per i dati fatti circolare nella dimensione pubblica virtuale di internet, come ad esempio sulle piattaforme dei *social network*, ove gli utenti dovrebbero poter optare per il livello di privacy con cui proteggere i dati nei propri profili personali[132]. In ciascuno di questi casi restano fermi gli obblighi informativi a beneficio del titolare dei dati, di cui si dirà a breve[133].

4.3. *La necessità di una previsione legislativa e il rispetto del canone di proporzionalità nelle limitazioni ai diritti*

Le previsioni normative che autorizzano l'impiego di TRF in presenza di un "interesse pubblico" offrono anche l'occasione di precisare

[130] Cfr. C. EDU, *P.G. and J.H. v. the United Kingdom*, 25 settembre 2001, par. 56; C. EDU, *Peck v. The United Kingdom*, 28 gennaio 2003, par. 59.

[131] GRUPPO DI LAVORO ARTICOLO 29, *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, cit., 10. Mette in guardia da questo rischio anche CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on Facial Recognition*, cit., 6.

[132] A.R. POPOLI, *L'adeguamento dei social network sites al GDPR: un percorso non ancora ultimato*, in *Il Diritto dell'informazione e dell'informatica*, 6, 2019, 1289 ss.; EAD., "*Social network*" *e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, *ivi*, 6, 2014, 981 ss.; D. TROTTIER, *Social Media as Surveillance. Rethinking Visibility in a Converging World*, London - New York, Routledge, 2016.

[133] Cfr. *infra* par. 6.1.

due aspetti che assumono una valenza più generale, riferita ai trattamenti di dati personali per qualunque finalità e in presenza di qualsiasi fondamento giuridico, specie – come visto – a fronte della debolezza del consenso esplicito. Si tratta di quelle condizioni attinenti alla necessità che, da una parte, vi sia una chiara disciplina a livello normativo che circostanzi il fondamento giuridico cui ricorrere e le condizioni alle quali utilizzare le TRF e, dall'altra, sia garantito il rispetto del principio di proporzionalità nelle limitazioni dei diritti perpetrabili tramite queste tecnologie, su cui anche l'*High-Level Expert Group* istituito dalla Commissione europea ha richiamato l'attenzione[134].

Il primo profilo, come detto, impone che vi sia una *previsione normativa* a supporto. A riprova della ritrosia o delle difficoltà delle autorità pubbliche a regolare l'uso di queste tecnologie, si pensi solo alla recente decisione del Garante della *privacy* italiano, che nel 2020 ha inibito al Comune di Como l'utilizzo dei sistemi di videosorveglianza integrati con TRF a scopo di indagine e di prevenzione nell'ambito delle politiche di sicurezza urbana. Il Comune aveva disposto tali misure in forza della legislazione che consente l'uso di misure di sorveglianza in ambito urbano, la quale tuttavia non autorizza espressamente il trattamento di dati biometrici, come invece richiesto dall'art. 7 del citato d.lgs. n. 51/2018, adottato in attuazione della LED[135].

Per comprendere meglio le caratteristiche e i contenuti della previsione giuridica in questione, si possono richiamare le precisazioni formulate dalla Corte EDU a proposito dell'interpretazione da offrire alla

[134] Cfr. l'HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, *Ethics Guidelines FOR Trustworthy AI*, cit., 130, ove si osserva che «l'identificazione automatica [...] desta enormi preoccupazioni di natura sia giuridica che etica, in quanto può avere effetti non previsti sotto molti aspetti a livello psicologico e socioculturale. Per salvaguardare l'autonomia dei cittadini europei è necessario ricorrere alle tecniche di controllo tramite l'IA in modo proporzionato. Definire chiaramente se, quando e come l'IA può essere utilizzata per l'identificazione automatica degli individui e differenziare tra l'identificazione di un individuo e la sua tracciatura e localizzazione, e tra sorveglianza mirata e sorveglianza di massa, sarà fondamentale per ottenere un'IA affidabile. L'applicazione di tali tecnologie deve essere chiaramente motivata dal diritto vigente» (versione italiana).

[135] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 26 febbraio 2020*, 26 febbraio 2020, n. 54, con riguardo ai limiti dell'art. 6, d.l. n. 11/2009, e dell'art. 7, d.l. n. 14/2017, quanto all'uso delle TRF.

necessità che le limitazioni al diritto al rispetto della vita privata *ex* art. 8, par. 2, della CEDU siano "previste dalla legge" [136]. Sulla base di indirizzi consolidati in tema di sorveglianza e forme di controllo, il riferimento deve intendersi soprattutto alla "qualità" delle norme[137]: occorre infatti che la legislazione nazionale sia "chiara, prevedibile e adeguatamente accessibile", in modo da consentire alle persone di agire in conformità alla legge e da delimitare chiaramente la portata della discrezionalità delle autorità pubbliche, oltre che fornire ai cittadini indicazioni adeguate in ordine alle condizioni e alle circostanze in cui le autorità hanno la facoltà di ricorrere alla raccolta di dati. La Corte EDU, inoltre, ritiene che per valutare se gli Stati si siano mantenuti entro il margine di apprezzamento consentito rilevino anche le garanzie procedurali accordate all'interessato[138].

Anche la Corte di giustizia, dal canto suo, ha stabilito che la previsione all'art. 52, par. 1, della CDFUE, secondo cui qualsiasi limitazione nell'esercizio dei diritti fondamentali deve «essere prevista dalla legge», implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato[139]. La normativa in questione, dunque, deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura *de qua* e impongano requisiti minimi in modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro da-

[136] Più in generale, sul concetto di "legge" e le sue caratteristiche sostanziali secondo la CEDU, N. LUPO, G. PICCIRILLI, *European Court of Human Rights and the Quality of Legislation: Shifting to a Substantial Concept of 'Law'?*, in *Legisprudence*, 6, 2, 2012, 229 ss. Per ulteriori considerazioni sul principio di legalità sostanziale, v. *infra* Cap. V, par. 7.

[137] Cfr. *ex multis* Corte EDU, *Silver e altri c. Regno Unit*o, 25 marzo 1983, p. 87 ss.; *Malone c. Regno Unito*, 2 agosto 1984, p. 67; *Halford c. Regno Unito*, 25 giugno 1997, p. 49; più di recente, *Khan c. Regno Unito*, 12 maggio 2000, p. 26; *Shimovolos c. Russia*, 21 giugno 2011, p. 68.

[138] Così che il processo decisionale che conduce a misure di ingerenza possa essere equo e tale da rispettare debitamente gli interessi della persona tutelati dall'art. 8 CEDU, v. Corte EDU, *Buckley c. Regno Unito*, 29 settembre 1996, p. 76; *M.S. c. Ucraina*, 11 luglio 2017, p. 70.

[139] CGUE, parere 1/15 (Accordo PNR UE-Canada), 26 luglio 2017, 139; CGUE, C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems*, 16 luglio 2020, p. 175.

ti personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti[140].

Da questi indirizzi giurisprudenziali, dunque, emerge chiaramente come a dover essere valorizzato non è tanto l'elemento formalistico delle norme in questione, fosse anche la presenza di un atto propriamente legislativo, quanto piuttosto la "sostanza" e la "qualità" delle stesse per come direttamente riferibili alle TRF[141].

Il secondo profilo da puntualizzare, come già anticipato, attiene invece al rispetto del *principio di proporzionalità* ai fini della valutazione circa la legittimità o meno del ricorso a TRF. È un giudizio che deve essere espresso caso per caso, sia sul contenuto delle norme per come sopra intese, sia sui concreti utilizzi che vengono fatti di queste tecnologie, tenendo conto della limitazione dei diritti, lo scopo e il contesto di impiego. A questo proposito, tutti i livelli di governo coinvolti nella protezione dei dati personali si sono interrogati sul punto e contribuiscono a definire la portata di tale principio.

Si pensi a quanto stabilito a proposito dal già richiamato art. 52 della CDFUE, secondo cui, come anche chiarito dalla Corte di giustizia, le ingerenze nella vita privata delle persone fisiche e nel diritto alla tutela dei dati personali, oltre che essere previste dalla legge e rispettare il contenuto essenziale di tali diritti, devono essere improntate proprio al rispetto del canone della proporzionalità, limitate allo stretto necessario e alle finalità di interesse generale[142]. Tali previsioni sono

[140] CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 54; CGUE, C-362/14, *Maximillian Schrems,* cit., par. 91; CGUE, C-203/15 e C-698/15, *Tele2 Sverige AB*, cit., p. 109: «Essa 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».

[141] In questo senso, cfr. G. PICCIRILLI, *La "riserva di legge". Evoluzioni costituzionali, influenze sovrastatuali*, Giappichelli, Torino, 2019, 237 ss., per cui la legge parlamentare non è condizione né necessaria, né sufficiente per soddisfare la legalità convenzionale citata. Per i riflessi sul principio di legalità interno, v. *infra* Cap. V, par. 7.

[142] CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 38; CGUE, C-291/12, *Schwarz v. Bochum*, 17 ottobre 2013, p. 34; CGUE, C-419/14, *WebMindLicenses Kft. v. Nemzeti Adó-es Vámhivatal Kiemelt Adó- és Vám Főigazgatóság*, 17 dicembre 2015, p. 69; CGUE, C-203/15 e C-698/15, *Tele2 Sverige AB*, cit., p. 94; CGUE, C-311/18, *Data Protection Commissioner,* cit., p. 174; CGUE, parere 1/15, cit., p. 138.

state poi sviluppate a livello normativo, ove peraltro si chiarisce come il diritto alla protezione dei dati personali non sia «una prerogativa assoluta», ma vada considerato alla luce della sua funzione sociale e contemperato con altri diritti fondamentali, «in ossequio al principio di proporzionalità»[143].

L'applicazione del principio di proporzionalità, secondo la Corte di giustizia, si colloca nel contesto di un iter valutativo più ampio, che guarda, come detto, alla previsione normativa, il perseguimento di un obiettivo generale, il rispetto del contenuto essenziale del diritto. Il test di proporzionalità vero e proprio si esplica poi nella valutazione sulla «idoneità» degli atti dei pubblici poteri a realizzare gli obiettivi legittimi perseguiti dalla norma e che tali atti «non superino i limiti» di ciò che è idoneo al conseguimento degli obiettivi stessi o «eccedano» più di quanto necessario a raggiungerli[144]. Il test così sviluppato – si potrebbe dire, con una certa semplificazione schematica – abbraccia il principio di proporzionalità in senso lato, nel quale vengono ricompresi i tre giudizi su[145]: idoneità del mezzo impiegato a perseguire gli obiettivi; la necessità in senso stretto, come scelta tra le varie soluzioni di quella più appropriata al perseguimento degli obiettivi con il minor sacrificio di interessi e diritti; la proporzionalità in senso stretto, come valutazione implicante la considerazione complessiva di vantaggi e

[143] Cons. 4 del GDPR. L'art. 23 elenca poi (par. 1) le finalità che possono giustificare la limitazione ai diritti e alle prerogative previste agli artt. da 12 a 22 e 34, nonché ai principi all'art. 5, e i contenuti necessari delle previsioni legislative limitative (par. 2).

[144] CGUE, C-291/12, *Schwarz*, cit., p. 45-46. CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 46-47.

[145] Cfr. G. DE BÙRCA, *The principle of proportionality and its application in EC law*, in *Yearbook of European law*, 13, 1993, 105 ss.; W. VAN GERVEN, *The Effect of Proportionality on the Actions of Member States of the European Comunity, National Viewpoints from Continental Europe*, in E. ELLIS (a cura di), *The Principle of Proportionality in the Laws of Europe*, Hart Publishing, Oxford-Portland, 1999, 37 ss., e T. TRIDIMAS, *Proportionality in Community Law: Searching for the Appropriate Standard of Scrutinity*, *ivi*, spec. 68 ss. La verifica dell'idoneità può essere accorpata anche al test di necessità in senso stretto, come ipotizzato in W. SAUTER, *Proportionality in EU law: A balancing act?*, in C. BARNARD, A. ALBORS-LLORENC, M.W. GEHRING, R. SCHÜTZE (a cura di), *Cambridge yearbook of European legal studies 2012-2013*, Hart Publishing, Oxford, 2013, 447 ss.

pregiudizi per diritti e interessi in gioco e che le limitazioni derivanti non siano eccessive rispetto agli scopi perseguiti[146].

Nell'operare tale valutazione, inoltre, occorre considerare che la portata del potere discrezionale del legislatore possa risultare limitata in funzione di un certo numero di elementi, tra i quali figurano, in particolare, il settore interessato, la natura del diritto di cui trattasi, la natura e la gravità dell'ingerenza, nonché la finalità di quest'ultima[147]. È una valutazione, in aggiunta, che deve essere condotta «in termini rigorosi»: è quanto specificato, ad esempio, allorché si tratti di autorizzare il rilascio di documenti biometrici idonei a evitarne la falsificazione o l'uso fraudolento[148], o della possibilità di conservare dati personali e sensibili a scopi di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali[149], o allorché sia possibile per le autorità pubbliche di trattare i dati per esigenze connesse alla sicurezza nazionale e all'interesse pubblico[150]. La necessità di disporre di siffatte garanzie è tanto più pressante allorché i dati personali siano soggetti a trattamento automatizzato[151].

Anche la Corte EDU, seppur in assenza di un riferimento testuale, usa richiamare il canone della proporzionalità, oltre che della necessità, per valutare se le limitazioni alla tutela della vita privata, e dunque anche dei dati personali, siano legittime[152].

[146] Distinzione particolarmente evidente in CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 65 e 69. Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, 19 dicembre 2019, 9. In dottrina, V. FIORILLO, *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di giustizia dell'Unione europea*, in *Federalismi.it*, 15, 2017. Più in generale, v. anche D.-U. GALETTA, *Il principio di proporzionalità fra diritto nazionale e diritto europeo (e con uno sguardo anche al di là dei confini dell'Unione europea)*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 6, 2019, 907 ss., ove si distingue tra giudizio di "idoneità", "necessità" e "proporzionalità".

[147] CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 46-47.

[148] CGUE, C-291/12, *Schwarz*, cit., p. 36.

[149] CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 38.

[150] CGUE, C-362/14, *Maximillian Schrems*, cit., p. 87.

[151] CGUE, parere 1/15 (Accordo PNR UE-Canada), cit., p. 141 s.; CGUE, C-311/18, *Data Protection Commissioner*, cit., p. 176; e giurisprudenza ivi citata.

[152] Cfr. A. TERRASI, *Il rapporto tra diritto alla privacy e protezione dei dati personali*

Secondo il Giudice di Strasburgo – limitandoci qui a richiamare il paradigmatico caso *S. e Marper* – per esprimere tale giudizio occorre, oltre ad una previsione legislativa, che una misura sia «necessaria» all'interno di «una società democratica» per il perseguimento dei fini elencati all'art. 8 CEDU. Per operare una valutazione su quest'ultimo aspetto, l'ingerenza è ammessa se risponde ad un bisogno sociale imperativo e, più in particolare, se essa è «proporzionata allo scopo legittimo perseguito» e se le ragioni addotte dalle autorità nazionali per giustificarla appaiano rilevanti e sufficienti[153]. Non solo, ma «qualsiasi Stato che pretenda di svolgere un ruolo pionieristico nello sviluppo di nuove tecnologie deve accollarsi anche la speciale responsabilità di individuare il corretto bilanciamento da applicare nella materia»[154]. Non stupisce, quindi, che nella Convenzione 108+ si preveda esplicitamente che «il trattamento dei dati dovrà essere proporzionato in rapporto allo scopo legittimo perseguito»[155].

Per chiudere il cerchio delle elaborazioni giurisprudenziali sul principio di proporzionalità, basti ricordare come anche la Corte costituzionale effettui un proprio test di proporzionalità, sebbene ricompreso nel più ampio giudizio di ragionevolezza[156]. È avvenuto di recente in occasione della sentenza 23 gennaio 2019, n. 20, in tema di protezione dei dati personali, ove la Corte ha ricordato che tale test, riconducibile nell'alveo dell'art. 3 Cost. per come integrato dai principi di derivazione europea, «richiede di valutare se la norma oggetto di scrutinio, con la misura e le modalità di applicazione stabilite, sia necessaria e idonea al conseguimento di obiettivi legittimamente perseguiti, in quanto, tra più misure appropriate, prescriva quella meno restrittiva dei diritti a confronto e stabilisca oneri non sproporzionati rispetto al perseguimento di detti obiettivi»[157].

tra Corte di giustizia dell'Unione europea e Corte europea dei diritti dell'uomo, in M. DISTEFANO (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Editoriale Scientifica, Napoli, 2017, spec. 133 ss.

[153] Cfr. Corte EDU, *S. e Marper c. Regno Unito*, 4 dicembre 2008, p. 101 ss.

[154] *Ivi*, p. 112.

[155] Art. 5, par. 1, Convenzione 108+.

[156] Come osserva M. CARTABIA, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, *Conferenza trilaterale delle Corte costituzionali italiana, portoghese e spagnola*, 25 ottobre 2013, 4 ss. Sul giudizio in base al principio di ragionevolezza v. *retro* Cap. II, nota 175.

[157] C.cost., sent. n. 20/2019, 3 cons. dir., ove si richiamano i precedenti costituiti

Il principio di proporzionalità, infine, ha ricevuto sistematica applicazione e affinamento anche da parte del Garante europeo per la protezione dei dati[158] e del Gruppo di lavoro "Articolo 29"[159], ora Comitato europeo per la protezione dei dati[160], ma anche per il tramite

da sentt. n. 137/2018, n. 10/2016, nn. 272 e 23/2015, nn. 162 e 1/2014. La Corte in questo caso si pronuncia sull'obbligo di pubblicazione per i titolari di incarichi dirigenziali nella P.A. di una serie di dati indicati all'art. 14, cc. 1-*bis* e 1-*ter*, d.lgs. n. 33/2013, stabilendo come nel bilanciamento tra principio di trasparenza amministrativa e di riservatezza le misure legislative risultino sproporzionate rispetto alle finalità perseguite e alla necessaria scelta della misura meno restrittiva dei diritti fondamentali in gioco. A commento, sullo specifico profilo del test di proporzionalità nel ragionamento della Corte, cfr. V. FANTI, *La trasparenza amministrativa tra principi costituzionali e valori dell'ordinamento europeo: a margine di una recente sentenza della Corte costituzionale (n. 20/2019)*, in *Federalismi.it*, 5, 2020, spec. 49 ss.; O. POLLICINO, F. RESTA, *Visibilità del potere, riservatezza individuale e tecnologia digitale. Il bilanciamento delineato dalla Corte*, in *Il diritto dell'informazione e dell'informatica*, 1, 2019, spec. 114 ss.; I.A. NICOTRA, *Privacy vs trasparenza, Il Parlamento tace e il punto di equilibrio lo trova la Corte*, *ivi*, 7, 2019, 7 ss.

[158] Cfr. EDPS, *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, cit.

[159] Già in GRUPPO DI LAVORO ARTICOLO 29, *Documento di lavoro sulla biometria*, WP 80, 1 agosto 2003, si affermava: «È necessario identificare con chiarezza le finalità del ricorso a sistemi biometrici e valutare se tale ricorso sia proporzionato rispetto alle finalità stesse, ossia se lo scopo che ci si prefigge può essere raggiunto egualmente attraverso modalità meno invasive». In ID., *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, cit., punto 2, si suggeriscono vari passaggi da esperire nella valutazione sull'adeguatezza di un sistema biometrico: la prima considerazione è se «il sistema sia inevitabile» per soddisfare la necessità accertata, ossia se è essenziale o, piuttosto, è il più conveniente o quello più efficace sotto il profilo dei costi; il secondo fattore di cui tener conto è la «potenziale efficacia» del sistema riguardo al soddisfacimento di tale necessità alla luce delle peculiarità della tecnologia biometrica di cui si prevede l'uso; il terzo aspetto da soppesare è se la conseguente perdita di riservatezza sia «proporzionata» al vantaggio previsto (nel caso in cui il vantaggio sia relativamente minore, come una maggiore comodità o un esiguo risparmio, la perdita di riservatezza non sarà ritenuta opportuna); il quarto aspetto è osservare se un «mezzo meno invasivo» della riservatezza possa raggiungere lo scopo desiderato. V. anche ID., *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, WP 211, 27 febbraio 2014.

[160] In COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 11, si legge che «prima di installare un sistema di videosorveglianza, il titolare del trattamento deve sempre valu-

delle autorità di controllo a livello nazionale, tra le quali si distingue anche il Garante italiano[161]. È grazie a questi che si trovano le applicazioni del principio di proporzionalità che più da vicino riguardano le TRF e su cui vale la pena spendere alcune considerazioni per verificare come tale principio operi in concreto.

La CNIL – come già anticipato[162] – si è pronunciata sui sistemi di riconoscimento facciale istallati all'ingresso di due scuole superiori francesi, aventi lo scopo di assistere i responsabili dei controlli al fine di prevenire intrusioni, furti di identità, e ridurre la durata degli stessi; misure alle quali gli studenti avevano precedentemente acconsentito. La *Commission* ha stabilito che tali forme di controllo fossero contrarie al principio di proporzionalità (ed anche di minimizzazione dei dati), dal momento che per raggiungere il medesimo scopo esistono mezzi molto meno invasivi in termini di *privacy* e libertà individuali, come, ad esempio, l'uso di badge[163]. Analoghe conclusioni sono tratte dall'Autorità di protezione dei dati svedese in un caso analogo, ove l'impiego di queste tecnologie è stato giudicato "troppo intrusivo" nei confronti dell'integrità personale degli studenti ed

tare criticamente se questa misura sia in primo luogo idonea a raggiungere l'obiettivo desiderato e, in secondo luogo, adeguata e necessaria per i suoi scopi. Si dovrebbe optare per misure di videosorveglianza unicamente se la finalità del trattamento non può ragionevolmente essere raggiunta con altri mezzi meno intrusivi per i diritti e le libertà fondamentali dell'interessato».

[161] Nel caso del Garante italiano, si veda, più di recente, il *Parere su uno schema di decreto del Presidente del Consiglio dei ministri concernente la disciplina di attuazione della disposizione di cui all'articolo 2 della legge 19 giugno 2019, n. 56, recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo"*, del 19 settembre 2019, con cui è stato rilevato non conforme al canone di proporzionalità la forma di attestazione della presenza in servizio dei dipendenti delle pubbliche amministrazioni basata contestualmente sulla videosorveglianza e la verifica biometrica, disposta in maniera sistematica, generalizzata e indifferenziata per tutte le pubbliche amministrazioni. Sul punto, si v. anche GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Verifica preliminare. Sistema di rilevazione delle immagini dotato di un software che permette il riconoscimento della persona (morfologia del volto)*, cit., 3; ID., *Verifica preliminare. Sistema di controllo accessi biometrico facciale*, cit., 3.1.

[162] V. *retro* par. 4.2.

[163] Cfr. CNIL, *Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position*, 29 ottobre 2019.

"eccessivo" rispetto a quanto necessario per monitorare la frequenza degli stessi[164].

Il Gruppo di lavoro "Articolo 29", invece, mette in guardia dalle funzionalità offerte dalle più moderne tecnologie di analisi video, grazie alle quali il datore di lavoro ha la possibilità di controllare le espressioni facciali del lavoratore utilizzando mezzi automatizzati al fine di individuare, fra l'altro, deviazioni da modelli di movimento predefiniti. Ciò – a detta del Gruppo di lavoro – «sarebbe sproporzionato nei confronti dei diritti e delle libertà dei dipendenti» e, di conseguenza, in linea di principio, illecito. Pertanto «i datori di lavoro dovrebbero astenersi dall'uso di tecnologie di riconoscimento facciale»[165].

Questi indirizzi, riferiti alla necessaria legislazione a supporto e al rispetto del principio di proporzionalità, costituiscono le architravi del contesto entro cui si collocano le articolazioni della disciplina sulla protezione dei dati. Ad essi occorrerà fare costante riferimento per verificare la tenuta, nei confronti delle TRF, dei principi e dei diritti che si andranno di seguito ad esaminare.

5. *Gli ulteriori principi a protezione dei dati*

5.1. *Limitazione delle finalità e uso secondario delle immagini*

Tra i principi a protezione dei dati personali che assumono maggiore rilievo nei confronti delle TRF vi è il principio di "*limitazione delle finalità*". Quale sviluppo diretto dell'art. 8 della CDFUE[166], tale

[164] Cfr. SWEDISH DATA PROTECTION AUTHORITY (*Integritetsskydds myndigheten*), *Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students*, cit.

[165] GRUPPO DI LAVORO ARTICOLO 29, *Parere 2/2017 sul trattamento dei dati sul posto di lavoro*, cit., 22, ove si osserva anche che «vi possono essere alcune eccezioni a questa regola, tuttavia tali scenari non possono essere utilizzati per invocare una legittimazione generale dell'utilizzo di tale tecnologia».

[166] Ove all'art. 8, parr. 1 e 2, la CDFUE stabilisce che «ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano» e «tali dati devono essere trattati [...] per finalità determinate».

principio impone che i dati personali debbano essere «raccolti per finalità determinate, esplicite e legittime» e «trattati in modo non incompatibile con tali finalità»[167].

In sostanza, con tale previsione si richiede la definizione di uno scopo preciso al momento della raccolta dei dati e che i dati non siano riutilizzati per altro scopo incompatibile[168]. Il principio si compone dunque di due parti, ovvero il riferimento alle "finalità determinate" al momento della raccolta e all'"uso compatibile" del trattamento[169].

In piena linea con l'evoluzione della concezione di fondo alla protezione dei dati personali[170], la *ratio* del principio è di rafforzare la libertà di autodeterminazione sui propri dati, esercitando su di essi una qualche forma di controllo; di prevenire la possibilità che siano lesi i propri diritti mediante l'utilizzo non dichiarato dei dati o la loro violazione tramite un accesso illegittimo; di promuovere al contempo la fiducia nei confronti del trattamento dei dati e, a livello economico, della concorrenza tra attività che ne fanno utilizzo[171].

Il legislatore, inoltre, si mostra consapevole della necessità che la tutela segua la circolazione dei dati, definendo i confini legittimi del loro possibile riutilizzo (c.d. *trattamenti secondari*)[172].

Nel caso del GDPR si consente un nuovo utilizzo purché sia "compatibile" con le finalità di raccolta, indicando allo scopo una serie di condizioni in assenza delle quali occorre chiedere un nuovo consenso o ricorrere ad una diversa base legale[173].

[167] Art. 5, par. 1, lett. b, del GDPR; art. 4, par. 1, lett. b della LED. A livello convenzionale, una formulazione analoga al GDPR è prevista anche dall'art. 5, par. 4, lett. b, della Convenzione 108+.

[168] N. FORGÓ, S. HÄNOLD B. SCHÜTZE, *The Principle of Purpose Limitation and Big Data*, in M. CORRALES, M. FENWICK, N. FORGÓ (a cura di), *New Technology, Big Data and the Law*, Springer, Singapore, 2017, 20.

[169] *Ivi*, 33 ss., anche per una ricostruzione dell'evoluzione storica della normativa UE sul punto.

[170] V. *retro* Cap. II, par. 4.

[171] T.Z. ZARSKY, *Incompatible: The GDPR in the Age of Big Data*, in *Seton Hall Law Review*, 47, 2017, 1007.

[172] Sia il GDPR (art. 5, par. 1, lett. b) che la LED (art. 3, par. 4) considerano compatibile con le finalità originarie il trattamento «a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

[173] Art. 6, par. 4 del GDPR. Si fa riferimento ad una valutazione di "compatibilità

La LED, sulla falsariga di quanto disposto a livello convenzionale, reca invece una disciplina più ampia rispetto al GDPR nel consentire l'accesso e il riutilizzo dei dati da parte delle forze di polizia[174], sebbene ciò debba sempre avvenire all'interno degli scopi rientranti nel più generale fine della prevenzione e della salvaguardia contro minacce alla sicurezza pubblica[175]. Resta fermo, tuttavia, che l'attività di contra-

delle finalità", che guarda a fattori come il nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; il contesto in cui i dati personali sono stati raccolti; la natura dei dati personali; le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; l'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione. Sul punto si veda anche il cons. 50 e GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 12.

Interessante al riguardo è la nuova formulazione della Convenzione 108+, che all'art. 5, par. 4, lett. b, stabilisce che i dati, una volta raccolti, non siano "trattati in maniera incompatibile con le finalità" di raccolta; L'*Explanatory Report* al testo chiarisce che i dati personali non dovrebbero essere ulteriormente trattati in modalità che il titolare degli stessi consideri inaspettate, inappropriate o altrimenti contestabili. Nel compiere questa valutazione, devono essere presi in considerazione, tra l'altro, il collegamento tra la finalità di raccolta e del riutilizzo; il contesto di raccolta e l'aspettativa ragionevole del titolare dei dati alla luce del rapporto con colui che li tratta; la natura dei dati; le conseguenze del riutilizzo; l'esistenza di appropriate misure di salvaguardia (punto 49).

[174] L'art. art. 4, par. 2 LED legittima un nuovo trattamento da parte delle autorità pubbliche ove previsto in conformità al diritto dell'UE o degli Stati e purché il trattamento sia necessario e proporzionato a tale nuove finalità. Principi analoghi si rintracciano anche a livello convenzionale. Sebbene nella Raccomandazione n. R(87) 15, punto 5, ci si riferisca a condizioni formulate in termini analogamente ampie, si suggerisce che il riutilizzo debba rispettare le garanzie perviste per il primo trattamento, ovvero essere previsto dalla legge, operato per uno scopo legittimo e risultare necessario e proporzionato con tale scopo; cfr. CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Practical guide on the use of personal data in the police sector*, T-PD(2018)01, 15 febbraio 2018, 4, ove si specifica anche che tale valutazione debba tener conto di ulteriori interessi come la gravità dei crimini o la necessità di tutelare vittime del reato o persone particolarmente fragili.

[175] Così il cons. 29 della LED, anche se, è stato osservato, in questo caso sarebbe stato meglio elencare esemplificativamente le finalità non incompatibili; cfr. A. RICCI, *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati*, cit., 582.

sto, di per sé, non possa essere ritenuta una finalità determinata, esplicita e tale da legittimare il riutilizzo dei dati, ad esempio, per indagare su reati diversi da quelli in relazione ai quali sono stati raccolti[176]. Anche sul punto, tuttavia, la disciplina attuativa a livello nazionale reca alcune incertezze, soprattutto nella misura in cui consente, a determinate condizioni, la comunicabilità dei dati anche ad altre amministrazioni o addirittura a privati[177].

La Corte di giustizia, nella giurisprudenza qui più rilevante, impone che vengano indicate le «condizioni sostanziali e procedurali» per il riutilizzo dei dati[178], e che si determinino «criteri oggettivi» rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso, sia la nuova utilizzazione di tali dati comporta rispetto alla finalità perseguita[179]. Anche la Corte EDU, con particolare chiarezza nel caso *S. e Marper*, ritiene essenziale, nel contesto di misure di sorveglianza e di utilizzo di dati biometrici, avere regole chiare e dettagliate volte a disciplinare la portata e le modalità di applicazione delle misure nonché le garanzie minime riguardanti, fra l'altro, la durata, la conservazione, l'utilizzo, l'accesso di terzi, le procedure destinate a preservare l'integrità e la confidenzialità dei dati e le procedure di distruzione degli stessi, in modo da prevedere sufficienti garanzie contro i rischi di abusi o utilizzi arbitrari[180].

[176] Come chiarito in GRUPPO DI LAVORO ARTICOLO 29, *Parere 03/2015 sulla proposta di direttiva concernente la tutela 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, e la libera circolazione di tali dati*, WP233, 1 dicembre 2015, 6, occorre esaminare caso per caso la compatibilità della finalità e verificare che la base giuridica includa chiare ed esplicite salvaguardie.

[177] Cfr. art. 13, c. 3, del d.P.R. n. 15/2018, che consente la comunicazione dei dati personali a pubbliche amministrazioni o enti pubblici e a privati quando risponde all'interesse della persona cui i dati si riferiscono e, comunque, nei singoli casi in cui è necessaria per evitare un pericolo grave e imminente alla sicurezza pubblica, o per la salvaguardia della vita e dell'incolumità fisica di un terzo.

[178] CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 61; CGUE, parere 1/15 (Accordo PNR UE-Canada), cit., p. 192.

[179] CGUE, C-362/14, *Maximillian Schrems*, cit., p. 93; CGUE, parere 1/15 (Accordo PNR UE-Canada), cit., 191.

[180] Corte EDU, *S. e Marper*, cit., p. 99; anche, *M.M. c. Regno Unito*, 13 novembre 2012, p. 195.

Il rispetto di tali criteri, tuttavia, può apparire problematico per fronteggiare l'impiego delle TRF.

Come anticipato a proposito dei *big data*[181], accanto ad un "uso primario" dei dati e delle immagini, legato al loro sfruttamento per rispondere direttamente agli interessi e alle esigenze per le quali sono state raccolte, vi è un "uso secondario" che disvela il "valore opzionale" dei dati, di cui non è possibile prevedere preventivamente l'esistenza e la consistenza[182]. I dati costituiti dalle immagini in formato digitale sono facili da captare, vengono raccolti in *database* in grado di contenerne enormi quantità e di facilitarne la cessione e circolazione[183]. Le TRF, come più in generale le *big data analytics*, consentono di rielaborare i dati e di utilizzarli in modi e per finalità che, sia il titolare del trattamento, sia l'individuo ripreso, difficilmente possono immaginare al momento della raccolta[184].

Le possibilità offerte da queste tecnologie aprono quindi a pericoli arginabili con grande difficoltà. Si pensi, ad esempio, alla facilità con cui le fotografie sul *web*, nei *social media* o nelle applicazioni per la relativa gestione vengono fatte oggetto di ulteriori trattamenti al fine dell'estrazione di modelli biometrici o di riconoscimento del volto in assenza di una specifica base giuridica – il consenso, per esempio – per questa nuova finalità[185].

[181] V. *retro* Cap. I, par. 3.2.

[182] M. DELMASTRO, A. NICITA, *Big data*, cit., 27. Non si tratta certo di una novità: già S. RODOTÀ, *Tecnologie e diritti*, cit., 47, sottolineava come «le informazioni fornite dagli interessati per ottenere determinati servizi sono tali, per quantità e qualità, da determinare la possibilità di una serie di impeghi secondari, particolarmente remunerativi per i gestori dei sistemi interattivi».

[183] Sulle modalità con cui vengono composti i *database* di immagini, v. anche *infra* par. 5.3.

[184] Con riguardo alle *big data analytics*, cfr. L. MITROU, *Data Protection, Artificial Intelligence and Cognitive Services. Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?*, cit., 46 ss.

[185] GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, cit., p. 2. Per questo, più in generale, si prevede che le immagini digitali e i modelli siano utilizzati esclusivamente allo scopo per il quale sono stati forniti; cfr. ID., *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile*, cit., 8, ove si imputa tale compito ai controlli tecnici dei responsabili del trattamento.

L'uso specifico di TRF da parte delle forze dell'ordine, inoltre, apre a rischi di abusi, ad esempio, in quelle pratiche chiamate di *fishing expeditions*, ovvero "rastrellamenti" di immagini ad ampio raggio, al limite della legalità, con lo scopo generico di raccogliere informazioni su di una popolazione di potenziali sospettati[186]. Occorre invece arginare quelle ipotesi in cui manchi una diretta ed evidente correlazione tra i dati trattati e la situazione riferibile ad uno specifico soggetto che abbia commesso o sia probabile che commetta un reato: questo implica che la polizia debba applicare il principio di limitazione delle finalità a tutti gli stadi del procedimento penale, garantendo un collegamento costante tra la persona titolare dei dati e lo scopo del trattamento, come ad esempio una indagine o compiti specifici[187]. Per questo anche l'Agenzia dell'UE per i diritti fondamentali suggerisce che le TRF debbano essere limitate a finalità di interesse pubblico strettamente circoscritte e disciplinate[188].

5.2. *La minimizzazione dei dati e la ricerca della giusta misura*

Altro principio a presidio dei dati personali e biometrici è quello riferito alla "*minimizzazione dei dati*".

La logica di fondo di questo principio è che occorre limitarsi alla

[186] Cfr. N. STROSSEN, *Post-9/11 Government Surveillance, Suppression and Secrecy*, in A.D. MOORE (a cura di), *Privacy, Security and Accountability. Ethics, Law and Policy*, Rowman & Littlefield, New York, 2016, 226 s.

[187] Così CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Practical guide on the use of personal data in the police sector*, cit., 3. Si v. il punto 2.1. della Raccomandazione n. R(87) 15, il quale parla di «raccolta di dati a carattere personale a fini di polizia [...] limitato a quanto necessario per la prevenzione di un pericolo concreto o alla repressione di una determinata infrazione penale. Ogni eccezione a tale disposizione dovrà essere oggetto di una specifica legislazione nazionale». Significativo altresì il principio 2.3, secondo cui «la raccolta di dati indiretta con mezzi tecnici di sorveglianza o altri mezzi automatizzati dovrà essere preceduta da specifiche disposizioni». Sulla necessità che la raccolta, conservazione e cancellazione delle schede dattiloscopiche sia giustificata sulla base di una condanna e non di un mero sospetto, a fronte della conservazione per un lungo periodo di tempo, v. anche Corte EDU, *S. e Marper*, cit., p. 107 ss.; *M.K. c. Francia*, 18 aprile 2013, p. 39.

[188] FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., 25.

raccolta dei dati personali necessari per raggiungere la finalità legittima, cancellando quelli non necessari o non conformi a tale finalità.

Le diverse normative sulla protezione dei dati offrono una specificazione in termini parzialmente difformi[189]. In particolare, sia il GDPR che la LED fanno riferimento alla necessità che i dati personali siano «adeguati» e «pertinenti» rispetto alle finalità per le quali sono trattati. Mentre però il regolamento prevede che i dati siano «limitati a quanto necessario»[190], la direttiva si riferisce invece a dati «non eccedenti»[191] rispetto a tali finalità, lasciando intendere un vincolo potenzialmente meno stringente in relazione al perseguimento degli scopi di pubblico interesse ad essa sottesi[192]. La normativa italiana recupera in parte tale rigore nella misura in cui dispone che le riprese video-fotografiche implichino la raccolta di dati strettamente necessari per le finalità di polizia, registrando solo «quelli indispensabili»[193].

La *ratio* garantistica e i valori presidiati dal principio di minimizzazione dei dati sono quindi del tutto analoghi a quelli enunciati sopra a

[189] L'art. 5, lett. c, della Convenzione 108 parla di dati registrati «adeguati, pertinenti e non eccessivi in rapporto ai fini per i quali sono registrati». Di «dati necessari» parla invece il principio 3.1 della Raccomandazione n. R(87) 15.

[190] Art. 5, par. 1, lett. c, del GDPR. Tale principio è richiamato anche nella enunciazione del principio di "*privacy by design*" all'art. 25, par. 1, su cui v. *infra*, Cap. V, par. 5.

[191] Art. 4, par. 1, lett. c, della LED.

[192] Disparità sottolineata in GRUPPO DI LAVORO ARTICOLO 29, *Parere 03/2015 sulla proposta di direttiva concernente la tutela 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, e la libera circolazione di tali dati*, cit., 7. V. anche T. MARQUENIE, *The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework*, cit., 331. Osserva invece A. RICCI, *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati*, cit., 579, come la "necessità" vada riferita ai dati oggetto di trattamento e ai requisiti ad esso intrinseci, e non coincide con la necessità del trattamento in sé considerato, che invece costituisce uno dei presupposti per la sua liceità, da ravvisarsi con la LED nella strumentalità del dato al perseguimento di finalità di prevenzione, indagine, accertamento e perseguimento dei reati.

[193] Così art. 23, c. 2, del d.P.R. n. 15/2018, sebbene – si ricorda – le finalità di polizia ivi indicate siano espresse in termini parzialmente differenti dal d.lgs. n. 51/2018 (v. *retro* par. 2).

proposito del principio di limitazione delle finalità, riferiti all'autodeterminazione e al controllo sui propri dati, anche con lo scopo di prevenire violazioni dei propri diritti[194].

Venendo alle TRF, il principio di minimizzazione assume una rilevanza immediata in quella fase del trattamento dei dati biometrici costituita dalla costruzione del *template* biometrico. I titolari del trattamento, infatti, devono garantire che i dati estratti da un'immagine digitale per costruire un modello non siano eccessivi, per evitare ingerenze ingiustificate, e contengano unicamente le informazioni richieste ai fini dell'utilizzo specificato, in modo da scoraggiare così ogni eventuale ulteriore trattamento per finalità incompatibili[195].

Le dimensioni dei modelli biometrici e la quantità dei dati contenuti, da una parte, devono essere *sufficientemente ampie* da rendere il *template* utile alle finalità di trattamento e permettere di garantire la sicurezza dei dati, evitando il rischio di sovrapposizione tra dati biometrici diversi o di sostituzione di identità, come avverrebbe nel caso di modelli troppo poco accurati; dall'altra, le dimensioni del *template* devono essere *sufficientemente ristrette*[196], per mantenere l'univocità della costruzione del modello e non consentire di risalire ai dati biometrici raccolti dai quali esso è stato costruito[197]. L'eccessiva ampiezza, inoltre, favorirebbe il trasferimento dei *template* tra sistemi biometrici diversi, con possibili riutilizzi incompatibili con il fondamento giuridico iniziale[198].

Il principio in questione viene in rilievo anche al momento della

[194] In questo modo, il principio in parola costituisce la combinazione dei tradizionali principi di limitazione nella raccolta dei dati, qualità degli stessi, specificazione delle finalità e limitazione nel loro utilizzo; cfr. L. MITROU, *Data Protection, Artificial Intelligence and Cognitive Services. Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?*, cit., 49.

[195] Cfr. COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 22; GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile*, cit., 9.

[196] Come osservato in GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, cit., p. 2.

[197] *Ibidem*.

[198] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 22.

costruzione delle gallerie (c.d. *watchlist*) con cui vengono confrontate le immagini delle persone da identificare. Su questo aspetto la ICO ha recentemente imposto l'attenzione, nella misura in cui prassi difformi da parte delle forze dell'ordine rischiano di risolversi, fra l'altro, in una violazione del principio di minimizzazione[199]. È il caso, ad esempio, del *Metropolitan Police Service* di Londra, che confeziona specifiche *watchlist* a seconda del tipo di operazione da condurre (ad esempio, in occasione di manifestazioni sportive, con soggetti che si siano resi partecipi di episodi di violenza in tali contesti), e della *South Wales Police* di Cardiff, che ritiene sia più efficiente ampliare la platea delle immagini sottoposte a confronto, rischiando però di dar vita ad una misura sproporzionata allorché si processino contestualmente immagini di soggetti all'attenzione delle forze dell'ordine per differenti ragioni con quelle, ad esempio, raccolte dai *social media*[200].

Come detto a proposito del principio di limitazione delle finalità, anche il principio di minimizzazione dei dati manifesta alcune vulnerabilità di fronte alla diffusione delle tecnologie in parola. Il concetto stesso di minimizzazione dei dati si dimostra incompatibile con le tecniche di *big data analytics* e di *machine learning*, che richiedono *ab origine* un'enorme quantità di dati da processare[201]. Si è visto come il valore dei dati nella economia digitale rappresenti un valore "latente", che può essere pienamente sfruttato non al momento della raccolta, ma nel momento in cui il dato viene utilizzato, riutilizzato e combinato con altri dati per una molteplicità di scopi. I *Big tech* hanno tutto l'interesse ad acquisire la maggior quantità di dati possibile e conservarla il più a lungo possibile[202], mentre le stesse *big data analytics* cercano di sfuggire a qualsiasi forma di restrizione *ex ante*[203].

[199] INFORMATION COMMISSIONER'S OFFICE, *ICO investigation into how the police use facial recognition technology in public places*, 31 ottobre 2019, 14 ss.

[200] Sulla vicenda giudiziaria che ha coinvolto le *South Wales Police*, v. *infra* par. 8.

[201] M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges*, cit., 64.

[202] V. MAYER-SCHÖNBERGER, Y. PADOVA, *Regime Change? Enabling Big Data through Europe's New Data Protection Regulation*, cit., 320.

[203] I.S. RUBINSTEIN, *Big Data: The End of Privacy or a New Beginning?*, in *International Data Privacy Law*, 3, 2, 2013, 78.

5.3. *Conservazione delle immagini e problematiche connesse*

Il principio di minimizzazione dei dati, riguardante lo scopo e la quantità di dati utilizzati, è strettamente collegato anche ai limiti teleologici e temporali del relativo utilizzo. Sotto questo profilo vi è quindi continuità con un altro principio, ovvero quello della "*limitazione della conservazione*", secondo cui i dati personali devono 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[204].

Secondo quanto stabilito dalla Corte di giustizia a partire dal caso *Digital Rights Ireland*, la *mera conservazione* per un certo periodo dei dati relativi alla vita privata di una persona e alle sue comunicazioni costituisce di per sé un'ingerenza nei diritti garantiti dall'art. 7 della CDFUE e nella protezione dei dati personali garantito dall'art. 8 CDFUE[205]. La conservazione dei dati, dunque, deve «rispondere sempre a criteri oggettivi, istituendo un rapporto tra i dati da conservare e l'obiettivo perseguito»[206].

Sulla falsariga, la Corte EDU aggiunge, nel caso *S. e Marper*, che «il carattere generale ed indifferenziato» della conservazione delle impronte digitali, dei campioni di cellule e dei profili di DNA di individui sospettati della commissione di determinati reati, che però non sono poi condannati, «non garantisce un corretto bilanciamento dei concorrenti interessi pubblici e privati in gioco» e pertanto «costituisce una ingerenza sproporzionata nel diritto dei ricorrenti al rispetto della vita privata»[207]. Come chiarito aggiuntivamente nel caso *M.M.*, la rac-

[204] Il principio della "limitazione della conservazione" viene sancito dall'art. 5, par. 1, lett. e, del GDPR, e dall'art. 4, par. 1, lett. e, della LED; il regolamento fa salvi i fini di archiviazione nel pubblico interesse, ricerca scientifica o statistici, e la predisposizione di misure tecniche e organizzative adeguate; cfr. T.Z. ZARSKY, *Incompatible: The GDPR in the Age of Big Data*, cit., 1009. V. anche l'art. 5, par. 1, lett. e, della Convenzione 108.

[205] CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 34-35.

[206] CGUE, C-203/15 e C-698/15, *Tele2 Sverige AB*, cit., p. 110, ove si aggiunge che «tali condizioni devono risultare, in pratica, idonee a delimitare effettivamente la portata della misura e, di conseguenza, il pubblico interessato».

[207] Corte EDU, *S. e Marper*, cit., p. 125.

colta indiscriminata e per un periodo indeterminato di dati relativi anche alle condanne penali viola il diritto l'art. 8 della CEDU, in assenza di norme chiare e dettagliate che specifichino le garanzie applicabili ed enuncino le regole che disciplinano, fra l'altro, le circostanze che consentono di raccogliere i dati, la durata della loro conservazione, l'utilizzo che se ne può fare e le circostanze che ne consentono la distruzione[208].

Ne deriva, quindi, che allorquando venga meno il rapporto tra la conservazione dei dati e la finalità che ne ha giustificato la raccolta, in mancanza di una base giuridica ulteriore per il trattamento è necessario procedere alla *cancellazione dei dati*. Nel caso del riconoscimento facciale, questo obbligo vale sia per i *template* biometrici, sia per i dati biometrici "grezzi" – ovvero i dati personali costituiti dalle immagini del volto una volta identificati – generati nel corso del procedimento di acquisizione[209]. Infatti, nella misura in cui i modelli biometrici derivano da tali dati, la costituzione di *database* contenenti queste immagini potrebbe rappresentare una minaccia anche più seria. Mentre non è sempre facile leggere un modello biometrico senza conoscere l'algoritmo con il quale è stato prodotto, i dati grezzi sono gli elementi costitutivi di qualsiasi modello e permettono di replicarlo con diverse tecniche algoritmiche[210].

Il momento della cancellazione, inoltre, può variare a seconda dei risultati del riconoscimento facciale: in caso di mancata corrispondenza, i dati dovrebbero essere cancellati automaticamente, mentre in caso di corrispondenza la conservazione dovrebbe avvenire per il tempo

[208] Corte EDU, *M.M.*, cit., p. 199.

[209] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee-guida in materia di riconoscimenti biometrico e firma grafometrica*, cit., 25, che sollecita a cancellare complessivamente tali dati dalle aree di memoria temporanea, centrale e secondaria, e dal *filesystem* del sistema utilizzato per l'acquisizione immediatamente dopo la generazione del modello biometrico.

[210] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 23, ove si suggerisce, nel caso in cui si debba conservare tali dati, l'applicazione di "rumore additivo" per impedire la creazione del modello. Occorrerebbe inoltre cancellare i dati biometrici e i modelli in caso di accesso non autorizzato al terminale di lettura e raffronto o al server di conservazione, oppure al termine della vita utile del dispositivo biometrico.

strettamente necessario agli scopi definiti per i quali sussiste un fondamento legittimo[211].

Alla luce di questo principio risultano problematiche tutte quelle ipotesi in cui i *dataset* con cui allenare gli algoritmi di riconoscimento facciale vengono costruiti attraverso la pratica del c.d. *data scraping*[212], ovvero la raccolta massiccia e indistinta di immagini da internet, molto spesso senza ottenere il consenso degli interessati o delle piattaforme *social* nelle quali sono ospitate[213]. Il caso più eclatante è offerto dal servizio di riconoscimento facciale ideato da Clearview AI e messo a disposizione di numerose agenzie di polizia degli Stati Uniti[214]. Non stupisce, dunque, che il Comitato europeo per la protezione dei dati sia del parere che il ricorso in Europa a tale servizio difficilmente potrebbe considerarsi coerente con il regime relativo di protezione dei dati[215]. Le stesse piattaforme di *social network* hanno ingiunto a Clearview AI di interrompere queste pratiche di rastrellamento dei dati[216].

Anche per la conservazione dei dati biometrici a fini di polizia possono sorgere analoghi problemi quanto al venir meno delle finalità per

[211] CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on Facial Recognition*, cit., 12.

[212] Cfr. F. CAMPBELL, *Data Scraping – What Are the Privacy Implications*, in *Privacy & Data Protection*, 20, 1, 2019, 3.

[213] Per l'indicazione di alcuni tra i *dataset* pubblicamente disponibili v. U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, cit., 19 s. Queste pratiche, oltre a violare i limiti alla conservazione dei dati, originano una serie di problematiche accessorie in termini di fenomeni discriminatori sulle quali occorrerà soffermarsi ulteriormente *infra* par. 7.

[214] V. *retro* Introduzione.

[215] Cfr. COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Comunicato stampa*, 10 giugno 2020. Più ampiamente, sulle problematiche sollevate, v. I. NERONI REZENDE, *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, cit., spec. 382 ss.

[216] G. PEREZ, H. COOK, *Google, YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app that helps law enforcement*, in *CBS News*, 5 febbraio 2020 [cbsn.ws/31TA5R2]. In risposta, Clearview AI ha replicato come la sua attività di raccolta dati sia coperta dal Primo Emendamento della Costituzione degli USA; cfr. K. FAN, *Clearview AI Responds to Cease-and-Desist Letters by Claiming First Amendment Right to Publicly Available Data*, in *JoltDigest*, 25 febbraio 2020 [bit.ly/2Q7J2ni].

le quali sono stati raccolti e alla loro perdurante conservazione[217]. Si pensi alla costruzione di banche dati da parte delle forze dell'ordine per scopi di *intelligence*[218], da utilizzare stabilmente come gallerie per il confronto durante attività investigative a fini di identificazione. A porre problemi in questo senso, dunque, non sono tanto le immagini e i dati biometrici legati ad una indagine penale ben precisa, per la quale il periodo di conservazione è correlato alla durata della stessa, quanto la conservazione a fini di prevenzione, per la quale ci si basa su una valutazione dei rischi riguardanti determinati soggetti[219]. Anche per questo viene previsto l'obbligo per gli Stati di fissare "termini adeguati" per la cancellazione o quantomeno per un "esame periodico" sulla necessità della conservazione degli stessi[220].

Accanto alla delimitazione temporale dei termini di conservazione,

[217] A questo proposito, si v. il principio 7 della Raccomandazione n. R(87) 15, secondo cui «dovranno essere prese adeguate misure perchè dati a carattere personale conservati a fini di polizia vengano cancellati quando non sono più necessari per i fini per i quali sono stati precedentemente registrati. A questo fine, si conviene, in particolare, di prendere in considerazione i seguenti criteri: necessità di conservare i dati alla luce delle conclusioni di un'inchiesta per un certo caso; pronuncia di una decisione definitiva e, in particolare, assoluzione; riabilitazione; prescrizione; amnistia; età della persona interessata; categoria particolare di dati. Dovranno essere stabilite, in accordo con l'autorità di controllo o in conformità al diritto interno, una serie di regole tese a stabilire i periodi di conservazione per le differenti categorie di dati a carattere personale, così come i controlli periodici sulla loro qualità».

[218] Per *intelligence* si intende qui la raccolta e la successiva analisi di dati e notizie dalla elaborazione delle quali si ricavano informazioni utili per indirizzare le indagini penali. Osserva M. TORRE, Privacy *e indagini penali*, GFL, Milano, 2018, 133 ss., come il più fertile terreno per queste attività è rappresentato proprio dalle c.d. fonti aperte, ossia fonti di informazione in partenza non riservate e disponibili al pubblico.

[219] GRUPPO DI LAVORO ARTICOLO 29, *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, cit., 4.

[220] Art. 5 LED. Per la disciplina sui termini di conservazione vigente nel nostro ordinamento, v. art. 10 del d.P.R. n. 15/2018. Per la conservazione della particolare categoria dei dati relativi al traffico telefonico e telematico ai fini di accertamento e repressione di reati e i conseguenti obblighi del fornitore di servizi, v. art. 132 del d.lgs. n. 196/2003, su cui si rinvia più approfonditamente a M. TORRE, Privacy *e indagini penali*, cit., 51 ss., anche per le procedure di accesso da parte delle forze dell'ordine.

inoltre, il principio in parola origina alcune conseguenze anche nelle *modalità di conservazione* dei dati biometrici, nella specie dei modelli di riferimento per il riconoscimento facciale.

È probabile, infatti, che la verificazione e l'autenticazione richiedano la conservazione del *template* da utilizzare per i successivi raffronti. In questo caso occorre valutare quale sia il luogo e la modalità più appropriata per la conservazione dei dati, ovvero se nella disponibilità del titolare dei dati oppure del titolare del trattamento[221]. Nel primo caso, è possibile fare ricorso a dispositivi sicuri, come *smartphone* o *smartcard*, affidati direttamente ed esclusivamente agli interessati. Nel secondo, i dati biometrici sono affidati alla gestione di colui che tratta i dati, che li conserva in *database* centralizzati o sugli stessi dispositivi di acquisizione biometrica. Con specifico riguardo alle TRF, la prima soluzione sembrerebbe la più rispettosa del diritto alla protezione dei dati nell'ipotesi di verificazione[222], mentre per finalità di identificazione, ove necessario per scopi specifici ed esigenze oggettive, sarebbe possibile ricorrere a banche dati centralizzate[223].

L'attività di conservazione dei dati, infine, si lega direttamente anche ad altri principi a protezione dei dati personali e biometrici rilevanti per le TRF, quali i principi "*integrità e riservatezza*". In forza di

[221] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee-guida in materia di riconoscimenti biometrico e firma grafometrica*, cit., 20.

[222] Cfr. CNIL, *Reconnaissance faciale dans les aéroports: quels enjeux et quels grands principes à respecter ?*, cit., che indica tra ai principi necessari da rispettare anche «maintenir les données biométriques sous le contrôle exclusif des passagers concernés». Ciò nonostante che in caso di furto, smarrimento o distruzione del dispositivo, l'interessato potrebbe essere temporaneamente impossibilitato all'utilizzo del sistema biometrico.

[223] Così già in GRUPPO DI LAVORO ARTICOLO 29, *Documento di lavoro sulla biometria*, cit., 4 s. In COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 23, si specifica che in questo caso occorrerebbe conservare i dati in forma cifrata con una chiave segreta nota esclusivamente all'interessato, per impedire l'accesso non autorizzato al modello o al luogo ove viene conservato. Se il titolare del trattamento non può evitare di accedere ai modelli, deve adottare le opportune misure per garantire la sicurezza dei dati conservati. Sui sistemi di criptazione o di anti-falsificazione dell'identità, maggiori dettagli in GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, cit., p. 5.4.1.

essi, i dati devono essere trattati in maniera da garantire un'adeguata sicurezza contro trattamenti illeciti o la perdita, la distruzione e i danni accidentali, contemplando anche il ricorso a "misure tecniche e organizzative" adeguate[224].

Tali principi, da considerare un portato del più generale principio di responsabilità, informano l'intero procedimento di riconoscimento facciale e le varie fasi di trasferimento dei dati, nei vari passaggi tra l'acquisizione delle immagini, l'impiego di un software o il caricamento delle immagini su un sito web per l'estrazione delle caratteristiche, l'effettuazione del confronto, sino all'archiviazione del *template* biometrico ai fini di un successivo utilizzo[225].

Le misure tecniche e organizzative che il titolare del trattamento deve porre in atto, infine, sono preordinate a garantire l'ulteriore principio di "*sicurezza del trattamento*", da parametrare in relazione alla natura, l'oggetto, il contesto e le finalità del trattamento, come anche il rischio di varia probabilità e gravità per i diritti[226]. A questo riguardo, la normativa dell'UE elenca espressamente una serie di obiettivi e di misure ritenute adeguate[227] – fra le quali spicca la pseudonimizzazione

[224] Art. 5, par. 1, lett. f, del GDPR; art. 4, par. 1, let. f, della LED. La sicurezza dei dati deve essere salvaguardata anche ai sensi dell'art. 7 della Convenzione 108 e della Convenzione 108+. V. anche il principio 8 della Raccomandazione n. R(87) 15. In attuazione, il d.P.R. n. 15/2018 indica all'art. 24 una disciplina sulle "speciali misure di sicurezza" richieste per il trattamento di dati attraverso sistemi di videosorveglianza e di ripresa video-fotografica, stabilendo che i sistemi informativi e i programmi informatici destinati alla registrazione e alla conservazione dei dati personali così raccolti siano configurati «in modo da ridurre al minimo l'utilizzazione di dati relativi a persone identificabili» (c. 1); che siano configurati «diversificati livelli di visibilità e di trattamento delle immagini», tramite credenziali di autenticazione (c. 2); che gli accessi e le operazioni siano registrati in appositi file di log, da conservare per 5 anni (c. 4), impiegabili ai soli fini della verifica della liceità del trattamento, del controllo interno, per garantire l'integrità e la sicurezza dei dati personali e nell'ambito del procedimento penale (c. 5).

[225] GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile*, cit., 8 s.

[226] Art. 32 del GDPR; art. 29 della LED.

[227] Art. 32, par. 2, del GDPR; art. 29, par. 2, della LED. Sul primo, v. più ampiamente V. D'ANTONIO, *Oblio e cancellazione dei dati nel diritto europeo*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, cit., 248 ss.

dei dati[228], richiamata anche da altri principi[229] –, che sono state poi sviluppate, con riguardo ai dati biometrici trattati in occasione di videosorveglianza, dal Comitato europeo per la protezione dei dati[230] e dalle autorità nazionali di controllo[231].

La sicurezza del trattamento di dati biometrici è funzionale a evitare, innanzitutto, di incorrere nella violazione o nel furto dei dati[232]. I

[228] La pseudonimizzazione è da intendersi come «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive» (art. 4, par. 1, n. 5). In particolare, essa consiste nella sostituzione di un attributo, solitamente univoco, di un dato con un altro, ugualmente univoco e solitamente non immediatamente intellegibile. Questo accorgimento mantiene univoca l'attribuzione del dato pseudonimo ad una persona, sebbene ne renda più complessa e onerosa l'identificazione. Il risultato della pseudonimizzazione può essere indipendente dal dato iniziale, come avviene nel caso di un valore casuale assegnato a un attributo di un dato, oppure può essere calcolato a partire dal valore originale di un attributo, ad esempio, mediante l'applicazione di una tecnica crittografica. La pseudonimizzazione si differenzia quindi dalla anonimizzazione, che si basa sulla introduzione di incertezze nell'attribuzione di un dato ad un soggetto determinato tramite una nuova rappresentazione del dato. Sul punto, cfr. G. D'ACQUISTO, M. NALDI, *Big data e privacy by design. Anonimizzazione. Pseudonimizzazione. Sicurezza*, Giappichelli, Torino, 2017, 33 ss.

[229] Fra cui la limitazione delle finalità, quale condizione da considerate per un potenziale riutilizzo (art 6, par. 4, lett. e), il principio di minimizzazione e di *privacy by design* (art. 25, par. 1); su quest'ultimo v. *infra* Cap. V, par. 5.

[230] Cfr. COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 23, che richiama misure quali: trasmettere e conservare i dati in forma compartimentalizzata, conservare modelli biometrici e dati grezzi o dati di identità in banche dati distinte, cifrare i dati biometrici, in particolare i modelli biometrici, e definire una politica per la cifratura e la gestione delle chiavi, prevedere una misura organizzativa e tecnica per il rilevamento delle frodi, associare un codice di integrità ai dati (ad esempio, firma o codice *hash*) e vietare qualsiasi accesso esterno ai dati biometrici. Tali misure dovranno evolversi con il progredire delle tecnologie.

[231] In GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee-guida in materia di riconoscimenti biometrico e firma grafometrica*, cit., 26, ad esempio, si indica come i campioni o i modelli biometrici, laddove indispensabile per consentire i confronti, vadano conservati in aree di *filesystem* protette con strumenti crittografici che li rendano inintellegibili o in *database* che supportino tecniche di cifratura avanzata e con lunghezza adeguata alla dimensione e al ciclo di vita dei dati.

[232] Come accaduto, ad esempio, con i dati estratti dal riconoscimento facciale di oltre un milione di persone raccolti dalla *UK Metropolitan police*, aziende appaltatrici

dati biometrici, nello specifico, risultano particolarmente vulnerabili perché, a differenza di quanto accade con un comune documento, in caso di violazione o di furto non possono essere sostituiti dal titolare. Ne deriva che, oltre ai possibili danni economici e sociali conseguenti all'utilizzo fraudolento dei dati, si associano anche gli effetti inibitori sul comportamento rispetto a tutte quelle conseguenti cautele che devono essere adoperate di conseguenza[233].

Tra le minacce più frequenti alla sicurezza dei sistemi di riconoscimento facciale, inoltre, vi sono i furti di identità digitale[234], ovvero i tentativi di sostituirsi ad un soggetto inducendo un sistema di verificazione in un falso-positivo. Per contrastare questi atteggiamenti fraudolenti, che si risolvono in una violazione di quella che – come visto[235] – può essere considerata la proiezione dell'identità personale nello spazio virtuale, sono invalse diverse contromisure per evitare che un sistema possa essere ingannato da maschere indossate dai malintenzionati oppure dal ricorso a forme di alterazione e distorsione delle immagini digitali[236]. Da qui l'implementazione di tecniche di protezione atte a verificare che l'immagine acquisita provenga da un essere vivente[237], oppure l'integrazione di metodi multimodali di verifica che ri-

della difesa e istituti bancari, trovati pubblicati *online* su internet nell'agosto del 2019; cfr. J. TAYLOR, *Major breach found in biometrics system used by bank, UK police and defence firms*, in *The Guardian*, 14 agosto 2019 [bit.ly/3wwnotD]. Ma si consideri anche la violazione di 533 milioni di profili Facebook, contenenti nome, numero di telefono, email, relazione sentimentale, posizione lavorativa e appartenenza a gruppi Facebook, messi in vendita online, segnalata da A. DI CORINTO, *Ecco i database rubati a Facebook. Che cosa possono farne gli hacker*, in *Repubblica.it*, 15 febbraio 2021 [bit.ly/3rYxNKT].

[233] D.J. SOLOVE, D.K. CITRON, *Risk and Anxiety: A Theory of Data-Breach Harms*, in *Texas Law Review*, 96, 2018, spec. 756 ss.

[234] I. BERLE*, Face Recognition Technology*, cit., 16 ss.

[235] V. *retro* Cap. par. 2.

[236] Cfr. K. HAO, P. HOWELL O'NEILL, *The hack that could make face recognition think someone else is you*, in *MIT Technology Review*, 5 agosto 2020; Y. ALPARSLAN ET AL., *Adversarial Attacks on Convolutional Neural Networks in Facial Recognition Domain*, in *arXiv:2001.11137v3 [cs.LG]*, 8 febbraio 2021.

[237] Secondo A. ANJOS, S. MARCEL, *Counter-measures to photo attacks in face recognition: a public database and a baseline*, *International Joint Conference on Biometrics*, 2011, 1 ss., tali contromisure sono distinguibili tra analisi del movimento, in cui si ri-

chiedono il riconoscimento tramite impronte digitali oltre che tramite il volto[238]. Nonostante questi accorgimenti, tuttavia, il ricorso alle TRF non può dirsi mai del tutto innocuo, ed anche un uso legittimo e ben definito può essere esposto a seri rischi a causa di errori o cyber-aggressioni[239].

6. *I diritti conseguenti alla sottoposizione a riconoscimento facciale*

6.1. *Il diritto ad essere consapevoli e ricevere informazioni…*

La tutela dei dati personali, oltre ad offrire principi ai quali conformare il relativo trattamento, implica anche il conferimento di diritti ai soggetti interessati da esercitare anche in ipotesi di sottoposizione a riconoscimento facciale.

Il primo tra essi può essere considerato il *diritto a ricevere informazioni* da parte del titolare del trattamento prima che quest'ultimo avvenga, o comunque nel momento in cui i dati vengono prodotti. L'obiettivo è di evitare, ad esempio, che un soggetto sottoposto a videosorveglianza venga ripreso a sua insaputa[240].

Si tratta delle informazioni che, per quanto qui rileva maggiormente, il titolare del trattamento ha l'obbligo di fornire all'interessato, consentendogli di venire a conoscenza dell'esistenza di un trattamento in corso[241], di identificare il titolare stesso, di comprendere le finalità del

cercano quei movimenti percettibili o meno nei volti reali; analisi della *texture*, ovvero allenando il sistema a distinguere la trama delle pelli naturali con quelle riprodotte artificialmente; rilevamento dei segni di vita, quali il battere delle ciglia.

[238] Cfr. M.O. OLOYEDE, G.P. HANCKE, *Unimodal and Multimodal Biometric Sensing Systems: A Review*, in *IEEE access*, 4, 2016, 7532 ss.

[239] CNIL, *Facial recognition: for a debate living up to the challenges*, cit., 6.

[240] Più ampiamente, cfr. GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679*, 11 aprile 2018, che, nello specifico, chiarisce che gli artt. 13 e 14 del GDPR trovino applicazione anche quando oggetto di trattamento sono i dati che «il titolare del trattamento raccoglie presso l'interessato mediante osservazione (ad es. utilizzando dispositivi o software per catturare dati in modo automatizzato quali telecamere [...])» (15).

[241] Di converso, l'interessato ha diritto ad ottenere conferma del trattamento; v. *infra* par. 6.2.

trattamento, nonché di esercitare i diritti di cui si dirà a breve[242]. In questo modo, per quanto qui interessa sottolineare, all'interessato viene offerto un primo livello di garanzia per non subire inconsapevolmente il riconoscimento facciale.

Nel caso del GDPR, il diritto a ricevere tali informazioni può essere considerato un corollario del più ampio *principio di trasparenza*, quale novità introdotta dal regolamento[243] da intendere come sviluppo diretto della libertà di autodeterminazione informativa[244]. Il diritto in questione appare ancor più decisivo nel contesto di trattamenti diffusi che sfruttano il ricorso a nuove tecnologie la cui natura e funzionamento non sempre risultano comprensibili nella loro complessità e nella loro portata, come avviene per le TRF[245].

Nella LED, a differenza del GDPR, non è previsto invece un principio di trasparenza, giudicato incompatibile con le finalità cui è preposta[246]. Tale direttiva distingue invece tra le informazioni da «mettere

[242] Artt. 12-14 del GDPR; artt. 12-13 della LED. Anche la Convenzione 108 impone di dare informazione sulla conoscenza della «esistenza di una collezione automatizzata di dati a carattere personale, i suoi fini principali, nonché l'identità e la residenza abituale o la sede principale del responsabile della collezione» (art. 8, par. 1, lett. a). V. anche art. 9, par. 1, lett. b, della Convenzione 108+.

[243] V. spec. art. 5, par. 1, lett a, per il riferimento generale alla necessità che i dati siano trattati in modo trasparente, e art. 12 sulle modalità generali con cui occorre assolvere al dovere di informazione. Più ampiamente, nel dettaglio di tale disciplina, v. A. RICCI, *I diritti dell'interessato*, cit., 392 ss.

[244] Aspetto particolarmente sottolineato in G. DI GENIO, *Trasparenza e accesso ai dati personali*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, cit., 164 ss.

[245] Come puntualizzato in GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 10, «le persone fisiche hanno gradi diversi di comprensione e per alcune potrebbe essere difficile comprendere le complesse tecniche coinvolte nella profilazione e nei processi decisionali automatizzati». Per questo il GDPR ha introdotto l'obbligo per il titolare del trattamento di fornire all'interessato le informazioni relative al trattamento «in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro» (art. 12, par. 1). Per maggiori approfondimenti, v. GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679*, cit., 6. Sulla comprensibilità delle TRF, v. più approfonditamente *infra* par. 6.5.

[246] P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei*

a disposizione» in termini generalizzati al pubblico e le ulteriori informazioni da fornire ad un determinato interessato «in casi specifici»[247]. In questo modo, le forze dell'ordine che volessero impiegare un sistema di riconoscimento facciale in un luogo pubblico a scopi di sicurezza, dovrebbero distinguere tra le informazioni da rivolgere alla generalità dei cittadini e quelle da riservare alle persone soggette a rilevamento.

Più in generale, per rendere le informazioni più fruibili ai cittadini, viene fatta salva la possibilità di strutturare l'informativa su più livelli, con una prima segnaletica di avvertimento nell'immediatezza del luogo di acquisizione delle immagini – sia esso il varco in un aeroporto, lo stabilimento di un centro produttivo o una pubblica strada – ed una seconda con le ulteriori informazioni necessarie in formato più dettagliato[248].

Tra GDPR e LED, tuttavia, occorre segnalare un profilo di differenza significativo, che riguarda le possibili limitazioni ai diritti e ai principi introdotti dalla relativa disciplina, compreso il dovere di informativa. Mentre il regolamento rimette agli Stati la possibilità di prevedere con legge tali limitazioni, garantendo comunque che queste norme presentino determinati contenuti minimi[249], la LED ammette sì

reati, cit., 335 s. Anche se al cons. 26 c'è un riferimento alla trasparenza, a riprova che il diritto dell'interessato a ricevere informazioni sul trattamento precedentemente alla raccolta di dati personali non ha carattere assoluto, come osservato da A. RICCI, *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati*, cit., 582 s.

[247] Rispettivamente art. 13, par. 1 e par. 2, della LED.

[248] Così COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 28 ss.

[249] L'art. 23 del GDPR, al par. 1 elenca le finalità – fra cui «la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica» (lett. d) oppure «altri importanti obiettivi di interesse pubblico generale» (lett. e) – che possono giustificare la limitazione ai diritti e alle prerogative previste agli artt. da 12 a 22 e 34, nonché ai principi all'art. 5, ma al par. 2 indica i contenuti che le previsioni legislative limitative devono necessariamente assumere, ovvero: le finalità o le categorie di trattamento; le categorie di dati personali; la portata delle limitazioni introdotte; le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti; l'indicazione precisa del titolare del trattamento o delle categorie di titolari; i periodi

la possibilità di stabilire analoghe limitazioni, parametrandole alle esigenze dei procedimenti penali[250] o agli interessi pubblici di contrasto cui è preposta[251], ma non indica quali contenuti minimi la legislazione debba assumere. Ne deriva, nel complesso, una differenza sostanziale sia nei contenuti e nei limiti di tale legge limitativa[252], sia nella quantità di informazioni da rendere agli interessati, che nel caso della LED trova precisazione al d.lgs. n. 51/2018[253].

di conservazione e le garanzie applicabili; i rischi per i diritti e le libertà degli interessati; il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

[250] Art. 18 della LED.

[251] Rispettivamente art. 18 e art. 13, par. 3, con riguardo alle "informazioni ulteriori" indicate dal par. 2, della LED.

[252] Il GDPR, peraltro, prevede che le limitazioni all'art. 23 siano definite dal «diritto dell'Unione o dello Stato membro [...] mediante misure legislative», ma solo «qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica». La LED fa riferimento ad analoghe condizioni, ma solo per le limitazioni alle "informazioni ulteriori" (art. 13, par. 3), e non anche per le limitazioni ai diritti dell'interessato nel corso di indagini e procedimenti penali (art. 18).

Anche la Convenzione 108 autorizza deroghe alle previsioni concernenti, fra l'altro, i diritti dell'interessato ove ciò costituisca «una misura necessaria, in una società democratica: per la protezione della sicurezza dello Stato, per la sicurezza pubblica, per gli interessi monetari dello Stato o per la repressione dei reati» (art. 9, par. 2). La Raccomandazione n. R(87) 15, impone di informare la persona i cui dati siano stati raccolti a sua insaputa «ove possibile, e se l'oggetto dell'attività della polizia non rischi di subirne un maggiore pregiudizio» (p. 2.2).

[253] La LED, nella sua formulazione, non riconosce i diritti alla limitazione al trattamento, alla portabilità dei dati e di opposizione, in ragione delle finalità del trattamento cui è preposta. L'art. 10, c. 1, d.lgs. n. 51/2018, conseguentemente, impone di mettere a disposizione dell'interessato solo alcune informazioni, ovvero, oltre a quelle che permettono di identificare il titolare del trattamento e le finalità dello stesso, anche i diritti di: reclamo all'autorità di controllo *ex* art. 52 LED; accesso ai dati *ex* art. 11; rettifica, cancellazione, limitazione al trattamento *ex* art. 12. Le informazioni "ulteriori", invece, in quanto funzionali all'esercizio dei diritti dell'interessato, devono essere fornite solo se previsto da legge o regolamento e possono consistere in: titolo giuridico del trattamento; regime di conservazione; destinatari dei dati; ulteriori informazioni, fra cui la raccolta all'insaputa dell'interessato. Cfr. A. RICCI, *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati*, cit., 583.

In questo modo, la LED contribuisce a stabilire la misura con cui viene garantito il rispetto della "libertà morale" di una persona sottoposta a riconoscimento facciale nel corso di un procedimento penale, intesa come forma di autodeterminazione nelle proprie scelte difensive[254]. L'esempio di quanto accade Stati Uniti, tuttavia, seppure riferito ad un quadro normativo profondamente diverso, è indicativo dei rischi legati ad un uso poco trasparente di questi strumenti da parte delle forze dell'ordine, nonché dello stato di soggezione e frustrazione che questo può ingenerare nei cittadini[255].

6.2. (segue) *…quale condizione per esercitare i diritti di autodeterminazione informativa*

La consapevolezza della sottoposizione a riconoscimento facciale manifesta tutto il suo rilievo in vicende come quella scaturita dall'uso di queste tecnologie da parte della polizia di Amburgo in occasione del summit G20 del luglio 2017. In tale occasione, le forze di polizia hanno sfruttato un enorme *database* realizzato da loro stesse tramite l'acquisizione di immagini da una molteplicità di fonti, quali videoriprese nelle stazioni ferroviarie o metropolitane, foto segnaletiche delle forze dell'ordine, fino a materiali multimediali offerti dai cittadini o reperiti su internet. A tali immagini sono state applicate TRF che hanno permesso di individuare e perseguire gli autori di alcuni reati. Il Commissario per la protezione dei dati e la libertà di informazione di Amburgo, tuttavia, nel dicembre 2018 ha ingiunto loro di cancellare il *database* con i *template* biometrici, in quanto realizzati coinvolgendo una quantità considerevole di persone senza che queste ne fossero minimamente consapevoli o che fossero sospettate della commissione di alcun reato. Come sottolineato dal Commissario, inoltre, l'assenza di un fondamento legislativo non solo osterebbe al trattamento dei dati reperiti delle forze dell'ordine mediante altre fonti, ma soprattutto im-

[254] Sul punto v. *retro*, cap. II, par. 5.

[255] Come rilevato in C. GARVIE ET AL., *The Perpetual Line-Up. Unregulated Police Face Recognition in America*, cit., 58 ss., a proposito della ritrosia delle forze dell'ordine ad ammettere o rivelare l'uso di TRF. Sulle proteste legate all'impiego di queste tecnologie, v. anche *retro* Cap. II, par. 6.

pedirebbe ai cittadini di esercitare la propria pretesa a conoscere ed essere informati del trattamento e, conseguentemente, a poter ottenere tutela dei propri diritti[256].

Il diritto di ricevere informazioni si dimostra così prodromico anche alla garanzia di ulteriori diritti esercitabili a seguito di riconoscimento facciale, nei quali si sostanzia la più volte citata condizione di *autodeterminazione informativa*, che rappresenta uno degli ultimi approdi della tutela dei dati personali[257], dalla quale passa anche la tutela della propria identità digitale[258].

In questo senso, il diritto all'autodeterminazione informativa può essere specificato in due direzioni, a seconda che esiga una *aggiunta* o una *sottrazione* di dati personali e biometrici coinvolti nel riconoscimento facciale. Dal primo punto di vista, esso si esplica come potere di esigere la rappresentazione integrale della identità "frammentata" e "decontestualizzata", tramite l'integrazione o la modifica dei propri dati[259]. Dal secondo punto di vista, si può fare riferimento alla revoca

[256] Cfr. Ordinanza (*Anordnung*) 18 dicembre 2019, p. 3. Osserva T. RAAB, *Germany. Video Surveillance and Face Recognition: Current Developments*, in *European Data Protection Law Review*, 5, 2019, 544 ss., come tale ingiunzione sia stata poi impugnata di fronte al Tribunale amministrativo di Amburgo (*Verwaltungsgericht Hamburg*), che l'ha annullata con ordinanza del 23 ottobre 2019, sul presupposto, fra l'altro, che, per ravvisare una violazione della normativa dell'UE, il Commissario avrebbe dovuto valutare concretamente il trattamento operato dalle forze dell'ordine nella forma effettivamente praticata. Il Commissario ha successivamente impugnato tale decisione presso il giudice amministrativo di secondo grado (*Oberverwaltungsgericht*), con il risultato di indurre la polizia a cancellare i *database* e le immagini utilizzate. Maggiori informazioni disponibili su: [bit.ly/31WsPDP].

[257] A questo proposito, la CGUE ha inoltre determinato che il difetto di conoscenza di un trattamento di dati personali può determinare anche una lesione del contenuto essenziale del diritto ad una tutela giurisdizionale effettiva ai sensi dell'art. 47 CDFUE, in quanto preclusiva della possibilità di esercitare una serie di diritti a protezione dei propri dati personali di cui si dirà a breve; cfr. CGUE, C-362/14, *Maximillian Schrems*, cit., p. 95; CGUE, C-203/15 e C-698/15, *Tele2 Sverige AB*, cit., p. 121; CGUE, parere 1/15 (Accordo PNR UE-Canada), cit., p. 220; CGUE, C-311/18, *Data Protection Commissioner*, cit., p. 183, 187.

[258] V. *retro* Cap. II, par. 2.

[259] Entro questa logica si può considerare anche il rifiuto di un trattamento completamente automatizzato, su cui v. *infra* par. 6.3.

del consenso reso esplicitamente al trattamento, la limitazione del trattamento e la cancellazione dei dati[260].

Il presupposto per l'esercizio di questi diritti è, a sua volta. il diritto a ricevere conferma della sottoposizione ad un trattamento specifico[261] – quale risvolto dell'obbligo del titolare di fornire le informazioni suindicate – che innesca poi la possibilità di accedere ai dati personali trattati e alle informazioni relative a tale trattamento[262].

Più in particolare, il titolare dei dati ha *diritto ad accedere* ai propri dati personali oggetto di trattamento, ed eventualmente ad averne una copia, oltre che a ricevere una serie di informazioni analoghe a quelle che il titolare del trattamento ha l'obbligo di fornire secondo quanto detto in precedenza[263]. In questo caso, però, il diritto può anche essere esercitato – con riguardo specifico alle TRF – dopo che il trattamento consistente nella captazione dell'immagine o di una videoripresa è iniziato, oppure nel momento in cui l'interessato ne ha avuto notizia[264]. Condizione necessaria, inoltre, è che il trattamento sia ancora in corso,

[260] In questa logica rientra pure l'anonimizzazione, su cui v. *retro* nota 228, e l'opposizione al trattamento, il cui diritto viene sancito dall'art. 21 del GDPR, e risulta applicabile solamente nei casi in cui il trattamento è necessario per l'esecuzione di un compito di interesse pubblico (art. 6, par. 1, lett. e; unico caso rilevante ai fini del presente discorso), ovvero per il perseguimento di un legittimo interesse del titolare (art. 6, par. 1, lett. f); cfr. più ampiamente A. RICCI, *I diritti dell'interessato*, cit., 446 ss.

[261] Per la conferma dell'esistenza di un trattamento in corso v. art. 15 GDPR e art. 14 LED. V. anche l'art. 8, par. 1, della Convenzione 108, sulla comunicazione dei dati.

[262] Come sottolineato in G. DI GENIO, *Trasparenza e accesso ai dati personali*, cit., 170.

[263] V. le informazioni riportate *retro* par. 6.1. La Raccomandazione n. R(87) 15 sancisce che «La persona interessata dovrà poter ottenere l'accesso ad un archivio di polizia ad intervalli ragionevoli e senza ritardi eccessivi, in conformità con quanto previsto dal diritto interno». Ciò deve avvenire in maniera intellegibile, tanto con riguardo a contenuto, quanto alla forma di comunicazione; cfr. CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Practical guide on the use of personal data in the police sector*, cit., 7.

[264] Come riportato in GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 30, il GDPR qui «afferma che il titolare del trattamento deve fornire all'interessato informazioni sulle *conseguenze previste* del trattamento, piuttosto che una spiegazione di una *particolare* decisione». «Esercitando i diritti di cui all'articolo 15, l'interessato può prendere atto di una decisione presa nei suoi confronti, ivi compresa una decisione basata sulla profilazione».

ovvero vi sia conservazione dei dati costituiti, ad esempio, dai *template* biometrici[265].

In questo modo, l'interessato mantiene il controllo sui propri dati e, grazie alle informazioni fornite, verifica consapevolmente la legittimità del trattamento, decidendo nel caso di attivarsi[266]. Il diritto all'accesso ai dati o più in generale a conoscere l'esistenza di un trattamento, infatti, consente poi di esercitare i diritti di intervento che riguardano, segnatamente, la *rettifica* dei propri dati inesatti – come una immagine che possa risultare non adeguata se utilizzata in un processo di verificazione – e la *cancellazione* degli stessi entro determinate ipotesi[267], come ad esempio nel caso di revoca del proprio consenso o di illiceità di una videoripresa con contestuale conservazione dei dati biometrici[268].

[265] Se nessun dato è conservato o trasferito, una volta trascorso il momento del monitoraggio in tempo reale, il titolare potrebbe soltanto comunicare che nessun dato personale è più oggetto di trattamento (oltre alle informazioni generali obbligatorie di cui all'art. 13 GDPR. Se tuttavia i dati sono ancora in corso di trattamento al momento della richiesta (vale a dire se i dati sono conservati o trattati ininterrottamente in qualsiasi altro modo), l'interessato dovrebbe ricevere accesso e informazioni conformemente alle disposizioni dell'articolo 15; cfr. COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 24.

[266] A. RICCI, *I diritti dell'interessato*, cit., 397. Così facendo si tutela l'interesse a che la rappresentazione della propria persona sia rispondente alla situazione effettiva e attuale, tramite una informazione vera, completa ed aggiornata (406).

[267] Rispettivamente art. 16 GDPR sul diritto di rettifica e art. 17 GDPR sul diritto di cancellazione (o di oblio), da esercitare quando i dati non siano più necessari al trattamento, l'interessato revochi il consenso, vi sia una legittima e fondata opposizione al trattamento, i dati siano trattati illegittimamente o vadano cancellati per adempiere ad un obbligo legale (par. 1), salvo le ulteriori eccezioni previste successivamente (par. 3). Sulla distinzione tra diritto alla cancellazione e all'oblio, alla luce del comune appiattimento nella cessazione del trattamento, v. V. D'ANTONIO, *Oblio e cancellazione dei dati nel diritto europeo*, cit., 197 ss., e la bibliografia richiamata, soprattutto per una ricostruzione della elaborazione giurisprudenziale del diritto all'oblio "*off-line*" e la fondamentale sent. della Corte di giustizia, C-131/12, *Google Spain e Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 13 maggio 2014, sul diritto all'oblio "*on-line*". L'art. 16 LED limita il diritto alla cancellazione allorché l'inesattezza non possa essere accertata o i dati debbano essere conservati a fini probatori (par. 3). cfr. A. RICCI, *I diritti dell'interessato*, cit., 406.

[268] V. anche art. 9, par. 1, lett. è della Convenzione 108+. Per ulteriori considerazioni, v. *retro* par. 5.3.

Il diritto all'accesso alle informazioni personali e ai dati trattati deve però essere contemperato anche con gli interessi della sicurezza pubblica e della repressione dei reati, come stabilito in generale anche dalla Corte EDU[269]. L'introduzione da parte della LED di questi diritti è una significativa novità rispetto al regime precedente[270], sebbene anche qui, come stabilito pure dalla Convenzione 108[271], sia consentito agli Stati di limitare i diritti enunciati – introducendo il regime della c.d. "nessuna conferma, nessuna smentita"[272] – sulla base degli stessi presupposti citati sopra per limitare il diritto all'informazione[273]. Qualora siano previste tali forme di limitazione, l'interessato può richiedere di esercitare i suindicati diritti o chiedere spiegazioni sul relativo rifiuto anche tramite l'autorità di controllo (c.d. accesso indiretto)[274].

Il solo GDPR, infine, contempla anche il diritto di ottenere la *limitazione del trattamento*, entro alcune ipotesi concernenti, fra l'altro, un difetto nell'esattezza dei dati personali o come alternativa alla cancellazione degli stessi a causa della illiceità del trattamento[275]. La LED non

[269] Sull'accesso a informazioni personali in possesso dei servizi di sicurezza e la circostanza che gli interessi della sicurezza nazionale e la lotta al terrorismo prevalgano sull'interesse dei ricorrenti ad accedere alle informazioni che li riguardavano, v. Corte EDU, *Segerstedt-Wiberg e altri c. Svezia*, 6 giugno 2006, parr. 81 ss.

[270] T. MARQUENIE, *The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework*, cit., 331. Più ampiamente v. anche art. 26 del d.P.R. n. 15/2018.

[271] Anche la Convenzione 108, al pari di quanto accade per il diritto di informazione, autorizza deroghe alle previsioni concernenti i principi sopra richiamati alle medesime condizioni (art. 9, par. 2). Anche la Raccomandazione n. R(87) 15 contempla espressamente la possibilità di derogare al diritto di accesso, di correzione e cancellazione, aggiungendo «se non nei limiti in cui una tale restrizione sia indispensabile per lo svolgimento di un compito legale della polizia o necessaria per la protezione della persona interessata o dei diritti e libertà altrui» (punto 6.4). Ciò si ritiene debba essere previsto con legge, secondo indicazioni formulate in termini possibilmente dettagliati; cfr. CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Practical guide on the use of personal data in the police sector*, cit., 8.

[272] GRUPPO DI LAVORO ARTICOLO 29, *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, cit., 19 s.

[273] V. *retro* par. 6.1.

[274] Art. 17 della LED.

[275] Art. 18 del GDPR.

contempla questo diritto nell'articolato, sebbene nei considerando se ne trovi traccia e il Gruppo di lavoro "Articolo 29" abbia incoraggiato gli Stati a disciplinarne l'introduzione, come avvenuto nell'ordinamento italiano[276].

6.3. *La difesa contro gli automatismi del riconoscimento facciale*

Si è già avuto modo di sottolineare come i più recenti sviluppi delle tecnologie basate sull'IA abbiano incredibilmente aumentato il grado di autonomia delle macchine, rendendole non solo capaci di assumere decisioni in proprio, ma sempre meno dipendenti dal controllo dell'essere umano[277]. Nelle visioni più pessimistiche, un progresso tecnologico così incalzante e incontrollato condurrà ben presto alla c.d. singolarità, ovvero ad uno scenario distopico in cui i sistemi di IA diverranno autocoscienti e soppianteranno con le proprie prestazioni cognitive persino l'intelligenza umana[278].

Simili visioni, al di là della loro fondatezza o meno, rappresentano bene il timore che nel rapporto uomo-macchine il primo dei due soggetti possa diventare la parte debole – inconsapevolmente, nella peggiore delle ipotesi[279] – e pertanto debba poter esercitare sempre una forma di comando sulle seconde[280]. È per questo motivo che i diritti

[276] V. conss. 47 e 48. Tale suggerimento è stato espresso in GRUPPO DI LAVORO ARTICOLO 29, *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, cit., 22. Il d.lgs. n. 51/2010, come anticipato, contempla tale diritto (artt. 10-12).

[277] V. *retro* Cap. I, par. 3.3.

[278] Cfr. K. KURZWEIL, *The Singularity is Near: When Humans Transcend Biology*, New York, Penguin, 2005; M. SHANAHAN, *The technological singularity*, MIT Press, Boston, 2015. Fortemente critica sulla ipotesi che possa verificarsi la "singolarità", ad esempio, M.A. BODEN, *L'Intelligenza Artificiale*, cit., 144 ss. Sulla possibilità di prevedere e conseguentemente indirizzare un simile fenomeno v. anche M. TEGMARK, *Vita 3.0. Essere umani nell'era dell'intelligenza artificiale*, cit., 207 ss.

[279] Cfr. G. ZICCARDI, *Internet, controllo e libertà*, cit., 50 ss., al termine di una carrellata di esempi cinematografici che ben rappresentano questi timori.

[280] Nella letteratura fantascientifica, tale timore viene emblematicamente espresso dalle c.d. "leggi di Asimov", riprese anche in PARLAMENTO EUROPEO, *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, (2015/2103(INL)), 16 febbraio 2017, lett. t, che le richiama nei seguenti termini: (1) Un robot non può recar

fin qui richiamati devono essere considerati in relazione alle cautele verso le *decisioni completamente automatizzate*, ossia procedimenti algoritmici, come quelli che animano le TRF, che portano ad assumere una decisione nei confronti di un soggetto e che, in aggiunta, prescindono completamente dall'intervento dell'uomo. Si pensi – solo per richiamare alcuni esempi già svolti – all'utilizzo di queste tecnologie per operare verificazioni e identificazioni che possono impedire l'accesso ad un esercizio commerciale o ad un determinato servizio pubblico, come il trasporto aeroportuale; oppure possono ostare al rilascio di un documento, come un passaporto; oppure – lo si vedrà – possono precludere il riconoscimento di un certo status, come quello di rifugiato.

Questo tipo di trattamenti impongono particolari cautele[281], tanto che la normativa europea più recente introduce uno specifico regime definibile come di "*non esclusività*". In questo senso, l'interessato ha il diritto non solo di essere informato circa l'esistenza di un procedimento di tale natura che tratta i suoi dati, ma anche di ottenere l'intervento di un essere umano qualora possano derivare effetti pregiudizievoli[282].

In ragione di tali previsioni, lo spazio di intervento dell'uomo può assumere diversa intensità (c.d. *human-in-the-loop*, *human-on-the-loop*, *human-in-command*[283]), ma al fondo è riconducibile ad una serie di esi-

danno a un essere umano né può permettere che, a causa del proprio mancato intervento, un essere umano riceva danno; (2) un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non contravvengano alla Prima Legge; (3) un robot deve proteggere la propria esistenza, purché questa autodifesa non contrasti con la Prima o con la Seconda Legge (cfr. I. ASIMOV, *Circolo vizioso*, in *Astounding Science Fiction*, 1942, 100 ss.); e (0) un robot non può recare danno all'umanità, né può permettere che, a causa del proprio mancato intervento, l'umanità riceva danno.

[281] Come chiarito anche dalla Corte EDU, ad esempio, in *Gardel c. Francia*, 17 dicembre 2009, p. 62.

[282] Come ribadito anche dalla Corte di giustizia, ad esempio, nel parere 1/15, cit., par. 173, ove si stabilisce che, nel caso delle analisi automatizzate dei dati PNR previste dall'Accordo UE-Canada, dato il tasso di errore occorrente, qualsiasi risultato «deve essere sottoposto a un riesame individuale con strumenti non automatizzati prima dell'adozione di una misura individuale che produca effetti pregiudizievoli».

[283] Come riferito in EUROPEAN COMMISSION, Communication "*Building Trust in Human-Centric Artificial Intelligence*", COM(2019) 168 final, 8 aprile 2019, 4, "*Human-in-the-loop*" si riferisce all'intervento umano in ogni ciclo decisionale del sistema, che in certi casi può non essere desiderabile; "*Human-on-the-loop*" si riferisce alla pos-

genze fondamentali che si sono imposte con il diffondersi, più in generale, dei sistemi di IA che possono prescindere dall'intervento umano[284]: si vuole identificare un agente morale, per consentire ad un soggetto umano, e non ad una macchina, di assumere decisioni riguardanti la vita di altri esseri umani[285]; si cerca di creare una sorta di meccanismo umano di salvaguardia, per impedire i danni provocati dal cattivo funzionamento delle macchine; si vuole stabilire un catalizzatore di responsabilità, così da permettere di valutare le ragioni della condotta e individuare il soggetto responsabile[286]. In assenza di queste garanzie, è possibile giungere a bandire l'uso di certe tecnologie per lasciare che queste decisioni vengano prese solamente dall'uomo[287].

Il regime di non esclusività si rivolge a quelle che vengono definite «decisioni basate unicamente su un trattamento automatizzato», che secondo la normativa in parola incidono «significativamente sull'interessato»[288] e che sono destinate a produrre «effetti giuridici negativi»[289].

sibilità che l'intervento umano avvenga durante il *design* del sistema e come monitoraggio durante il suo funzionamento; "*Human-in-command*" si riferisce invece alla possibilità di vigilare sull'attività complessiva di un sistema di IA (compreso il più ampio impatto economico, sociale, etico e legale) e alla capacità di decidere come e quando usare il sistema in una situazione particolare.

[284] D. AMOROSO, G. TAMBURRINI, *I sistemi robotici ad autonomia crescente tra etica e diritto: quale ruolo per il controllo umano?*, in *BioLaw Journal*, 1, 2019, 33, 51.

[285] Osserva M. LUCIANI, *La decisione giudiziaria robotica*, in *Rivista AIC*, 3, 2018, 876, come nel caso del processo giudiziario, anche solo a livello psicologico, si sarebbe più disposti ad accettare la decisione di una macchina purché antropomorfa, piuttosto che di un mero «ammasso di metallo e plastica».

[286] Su quest'ultimo aspetto, di «centro di imputazione e di responsabilità, che sia in grado di verificare la legittimità e logicità della decisione dettata dall'algoritmo» parla Cons. St., sez. VI, sent. 13 dicembre 2019, n. 8472, 14.2 dir. (in senso conforme anche n. 881/2020).

[287] Cfr. V. THOMAS, *Report on Artificial Intelligence: Part I –the existing regulatory landscape*, 14 maggio 2018 [bit.ly/3uwmPy1].

[288] Anche la Convenzione 108+ contempla il diritto a non essere sottoposto a decisioni completamente automatizzate che incidono significativamente sull'interessato senza prendere in considerazione l'opinione dello stesso (art. 9, par. 1, lett. a). Si tratta di una importante novità delle modifiche alla originaria Convezione 108, come sottolineato da S.L. DUQUE DE CARVALHO, *Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108*, cit., 56.

[289] Art. 22, par. 1 del GDPR; art. 11, par. 1, della LED.

Il GDPR assiste ulteriormente tali previsioni con il diritto a ricevere informazioni sulla «logica utilizzata», «l'importanza» e «le conseguenze» previste[290], nonché il diritto, a particolari condizioni, persino di rifiutare che venga operato un simile trattamento[291]. Quanto al fondamento giuridico, il regolamento autorizza il ricorso a questa tipologia di trattamenti solamente se autorizzati dal diritto dell'UE o degli Stati, qualora sia necessario per la conclusione o l'esecuzione un contratto, oppure in presenza del «consenso esplicito» dell'interessato. Il titolare del trattamento deve sempre attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, ma, solo nelle ultime due ipotesi di contratto e consenso appena indicate, si attribuisce espressamente anche il diritto di esprimere la propria opinione e di contestare la decisione assunta dal sistema automatizzato[292].

La LED, invece, in ragione degli interessi pubblici alla prevenzione, indagine e repressione dei reati, non contempla il diritto a ricevere le citate informazioni[293], anche per contemperare l'esigenza di preservare l'efficacia e l'integrità di questi sistemi decisionali; neppure consente di rifiutare un trattamento che offra come garanzie il fondamento legislativo e la tutela dei diritti, né qualifica come base per ricorrere a questi trattamenti il consenso del destinatario della decisione; di converso, attribuisce sempre il diritto ad ottenere l'intervento umano[294]. Per scopi di polizia, dunque, non è possibile ottenere tali informazioni e sottrarsi ad un trattamento interamente automatizzato, purché apprestato con le adeguate garanzie tecniche, legali e la supervisione dell'essere umano.

Anche qui, però, le decisioni assunte tramite ricorso alle TRF ten-

[290] Così sulla base dell'art. 13, par. 2, lett. f, e dell'art. 14, par. 2, lett. g, del GDPR, a seconda che i dati siano raccolti direttamente presso di lui o meno. Il concetto è ribadito anche nel cons. 63.

[291] Art. 22, par. 1, del GDPR.

[292] Art. 22, parr. 3 e 4, del GDPR.

[293] Sebbene sia previsto nel cons. 38 della LED, che richiama la possibilità «di esprimere la propria opinione, di ottenere una spiegazione della decisione raggiunta dopo tale valutazione e di impugnare la decisione».

[294] Art. 11 della LED. Aspetto sottolineato anche in F. COSTANTINI, G. FRANCO, *Decisione automatizzata, dati personali e pubblica amministrazione in Europa: verso un "*Social credit system*"?*, in *Istituzioni del Federalismo*, 3, 2019,732.

dono a porre in crisi le previsioni in questione e le ulteriori garanzie ad esse connesse.

Le problematiche principali ruotano attorno alla qualifica di decisioni come basate «*unicamente*» su trattamenti automatizzati, che apre al rischio di aggirare il regime di non esclusività garantendo un intervento non significativo, o addirittura fittizio, da parte dell'essere umano. Anche se Gruppo di lavoro "Articolo 29" ha posto in guardia contro la possibilità di elusione a seguito di un coinvolgimento meramente figurativo[295], il pericolo di affidarsi acriticamente alle macchine rimane ben presente[296]. Il ricorso a TRF viene molto spesso assistito dall'intervento di un essere umano, come ad esempio avviene nelle ipotesi in cui la verifica della coincidenza tra l'immagine catturata e una immagine presente nella galleria debba essere convalidata da un agente di polizia, in modo da limitare i casi di falsi-positivi. Nella prassi, però, non è peregrino che l'essere umano si limiti solamente a confermare quanto rilevato dal sistema, o che il controllo umano necessiti a sua volta di essere sottoposto a verifica[297]. Per richiamare ipotesi già viste, si pensi a quegli arresti effettuati sulla base di riconoscimenti facciali palesemente errati, oppure agli aspiranti lavoratori che si vedono respinti ad un colloquio di assunzione per via del responso di un algoritmo[298]. Per questo in molti preferiscono fornire una *interpretazione sostanziale* del regime di non esclusività, riconducendo sotto la

[295] Stabilendo che «per aversi un coinvolgimento umano, il titolare del trattamento deve garantire che qualsiasi controllo della decisione sia significativo e non costituisca un semplice gesto simbolico. Il controllo dovrebbe essere effettuato da una persona che dispone dell'autorità e della competenza per modificare la decisione. Nel contesto dell'analisi, tale persona dovrebbe prendere in considerazione tutti i dati pertinenti»; cfr. GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 23.

[296] S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 7, 2, 2016, 92; I.S. RUBINSTEIN, *Big Data: The End of Privacy or a New Beginning?*, cit., 79.

[297] B. GREEN, Y. CHEN, *Disparate Interactions: An Algorithm-in-the-Loop Analysis of Fairness in Risk Assessments*, *Conference on Fairness, Accountability, and Transparency (FAT* '19), 29–31 gennaio 2019*.

[298] Cfr. *retro* Cap. II, parr. 7 e 8.

sua copertura anche i processi decisionali in cui l'intervento umano appare meramente formale e non esprime alcuna valutazione attiva[299]. Analoga stretta si rintraccia nella giurisprudenza del *Conseil Constitutionnel* francese, il quale ha circondato l'uso di decisioni completamente automatizzate da parte dell'autorità pubblica con una serie di garanzie a tutela del cittadino[300], e in Italia nella giurisprudenza del TAR Lazio, che si è pronunciato direttamente sul punto nella prospettiva della istruttoria nei procedimenti amministrativi[301].

[299] Cfr. già L.A. BYGRAVE, *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, in *Computer Law & Security Review*, 17, 2001, 20; G. MALGIERI, G. COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 7, 4, 2017, 251.

[300] Cfr. decisione n. 2018-765 del 12 giugno 2018, che ha posto tre condizioni all'uso di un trattamento completamente automatizzato: la decisione amministrativa deve menzionare esplicitamente che è stata adottata sul fondamento di un algoritmo e, nel caso in cui l'interessato ne faccia richiesta, l'amministrazione deve essere in grado di comunicare le principali caratteristiche della logica sottesa ad esso; tale decisione, se grava su una posizione soggettiva, deve poter essere oggetto di ricorso amministrativo, e dunque l'amministrazione adita è obbligata ad assumere la decisione senza fare più esclusivo affidamento sul sistema algoritmico; i limiti all'assunzione di una decisione interamente automatizzata si riferiscono a sistemi algoritmici che operino sul trattamento di dati sensibili. Sul punto, v. S. SASSI, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, in *Analisi Giuridica dell'Economia*, 1, 2019, 116 ss.

[301] Il riferimento va a TAR Lazio, sez. III-*bis*, sent. 10 settembre 2018, n. 9227 (in senso conforme n. 6686/2019), in cui si stabilisce come «le procedure informatiche, finanche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione, non possano mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere» (punto 5). Secondo il Giudice, alle procedure informatiche e all'algoritmo, definito come «impersonale e orfano di capacità valutazionali delle singole fattispecie concrete» (punto 3.1), va dunque riservato «un ruolo strumentale e meramente ausiliario in seno al procedimento amministrativo e giammai dominante o surrogatorio dell'attività dell'uomo» (punto 5). Diversamente si determina una violazione dei valori costituzionali agli artt. 3, 24, 97 Cost., oltre che all'art. 6 della CEDU e ad una serie di istituti e principi generali sul procedimento amministrativo contenuti nella legge n. 241/1990, quali gli istituti di partecipazione, di trasparenza e di accesso, l'obbligo di motivazione, il principio dell'interlocuzione personale e quello ad esso presupposto di istituzione della figura del responsabile del procedimento. V. ancora S. SASSI, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, cit., 119

Una riprova della immediata pertinenza dei diritti in questione rispetto al riconoscimento facciale è offerta dalla recente pronuncia del Garante della *privacy* italiano del luglio 2018 sul sistema denominato "SARI *Enterprise*" (Sistema Automatico di Riconoscimento Immagini), che ha dato il via libera al relativo impiego da parte del Ministero dell'interno. Tale sistema è in grado di stabilire l'identità di un soggetto ripreso attraverso la comparazione dell'immagine del volto con le foto segnaletiche presenti nell'archivio "A.F.I.S. – S.S.A.", contenente anche le impronte digitali[302]. Pur sfruttando un sistema automatizzato, il SARI – a detta del Garante – rappresenta comunque un «mero ausilio all'agire umano», che consente di velocizzare l'identificazione di un soggetto ricercato di cui si disponga dell'immagine facciale, ferma restando l'esigenza dell'intervento da parte dell'operatore di polizia per verificare l'attendibilità dei risultati prodotti dalla decisione automatizzata. A questo proposito, tuttavia, si potrebbe ritenere che il riconoscimento dell'esperto, per superare il vaglio di ammissibilità, debba essere condotto rigorosamente e nel rispetto delle linee guida elaborate e riconosciute dalla comunità scientifica[303].

Altra nozione delle previsioni normative in discussione da valutare attentamente è data dal riferimento ad una «*decisione*» che ricorre in

ss. Sulle oscillazioni e incertezze nella giurisprudenza del TAR Lazio sul punto, cfr. S. CIVITARESE MATTEUCCI, *«Umano, troppo umano». Decisioni amministrative automatizzate e principio di legalità*, in *Dir. pubb.*, 1, 2019, 27 ss.; A. SIMONCINI, *Profili costituzionali dell'amministrazione algoritmica*, in *Rivista trimestrale di diritto pubblico*, 4, 2019, 1149 ss. Più in generale, sul rapporto tra PA e IA, D.-U. GALETTA, J.G. CORVALÁN, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 3, 2019; C. NAPOLI, *Algoritmi, intelligenza artificiale e formazione della volontà pubblica: la decisione amministrativa e quella giudiziaria*, in *Rivista AIC*, 3, 2020, 333 ss. La successiva giurisprudenza del Consiglio di Stato, tuttavia, ha allentato le maglie di tali affermazioni, ove ha stabilito che «non può [...] ritenersi applicabile in modo indiscriminato [...] all'attività amministrativa algoritmica, tutta la legge sul procedimento amministrativo, concepita in un'epoca nella quale l'amministrazione non era investita dalla rivoluzione tecnologica»; cfr. Cons. St., sez. VI, sentt. n. 8472/2019 e n. 881/2020.

[302] Per ulteriori riferimenti, v. *infra* par. 9.

[303] Come osserva R.V.O. VALLI, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati da immagini*, in *il Penalista*, 16 gennaio 2019, riferendosi ad esempio al "*Best Practice Manual for Facial Image Comparison*" dell'*European Network of Forensic Science Institutes* (ENFSI) del gennaio 2018.

relazione ai trattamenti interamente automatizzati. Si può dubitare, ad esempio, che l'invio di un messaggio pubblicitario (o *Digital advertising*: "*ad*") mirato, sfruttando un sistema algoritmico che riconosca dal volto un soggetto come potenziale consumatore[304], possa essere considerato una "decisione" ai sensi della normativa, dal momento che non produce effetti vincolanti e che la pubblicità può benissimo essere ignorata[305].

La stessa formulazione delle previsioni inerenti il regime di non esclusività, però, non chiarisce quando un trattamento automatizzato è destinato ad incidere «*significativamente*» sulla persona dell'interessato. Tornando all'esempio appena svolto, è vero che un "*ad*" non integra tipicamente una decisione significativa, ma una strategia pubblicitaria massiccia, rivolta ai singoli individui (c.d. "*micro-targeting*") a partire – come si vedrà a breve – dalla profilazione fondata sul riconoscimento facciale, può limitare il punto di vista e la libertà di scelta dei consumatori, dei cittadini che godono del diritto all'informazione, o dei votanti che esprimono le proprie opzioni. Testimonianza diretta si ha nel fenomeno distorto delle "*filter bubbles*", ossia delle bolle in cui l'utente viene rinchiuso per vedersi rivolgere solamente informazioni e notizie conformi alle proprie opinioni e pregiudizi[306]. Perciò, non solo il libero mercato, ma anche i sistemi democratici possono essere minacciati da tecniche di decisione automatizzata di questo tipo. Si comprende quindi come il concetto di decisione "significativa" debba essere relativizzato e declinato attentamente nei diversi contesti di vita e della società[307].

[304] G. TAYLOR, *Ruti Overcomes In-Store Personalization Challenge With Opt-In Facial Recognition*, in *Retail Touch Points*, 12 gennaio 2020 [bit.ly/3cWD0ig].

[305] L. EDWARDS, M. VEALE, *Enslaving the algorithm: from a 'right to an explanation' to a 'right to better decisions'?*, in *SSRN Electronic Journal*, gennaio 2017, 46 ss.

[306] Cfr. E. PARISER, *The filter bubble: What the Internet is hiding from you*, Penguin, London, 2011, e più di recente K. SHAFFER, *Data versus Democracy: How Big Data Algorithms Shape Opinions and Alter the Course of History*, Apress, Colorado, 2019; E. LONGO, *Dai* big data *alle «bolle filtro»: nuovi rischi per i sistemi democratici*, in *Percorsi costituzionali*, 2, 2019, 29 ss.; R. MONTALDO, *Le dinamiche della rappresentanza tra nuove tecnologie, populismo, e riforme costituzionali*, in *Quad. cost.*, 4, 2019, 790 ss.; M. FASAN, *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in *BioLaw Journal*, 1, 2019, spec. 107 ss.

[307] Di questo si dimostra consapevole lo stesso GDPR, che al cons. 71 cita a titolo esemplificativo «il rifiuto automatico di una domanda di credito online o pratiche di

Quanto alle specifiche previsioni del GDPR, infine, si considerino le possibili difficoltà concrete cui va incontro l'offerta di informazioni sulla «*logica*» utilizzata nella decisione. Queste ultime presuppongono che gli algoritmi possiedano una logica, e che questa sia comprensibile all'essere umano. Non tengono conto, dunque, di come tale assunto sia destinato a sfumare nel caso di sistemi complessi di *machine learning* o – come si vedrà[308] – dietro alle opacità con cui vengono celati i sistemi algoritmici.

6.4. *Profilazione e assottigliamento del confine pubblico/privato*

La protezione dei dati personali si rivolge anche al fenomeno della *profilazione*, considerata come tecnica automatizzata «per *valutare* determinati aspetti personali relativi a una persona fisica, in particolare per *analizzare* o *prevedere* aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica»[309].

La profilazione così definita sfrutta la propensione delle *big data analytics* e degli algoritmi di *machine learning* ad elaborare dati in forma aggregata, cioè afferenti a classi o gruppi di persone. I dati e le immagini di una persona vengono raccolti tramite – come detto[310] – le più ampia varietà di fonti, ovvero le pagine web visitate, le *app* utilizzate sugli *smarphone*, l'universo di dispositivi di *Internet of Things*. Una volta collezionati, tali dati possono essere raggruppati (*clustered*) in

assunzione elettronica senza interventi umani»; previsione poi sviluppata in GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 24, che individua come esempi decisioni che influenzano le circostanze finanziarie di una persona, come la sua ammissibilità al credito; decisioni che influenzano l'accesso di una persona ai servizi sanitari; decisioni che negano a una persona un'opportunità di impiego o pongono tale persona in una posizione di notevole svantaggio; decisioni che influenzano l'accesso di una persona all'istruzione, ad esempio le ammissioni universitarie.

[308] Cfr. *infra* par. 6.5.

[309] Art. 4, par. 1, n. 4, del GDPR; art. 3, par. 1, n. 4, della LED (enfasi aggiunta).

[310] V. *retro* Cap. I, par. 3.2.

profili sulla base di singoli aspetti della persona, riferiti variabilmente al comportamento, preferenze o altri attributi. Le persone che condividono uno o più di questi attributi vengono quindi associate ad un profilo. Possedere il medesimo profilo viene considerata ragione sufficiente per ritenere che si posseggano, sulla base di calcoli probabilistici, anche altri attributi ricorrenti nel medesimo gruppo di soggetti, pur in assenza di un riscontro diretto. La decisione che riguarda direttamente il singolo, quindi, non nasce dal calcolo sui dati personali riferiti propriamente a questi, ma su quelli riferibili al profilo in comune, i cui caratteri osservabili consentono di inferire, secondo la logica tipica dei *big data*, con un certo margine di errore, la sussistenza di altri caratteri non osservabili[311].

Tramite queste tecniche di profilazione i dati personali sono utilizzati per *prevedere* i comportamenti, a seconda della probabilità che in presenza di una caratteristica ne ricorrano altre rientranti nel medesimo profilo; ma anche per *influenzare* gli stessi, ove le correlazioni riguardino la propensione di un individuo, ad esempio, a rispondere in certi modi a determinati stimoli[312]. A partire dalla disponibilità di *big data* riferibili alla popolazione in generale, dunque, le imprese o i governi riescono a stabilire le preferenze, a predire i comportamenti, a influenzare le azioni – in una parola, a sorvegliare – in una maniera inimmaginabile[313].

L'elaborazione di dati in forma aggregata viene direttamente impiegata anche nelle TRF per le citate pratiche di categorizzazione, con

[311] Più ampiamente, sul procedimento di profilazione, cfr. M. HILDEBRANDT, *Defining Profiling: A New Type of Knowledge?*, in M. HILDEBRANDT, S. GUTWIRTH (a cura di), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008, 17 ss.; V. FERRARIS, *La profilazione e i suoi rischi*, in R. BRIGHI, S. ZULLO (a cura di), *Filosofia del diritto e nuove tecnologie*, cit., 70 ss. Ulteriori considerazioni in D. CARDON, *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei* big data, Mondadori, Milano, 2016, 43; C.J. BENNETT, R.M. BAYLEY, *Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments*, in B. VAN DER SLOOT, D. BROEDERS, E. SCHRIJVERS (a cura di), *Exploring the Boundaries of Big Data*, Amsterdam University Press, The Hague-Amsterdam, 2016, 210.

[312] F. LAGIOIA, G. SARTOR, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *Federalismi.it*, 11, 2020, 89 ss.

[313] R. CALO, *Artificial Intelligence Policy: A Primer and Roadmap*, in *University of California, Davis Law Review*, 51, 2017, 421.

le quali gli algoritmi sono in grado di isolare una o più caratteristiche che consentono di costruire e ricondurre un soggetto ad un determinato profilo. La classificazione deve poi essere funzionale ad una "valutazione" che consenta di formulare previsioni o trarre conclusioni in merito a una persona specifica[314].

Anche le TRF, dunque, sono funzionali al trattamento dei dati a fini di profilazione, aprendo innanzitutto a enormi potenzialità di sfruttamento nell'economia digitale, ove diviene possibile profilare mercato, risorse umane o clientela[315], e in particolare all'interno della *platform economy*[316]. I profili possono essere costruiti – ed anche venduti, grazie all'apporto di figure professionali specializzate come i *data brokers* o i *data consultant*[317] – per condurre, come accennato sopra, campagne di *microtargeting* di massa, attraverso una offerta mirata e personalizzata di prodotti rivolta ai singoli consumatori in base alle loro specifiche caratteristiche e preferenze[318]. Simili pratiche rivelano

[314] Come specificato in GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 7, la semplice classificazione di persone basata su caratteristiche note quali età, sesso e altezza non determina necessariamente una profilazione. Quest'ultima dipende infatti dalla finalità della classificazione.

[315] Come osserva P. PACILEO, *Profilazione e diritto di opposizione*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, cit., 179, è possibile profilare: le risorse umane, attraverso valutazione di potenziali capacità individuali, capacità relazionali, motivazione e gradi di soddisfazione personale; il mercato, semplificandone il processo di conoscenza, mappatura concettuale e analisi di posizionamento, e analizzando la concorrenza, fattori strategici di successo e la clientela potenziale; la clientela, tramite creazione dinamica di profili comportamentali di clienti già acquisiti o potenziali con la quale realizzare *offering* mirato.

[316] Cfr., di recente, A. CANEPA, *I mercanti nell'era digitale. Un contributo allo studio delle piattaforme*, Giappichelli, Torino, 2020.

[317] I c.d. *data brokers*, o i c.d. *data resellers*, sono terze parti che raccolgono i dati delle persone da una molteplicità di fonti, li elaborano allo scopo di creare profili, senza avere una relazione diretta con gli interessati, lasciando spesso questi ultimi all'oscuro del fatto che i loro dati siano trasferiti o venduti ad altri soggetti. I secondi offrono servizi di consulenza allo scopo di creare o ampliare i *dataset* esistenti; cfr. J. BRILL, *Demanding Transparency from Data Brokers*, in *The Washington Post*, 15 agosto 2013 [bit.ly/3cZM5a5].

[318] È rilevante notare come il 2019 segna l'anno in cui, negli Stati Uniti, le imprese hanno speso di più per pubblicizzare i propri prodotti tramite "Ads" che tramite i

una elevata capacità manipolativa di mercato e delle abitudini dei consumatori[319]: «i processi automatizzati non solo *conoscono* i nostri comportamenti, ma li *formano*»[320].

La profilazione, inoltre, consente anche una gestione di dati, informazioni e preferenze personali tale da riuscire a condizionare i sistemi democratici, come visto a proposito delle "*filter bubbles*", e persino la libera espressione del voto – il pensiero corre allo scandalo della società "Cambridge Analytica", legato alle elezioni presidenziali negli USA del 2016 e al referendum sulla Brexit dello stesso anno[321].

mezzi tradizionali di diffusione delle informazioni, come giornali, radio o televisione; cfr. K. WAGNER, *Digital advertising in the US is finally bigger than print and television. TV and newspapers are out. Facebook and Google are in*, in *Vox*, 20 febbraio 2019 [bit.ly/3dOneFs]. Per l'Italia, v. la relazione alla Camera dei Deputati per il 2019 del presidente Agcom Angelo Marcello Cardiani, che sottolinea come le piattaforme digitali aumentano «i loro ricavi a doppia cifra da molti anni avviandosi a valicare, in termini di valore, i 3 miliardi di euro». «Nelle telecomunicazioni tra il 2011 e il 2018 si sono persi circa un quarto dei ricavi. Nello stesso periodo, nel settore media il trend fortemente negativo dei ricavi pubblicitari ha trascinato in rosso i conti della tv in chiaro (-13% il valore economico del settore)». «Il settore editoriale ha proseguito una fase di vero e proprio declino strutturale con un calo generalizzato di valore economico (-40%), investimenti, occupazione, ricavi». Un indicatore economico in crescita, invece, «riguarda il mercato della raccolta della pubblicità online, le cui risorse sono passate dai 1407 milioni del 2011 agli oltre 2700 milioni del 2018 (+93%)»; cfr. CAMERA DEI DEPUTATI, XVIII legislatura, *Relazione sull'attività svolta e sui programmi di lavoro dell'Autorità per le garanzie nelle comunicazioni*, doc. CLVII n. 2, 7 ss.

[319] Gli interessi economici dietro una profilazione sempre più accurata trovano inoltre riscontro in quel fenomeno che viene definito come "*digital market manipulation*", ovvero una sorta di manipolazione attraverso offerte mirate che altera le scelte del consumatore facendolo deviare da decisioni razionali; cfr. R. CALO, *Digital Market Manipulation*, in *George Washington Law Review*, 82, 2014, 995 ss.

[320] Cfr. S. ZUBOFF, *Il capitalismo della sorveglianza*, cit., 18.

[321] Come noto, ci si riferisce a quella società i cui *data analysts* hanno lavorato per lo staff di Donald Trump e per la "*Vote Leave Campaign*" a favore della Brexit, e che, a partire dal 2014, ha operato su Facebook una massiccia raccolta di informazioni personali per profilare circa 87 milioni di utenti e indirizzare loro avvisi politici mirati. Questa raccolta, realizzata senza una autorizzazione diretta degli utenti, ma tramite una app per test psicologici, ha costretto i vertici di Facebook, tra cui il CEO Mark Zuckerberg, ad ammettere uno dei *data breach* più consistenti della storia. Il motto di Cambridge Analytica è, significativamente, "*Data drives all that we do*". Cfr. C. CADWALLADR, E. GRAHAM-HARRISON, *Revealed: 50 million Facebook profiles harvested for*

Più in generale, dunque, il riconoscimento facciale e le tecnologie biometriche favoriscono quei fenomeni di trasformazione dei corpi umani in flussi di dati e di informazioni, attraverso cui – come visto[322] – le molteplici identità digitali possono essere frammentate, riconfigurate e funzionalizzate alla creazione di diversi profili.

La normativa sulla protezione dei dati personali sembra cogliere queste potenzialità nella misura in cui distingue tra processi decisionali basati sulla profilazione, riconducibili alla disciplina generale sulla protezione dei dati personali, e le decisioni basate «unicamente» sul trattamento automatizzato, compresa la profilazione, che rispondono a condizioni più stringenti[323]. In quest'ultimo caso, il riferimento va al regime generale stabilito per il trattamento completamente automatizzato di dati personali – come richiamato sopra, con i limiti evidenziati – in termini di divieto generale, salva la sussistenza delle condizioni ivi previste[324]. Non solo, ma nel caso in cui tali trattamenti processino dati biometrici, come nel caso delle TRF, occorre – riprendendo le parole del GDPR e della LED – che «siano in vigore misure adeguate» poste «a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato»[325]. In aggiunta, la LED prevede che sia fatto divieto

Cambridge Analytica in major data breach, in *The Guardian*, 17 marzo 2018 [bit.ly/3cZb0KK]; M. ROSENBERG, N. CONFESSORE, C. CADWALLADR, *How Trump Consultants Exploited the Facebook Data of Millions*, in *The New York Times*, 17 marzo 2018 [nyti.ms/3t2xVdJ]. Il Garante della *privacy* italiano ha multato Facebook per 1 milione di euro in relazione alla vicenda richiamata. che ha interessato più di 200.000 utenti italiani; v. Ordinanza ingiunzione nei confronti di Facebook Ireland Ltd e Facebook Italy s.r.l., 14 giugno 2019.

[322] Cfr. *retro*, Cap. III, parr. 2 e 4.

[323] I due concetti non sono sovrapponibili, poiché, come osservato in GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 8 s., le decisioni automatizzate possono essere prese ricorrendo o meno alla profilazione, la quale a sua volta può essere svolta senza che vengano prese decisioni automatizzate.

[324] Più approfonditamente, v. anche E. PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, in *Le nuove leggi civili commentate*, 5, 2018, 1210 ss.

[325] Art. 22, par. 4, del GDPR, che ammette tale ipotesi solo se il trattamento dei dati biometrici ha come fondamento il consenso esplicito dell'interessato o risulti ne-

esplicito di sfruttare tecniche di profilazione che provochino effetti discriminatori[326].

Ne consegue, per limitarsi ad un esempio, che indirizzare le attività di polizia nei confronti di gruppi o soggetti a partire dalla loro religione sarebbe di per sé illegittimo. Tuttavia, in una indagine nei confronti di attività terroristiche perpetrate da appartenenti a determinati gruppi religiosi radicalizzati, potrebbe avere una sua necessità e risultare proporzionato trattare dati sensibili degli appartenenti ad un gruppo religioso attraverso una profilazione basata sulle medesime pratiche confessionali, la frequentazione degli stessi luoghi di culto o degli istituti di formazione[327]. Si tratta comunque di una pratica che deve ispirarsi alla massima cautela, come puntualizza la Corte di giustizia quando richiede che il trattamento in forma automatizzata dei dati sensibili – tra i quali, si ricorda, rientrano i dati biometrici – avvenga nel rispetto di una legge che fissi le condizioni «in termini rigorosi» e del canone di proporzionalità, per limitare l'ingerenza sui diritti «allo stretto necessario»[328].

Anche in ordine alla profilazione, tuttavia, la garanzia effettiva dei diritti ricavabili dal regime di non esclusività manifesta alcuni aspetti problematici. Oltre a quanto osservato più in generale sui trattamenti interamente automatizzati, bisogna considerare come l'estensione di tale regime apparirebbe troppo ristretto rispetto alle *big data analytics*, nella misura in cui non coprisse le attività preparatorie al processo decisionale vero e proprio, come la creazione dei criteri di profilazione[329].

cessario per motivi di interesse pubblico, alle condizioni previste dall'art. 9. V. anche art. 11, par. 2, della LED. Anche nell'ambito degli strumenti di protezione del Consiglio d'Europa la profilazione basata su dati sensibili è generalmente proibita, a meno che questi dati non siano necessari e proporzionati rispetto allo scopo specifico del trattamento e nella misura in cui la legislazione nazionale assicuri adeguate garanzie; cfr. CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Practical guide on the use of personal data in the police sector*, cit., 5.

[326] Art. 11, par. 3, della LED.

[327] Più ampiamente, sulla profilazione in generale, anche con riguardo alle attività di contrasto e gestione delle frontiere, v. FRA, *Preventing unlawful profiling today and in the future: a guide*, cit.

[328] CGUE, parere 1/15 (Accordo PNR UE-Canada), cit., p. 141 s.; CGUE, C-311/18, *Data Protection Commissioner*, cit., p. 176; e giurisprudenza ivi citata.

[329] M. BUTTERWORTH, *The ICO and artificial intelligence: The role of fairness in the GDPR framework*, in *Computer Law and Security Review,* 34, 1, 2018, 264.

Tale creazione, anche nel caso della categorizzazione operata tramite riconoscimento facciale, può avvenire a sua volta in maniera automatizzata, per il tramite di sistemi di *machine learning* che raggruppano i dati ricavati da immagini facciali accomunate da specifiche caratteristiche[330], operando – come detto[331] – in maniera inintelligibile per l'essere umano. Da qui la necessità che l'algoritmo venga progettato valutando accuratamente le variabili considerate o i dati con cui venire allenato, apprestando le cautele necessarie ad evitare che si producano, anche inconsapevolmente, possibili distorsioni ed effetti discriminatori[332].

A fronte di queste criticità, tuttavia, rimane un aspetto su cui conclusivamente si vuole attirare l'attenzione, e cioè la capacità della profilazione, specie se abbinata alle TRF, di assottigliare il confine tra dimensione pubblica e dimensione privata della vita di una persona. Tanto le autorità pubbliche quanto le piattaforme che operano sul *web*, possono impiegare la profilazione per massimizzare la propria capacità di sorveglianza ai più vari scopi, siano essi commerciali, di sicurezza pubblica o politici[333]. Queste tecniche, infatti, hanno raggiunto un livello di sofisticatezza ed efficienza tale da riuscire a ricollegare i dati acquisibili nel mondo reale, come una semplice immagine facciale catturata con discrezione in uno spazio pubblico, con la miriade di dati e informazioni presenti sul *web*, sia che queste vengano pubblicate consapevolmente, come avviene sui *social network*, sia che vengano generate dalle più varie forme di interazione svolte "in privato" su internet (a partire dai siti visitati o dagli acquisti effettuati), anche sotto forma di metadati (dati su altri dati, come ad esempio la durata o il luogo in cui è avvenuta la connessione), di semplici "tracce" lasciate o di "scarti" prodotti (c.d. *data exausted*, come la durata di visualizzazione di una pagina web o il modo con cui viene mosso il cursore del *mouse*), che vengono raccolte da qualcuno o da qualche dispositivo artificiale (c.d. *bots*)[334]. In questo modo, una semplice immagine del vol-

[330] F. LAGIOIA, G. SARTOR, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, cit., 88.

[331] Cfr. *retro* Cap. I, par. 3.3.

[332] Cfr. *infra* par. 7.

[333] N.M. RICHARDS, *The Dangers of Surveillance*, cit., 1958 ss.

[334] Cfr. V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data: A Revolution that will Transform How We Live, Work and Think*, cit., 234 ss.

to, attraverso la combinazione con dati apparentemente "neutri", personali o sensibili, può offrire il tramite per stilare quasi all'istante profili personali approfonditi[335]. La garanzia della *privacy* e dell'anonimato nello spazio pubblico, così, diventa sempre più illusoria.

Si tratta di potenzialità che le imprese non si lasciano certo sfuggire[336], sebbene se ne intuiscano anche le pericolosità. Paradigmatica al riguardo è la produzione e la libera commercializzazione di occhiali "*smart*" che integrano TRF, inizialmente sospese per i rischi cui i diritti e le libertà delle persone vengono esposti[337], ma oggetto di interesse sempre maggiore da parte del mercato[338]. Simili riguardi, però, non vengono mostrati da quei regimi politici in grado di dispiegare sistemi di sorveglianza capillari, come avviene per l'oramai famoso e controverso "*Social Credit System*" cinese[339]. Attraverso questa "infrastruttura di sorveglianza di Stato"[340], che combina anche TRF, a ciascun cittadino è attribuito un numero identificativo e, grazie alle informazioni raccolte in maniera automatizzata sulla vita pubblica e privata, viene associato un punteggio che ne qualifica l'affidabilità e ne oggettiva la reputazione. L'obiettivo del governo è quello di riuscire a orientare il comportamento di massa di persone, imprese e organizzazioni attraverso un sistema di benefici e sanzioni[341].

[335] Come dimostrano i risultati degli esperimenti riportati in A. ACQUISTI, R. GROSS, F. STUTZMAN, *Face recognition and privacy in the age of augmented reality*, in *Journal of Privacy and Confidentiality*, 6, 2, 2014, 1 ss.

[336] B. PEARSON, *3 Ways Retailers Can Use Facial Recognition To Create Better Experiences*, in *Forbes*, 15 marzo 2018 [bit.ly/3rTBXUx].

[337] C. ARTHUR, *Google 'bans' facial recognition on Google Glass - but developers persist*, in *The Guardian*, 3 giugno 2013 [bit.ly/3sYTHil].

[338] S. RODRIGUEZ, *Facebook is 'looking at' facial recognition technology for upcoming smart glasses, executive confirms*, in *CNBC*, 25 febbraio 2021 [cnb.cx/2OuN0px].

[339] Cfr. *retro* alla Introduzione.

[340] Cfr. F. LIANG, V. DAS, N. KOSTYUK, M.M. HUSSAIN, *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, in *Policy and Internet*, 4, 10, 2018, 415 ss., cui si rinvia anche per le tappe che hanno portato alla costruzione di questo sistema, a partire dal documento intitolato "*Planning Outline for the Construction of an SCS*", pubblicato nel 2014 da parte dello *State Council*, e dalle iniziative assunte dalle imprese commerciali.

[341] Il sistema analizza e aggrega le informazioni relative alla sfera pubblica e privata dei cittadini e a ciascun comportamento, in ambito finanziario (es. pagamenti delle

Tra le tecniche di sorveglianza di massa, dunque, la profilazione supportata da TRF, specie se combinata con trattamenti decisionali completamente automatizzati, si conferma uno dei mezzi più potenti e pervasivi, che venga praticata da governi o imprese private, che abbia come destinatari cittadini, consumatori o lavoratori, oppure che si giustifichi per motivi di sicurezza pubblica, finalità commerciali o scopi di selezione[342]. Occorre però essere consapevoli che la capacità di prevedere e influenzare i comportamenti, o l'assottigliamento del confine tra dimensione pubblica e privata che ne consegue, siano in grado di riverberarsi, direttamente o indirettamente, su pressoché tutti i diritti e le libertà fin qui trattati.

6.5. *La "comprensibilità" delle TRF*

Uno sviluppo del citato principio di trasparenza e del regime di non esclusività delle decisioni algoritmiche può essere considerato il diritto alla c.d. *explainability*, o comprensibilità[343], del sistema di riconoscimento facciale. Ad esso può essere ricollegato – seppur in termini

rate del mutuo), politico (es. partecipazione a manifestazioni), commerciale (es. abitudini di acquisto), giudiziario (es. condanne riportate), sociali (es. attività sui *social media*), assegna un punteggio, che può essere positivo o negativo. Il totale definisce il credito sociale di ciascun cittadino, in relazione al quale questi potrà o meno beneficiare di alcuni servizi pubblici (es. trasporti pubblici, iscrizione all'università) e privati (es. iscrizione ad agenzie matrimoniali), ambire a concorsi pubblici, ottenere finanziamenti, ecc. Cfr. F. COSTANTINI, G. FRANCO, *Decisione automatizzata, dati personali e pubblica amministrazione in Europa: verso un "*Social credit system*"?*, cit., 715 ss.; F. LAGIOIA, G. SARTOR*, Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, cit., 105 ss. Osserva G. KOSTKA, *China's social credit systems and public opinion: Explaining high levels of approval*, in *New media & society*, 21, 7, 2019, 1565 ss. (spec. 1573), come vi sia una larga approvazione da parte della popolazione cinese di questo sistema (80% degli intervistati), mentre solo una minoranza rimane indifferente (19%) o fortemente contraria (1%).

[342] D. LYON, *La società sorvegliata*, cit., 25 ss. e 46 ss.

[343] Si preferisce non utilizzare altri termini cui si fa ricorso anche in documenti ufficiali, come "spiegabilità" (utilizzato, ad esempio, in PARLAMENTO EUROPEO, *Una politica industriale europea globale in materia di robotica e intelligenza artificiale*, cit., p. 149) o "esplicabilità" (utilizzato, ad esempio, in GRUPPO DI ESPERTI AD ALTO LIVELLO SULL'INTELLIGENZA ARTIFICIALE, *Orientamenti etici per un'IA affidabile*, cit., 2), che nella lingua italiano non sono propriamente di uso comune.

problematici, come si vedrà – il diritto di comprendere non solo l'architettura e le caratteristiche del processo decisionale cui si è sottoposti, ma anche i criteri adoperati e le ragioni alla base delle singole decisioni cui si è soggetti[344].

L'obiettivo del diritto alla comprensibilità è scoprire la specifica "visione del mondo"[345] di cui si fanno portatori gli algoritmi, alla luce della radicale diversità che – come visto – distingue il pensiero che anima l'essere umano e i calcoli che muovono le macchine[346]. Così facendo, trovano soddisfazione molteplici interessi. Si pensi innanzitutto alla necessità che le persone sottoposte a TRF sviluppino fiducia nei confronti di questi strumenti, dato che non soltanto la sicurezza, ma soprattutto la percezione della sicurezza costituisce un presupposto necessario per rendere più accettabile l'impiego di una tecnologia e instaurare un rapporto collaborativo con essa[347]. La comprensibilità è utile anche per favorire la circolazione delle informazioni e migliorare la ricerca e sviluppo in questo settore, alimentando il dibattito della comunità scientifica e degli esperti. Non da ultimo, su un piano propriamente giuridico, la comprensibilità si rende necessaria per consentire di adire i rimedi più adeguati nel caso di lesione di diritti fondamentali e per riconoscere le responsabilità giuridiche derivanti dalle conseguenze della sottoposizione a riconoscimento facciale[348], ad esempio, in caso di malfunzionamento[349].

[344] Anche il Parlamento europeo sottolinea l'importanza «della spiegabilità dei risultati, dei processi e dei valori dei sistemi dell'IA, in modo da renderli comprensibili per un pubblico non tecnico e fornire a quest'ultimo informazioni significative, condizione necessaria per valutare l'equità e conquistare la fiducia»; cfr. PARLAMENTO EUROPEO, *Una politica industriale europea globale in materia di robotica e intelligenza artificiale*, cit., p. 161.

[345] D. CARDON, *Che cosa sognano gli algoritmi*, cit., 6.

[346] Cfr. *retro* Cap. I, par. 3.1.

[347] Cfr. W. PIETERS, *Explanation and trust: What to tell the user in security and AI?*, in *Ethics and Information Technology*, 13, 2011, 53 ss., che distingue la conoscibilità nei due profili della trasparenza, per consentire agli utenti di comprendere cosa i programmatori hanno fatto per strutturare il sistema, e giustificazione, per fornire le ragioni di una specifica azione.

[348] Cfr. L. MITROU, *Data Protection, Artificial Intelligence and Cognitive Services. Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?*, cit., 54; M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges*, cit., 48.

[349] È il grande tema della responsabilità per l'utilizzo dei sistemi di IA, ovvero

Il principale ostacolo alla comprensibilità dei sistemi di riconoscimento facciale è costituito dalla opacità delle c.d. "*black box*", entro cui vengono nascosti i processi decisionali algoritmici per renderli inaccessibili all'esterno[350]. Tale opacità, però, può trovare spiegazione in una molteplicità di ragioni[351]. In parte, si giustifica con la inevitabile complessità degli algoritmi di *machine learning* e del linguaggio tecnico-informatico utilizzato per scriverli, che impedisce ai non esperti di comprendere i codici utilizzati. Allo stesso tempo, l'opacità nasce dalla discrepanza tra la semantica umana e il linguaggio degli algoritmi, rispetto ai quali ci possono essere diversi livelli di trasparenza. Tuttavia, l'algoritmo può essere tenuto in tutto o in parte celato per scelta deliberata, allo scopo di non compromettere l'efficacia del sistema a tutela

come colmare il c.d. "*responsibility*" o "*liability gap*", che origina dalle condotte di questi sistemi, per il quale si rinvia a E. TJONG TJIN TAI, *Liability for (Semi)Autonomous Systems: Robots and Algorithms*, in V. MAK, E. TJONG TJIN TAI, A. BERLEE (a cura di), *Research Handbook on Data Science and Law*, Edward Elgar, Cheltenham-Northampton, 2018, 55 ss.; G. PASSAGNOLI, *Il diritto civile al tempo dell'intelligenza artificiale: spunti per una problematizzazione*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., 71. Più ampiamente sulla tematica, si veda anche G. GUERRA, *La sicurezza degli artefatti robotici in prospettiva comparatistica. Dal cambiamento tecnologico all'adattamento giuridico*, il Mulino, Bologna, 2018. Ci si limita qui a osservare come le soluzioni oscillino prevalentemente tra un riconoscimento di "soggettività giuridica piena" a questi sistemi tecnologici, che porrebbe problemi giuridici ed etici forse insuperabili, e attribuire loro una "soggettività giuridica parziale", la quale non attesta alcuna equiparazione sul piano ontologico del relativo titolare, bensì, prescindendo dal sostrato antropomorfico, conferisce una personalità "determinata funzionalmente", che costituisce il sistema di IA come centro di imputazione di diritti e obblighi solamente a determinate finalità. Sul punto, più approfonditamente, v. anche G. TEUBNER, *Soggetti giuridici digitali*, ESI, Napoli, 2019, 32 ss.; U. RUFFOLO, *La "personalità elettronica"*, in ID. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., 213; A. SANTOSUOSSO, *Intelligenza artificiale e diritto*, cit., 202 ss.

[350] Cfr. F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information,* Harvard University Press, Cambridge-London, 2015.

[351] M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges*, cit., 49; J. BURRELL, *How the machine 'thinks': Understanding opacity in machine learning algorithms*, in *Big Data & Society*, 3, 1, 2016, 1 ss.; J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YU, *Accountable Algorithms*, in *University of Pennsylvania Law Review*, 165, 2017, 638 s.

della sicurezza pubblica; per garantire la sicurezza del sistema e non esporsi ad attacchi informatici; ma anche per esigenze di proprietà intellettuale, per proteggere interessi commerciali e concorrenziali. Non di rado, questa opacità può servire anche a celare gli interessi dei soggetti che fanno ricorso a procedimenti decisionali algoritmici e rendere imperscrutabile l'uso effettivo che viene fatto dei dati[352], finanche per garantire una posizione di dominio, mantenere una forma di controllo e assicurarsi la possibilità di sfruttamento su – le informazioni di – utenti e soggetti destinatari delle decisioni algoritmiche[353].

Per contrastare gli abusi che si celano dietro questa opacità è nato un movimento scientifico volto a sviluppare una "*Explainable Artificial Intelligence*" (XAI)[354], che mira ad individuare una serie di interrogativi cui deve rispondere un algoritmo per poter essere "*explainable*"[355].

Come messo in luce dalla letteratura informatica specialistica, tuttavia, la *explainability*, o *interpretability* di un sistema di IA, è un concetto relativo, che cambia a seconda di numerosi fattori: il soggetto che vuol conoscere un certo sistema; il suo grado di conoscenza tecnologica; le finalità per cui si vanta questa pretesa; il linguaggio con cui si chiede di rendere le spiegazioni; se la spiegazione debba essere riferita all'architettura dell'intero sistema o ad una singola decisione e agli interessi con essa toccati[356]. Le variabili considerate dall'algoritmo e le

[352] F. PASQUALE, *The Black Box Society*, cit., 4 ss.

[353] Il riferimento va a S. ZUBOFF, *Il capitalismo della sorveglianza*, cit.

[354] Questo programma ha recentemente trovato slancio anche grazie ad un programma finanziato dalla *Defense Advanced Research Projects Agency* (DARPA) degli Stati Uniti, su cui v. i riferimenti in L. VIGANO, D. MAGAZZENI, *Explainable Security*, cit.

[355] Cfr. ad esempio B. WALTL, R. VOGL, *Explainable Artificial Intelligence – the New Frontier in Legal Informatics*, in *Jusletter IT*, 22 febbraio 2018, che a partire dal lavoro di D. GUNNING, *Explainable Artificial Intelligence (XAI)*, 2017, formulano le seguenti domande, successivamente specificate: «Why did that output happen? Why not some other output? For which cases does the machine produce a reliable output? Can you provide a confidence score for the machine's output? Under which circumstances, i.e. state and input, can the machine's output be trusted? Which parameters effect the output most (negatively and positively)? What can be done to correct an error?».

[356] Cfr. D. FINALE, B. KIM, *A Roadmap for a Rigorous Science of Interpretability*, in arXiv:1702.08608v2, marzo 2017; L. VIGANO, D. MAGAZZENI, *Explainable Security*, in arXiv:1807.04178 [cs.CR], 2018.

inferenze realizzate, poi, non sempre sono intellegibili all'uomo[357]. Accanto a questi fattori, inoltre, bisogna anche considerare che spesso più un algoritmo è complesso, più sarà accurato nei compiti che dovrà svolgere, ma meno sarà comprensibile e facilmente spiegabile[358]. La comprensibilità, dunque, non può essere concepita in astratto, ma deve sempre considerare il contesto ed essere tarata sul singolo procedimento decisionale, il soggetto interessato e la situazione specifica entro cui viene assunta la decisione algoritmica.

Volendo ricondurre il diritto alla comprensibilità delle TRF ad un dato normativo vigente, occorre osservare che né il GDPR, né tantomeno nella LED, contengono espressamente l'enunciazione del diritto in questione, dal momento che un accenno alla comprensibilità risulta solo dal considerando 71 del GDPR, le cui previsioni, sebbene esercitino una valenza interpretativa[359], non hanno avuto la forza di entrare nell'articolato in termini vincolanti[360]. Per questo, sulla base di una interpretazione restrittiva del GDPR assistita anche dai lavori preparatori, si è giunti ad escludere la configurabilità di un vero e proprio diritto a ottenere una spiegazione *ex post* sulla singola decisione, potendosi tutt'al più parlare di un diritto "ad essere informati" *ex ante* sull'esistenza di un processo decisionale automatizzato e sulla logica utilizzata[361].

[357] L. EDWARDS, M. VEALE, *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You are Looking for*, in *Duke Law & Technology Review*, 16, 1, 2017, 59 s.

[358] D. BAMMAN, *Interpretability in Human-Centered Data Science*, CSCW Workshop on Human-Centered Data Science, 2016 [bit.ly/3mufqw8], che pone in luce il *trade-off* tra *predictive accuracy*, *interpretability* e *representational complexity*.

[359] Al pari degli altri considerando, anche questo è parte integrante del regolamento e ha una valenza di indirizzo interpretativo, ma non ha una efficacia propriamente vincolante, come sottolineato, tra l'altro, da C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, cit., 90 s.

[360] Il trattamento automatizzato «dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore». L'uso del "dovrebbe", però, è certamente foriero di ambiguità; cfr. L. EDWARDS, M. VEALE, *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You are Looking for*, cit., 50.

[361] S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explanation of Au-*

Tuttavia, tale conclusione non sarebbe affatto univoca, specie se si volesse privilegiare una interpretazione non limitata al solo dato letterale. A detta di altri, infatti, un diritto alla comprensibilità si potrebbe fondare attraverso una interpretazione funzionale alla tutela e all'esercizio dei diritti dell'interessato fin qui richiamati[362]. Sempre accedendo ad una interpretazione sistematica, è stata anche avanzata l'ipotesi che il GDPR garantisca una "*legibility*" di *data* e *analytic algorithms*, intesa come comprensibilità e trasparenza tanto dell'architettura, quanto dell'implementazione del procedimento decisionale algoritmico[363].

Sul punto, inoltre, non mancano atti di *soft law* tesi a forzare la portata precettiva della disciplina a tutela dei dati personali, come testimoniato dalla risoluzione del Parlamento europeo del 2017 che concepisce la trasparenza a partire dal «fatto che dovrebbe sempre essere possibile indicare la logica alla base di ogni decisione presa con l'ausilio dell'intelligenza artificiale che possa avere un impatto rilevante sulla vita di una o più persone», e che «debba sempre essere possibile ricondurre i calcoli di un sistema di intelligenza artificiale a una forma comprensibile per l'uomo»[364]. Analogamente, il Gruppo di lavo-

tomated Decision-Making Does Not Exist in the General Data Protection Regulation, cit., 76 ss.

[362] Cfr. B. GOODMAN, S. FLAXMAN, *European Union Regulations on algorithmic decision-making and a "Right to Explanation"*, in *AI Magazine*, 38, 3, 2017, 6, secondo cui il diritto di conoscibilità si potrebbe ricavare dal combinato disposto dei citati artt. 13 e 14 (obbligo di notifica), art. 22 (divieto di essere sottoposto a decisione automatizzata), cui si affiancano il diritto di accesso (art. 15) e diritto a ottenere le informazioni riguardanti il trattamento (art. 12). Analogamente A.D. SELBST, J. POWLES, *Meaningful information and the right to explanation*, in *International Data Privacy Law*, 7, 2017, 235 ss., fanno leva sul concetto di informazioni «significative» sulla logica utilizzata, di cui agli artt. 13, 14 e 15, nel senso che tali informazioni devono essere significative non in astratto, ma per l'interessato, il quale non necessariamente possiede conoscenze tecniche specialistiche, e che invece deve poterne godere in funzione di esercitare specifici diritti, come la possibilità di contestare la decisione sancita all'art. 22, par. 3, o di comprendere le «conseguenze previste di tale trattamento».

[363] G. MALGIERI, G. COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, cit., 245 ss.

[364] PARLAMENTO EUROPEO, *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, cit.

ro "Articolo 29" ha stabilito che «il titolare del trattamento dovrebbe trovare modi semplici per comunicare all'interessato la logica o i criteri sui quali si basa l'adozione della decisione [...] ma non necessariamente una spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo. Le informazioni fornite dovrebbero tuttavia essere sufficientemente complete affinché l'interessato possa comprendere i motivi alla base della decisione»[365].

Tracce di simili aperture si ritrovano significativamente anche nella giurisprudenza italiana, come quella più recente del Consiglio di Stato con cui viene data una lettura del "diritto di conoscibilità" come declinazione del principio di trasparenza, riferita a tutti gli aspetti dell'algoritmo[366]. Nelle pronunce che si collocano in questo filone, inoltre, si prende posizione pure nei confronti delle *black box*, la cui

[365] GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 28.

[366] Cfr. Cons. St., sez. VI, sent. 8 aprile 2019, n. 2270 (in senso conforme nn. 8472/2019 e 881/2020), ove si legge che «il meccanismo attraverso il quale si concretizza la decisione robotizzata (ovvero l'algoritmo) deve essere "conoscibile", secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico. Tale conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti» (8.3 dir.). In questo modo può essere anche «garantita la verifica a valle, in termini di logicità e di correttezza degli esiti. Ciò a garanzia dell'imputabilità della scelta al titolare del potere autoritativo, individuato in base al principio di legalità, nonché della verifica circa la conseguente individuazione del soggetto responsabile, sia nell'interesse della stessa p.a. che dei soggetti coinvolti ed incisi dall'azione amministrativa affidata all'algoritmo» (sent. n. 8472/2019, 14.1 dir.). Ravvisano in tale passaggio il fulcro centrale della sentenza, e dunque il profilo particolare del principio di trasparenza applicato all'algoritmo, I.A. NICOTRA, V. VARONE, *L'algoritmo, intelligente ma non troppo*, in *Rivista AIC*, 4, 2019, 100, cui si rinvia anche per la giurisprudenza amministrativa successiva e le relative oscillazioni (105 s.). Sul punto, v. anche F. DONATI, *Intelligenza artificiale e giustizia*, in *Rivista AIC*, 1, 2020, 424 s.; A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica*, in *Riv. trim. dir. pubbl.*, 2019, 1149 ss.; ID., *Amministrazione digitale algoritmica. Il quadro costituzionale*, in R. CAVALLO PERIN, D.-U. GALLETTA (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Giappichelli, Torino, 2020, 26 ss.

opacità, si dice, non può offuscare tale trasparenza nella misura in cui gli strumenti algoritmici vengono "posti al servizio del potere autoritativo" delle amministrazioni pubbliche[367].

Si consideri però come questo contrasto tra esigenze contrapposte non risulta del tutto insanabile. Un contemperamento tra la "*explicability*" e le legittime aspettative che si celano in tale opacità è offerto da quelle tecniche per spiegare le scelte compiute dai programmatori di algoritmi senza aprire le "*black box*" entro cui sono rinchiusi. Si pensi, ad esempio, ai meccanismi di "*algorithm audits*", basati su simulazioni con cui vengono realmente processati dati che potrebbero portare a risultati discriminatori, allo scopo di approntare i possibili correttivi[368]. L'obiettivo è realizzare sistemi di verifica "agnostici" rispetto al modello di algoritmo oggetto di controllo[369], con cui ci si limita a interrogare l'algoritmo come se fosse un "oracolo", senza cioè avere pienamente accesso al funzionamento del procedimento decisionale e rispettandone così la segretezza, ma basandosi unicamente sui contenuti delle decisioni prodotte[370]. Risultati analoghi, infine, si possono ottenere anche

[367] Cfr. Cons. St., sez. VI, sent. 13 dicembre 2019, n. 8472, 11 dir. (in senso conforme n. 881/2020). Che un giudice sia abilitato a superare i segreti industriali che coprono gli algoritmi, spingendosi oltre a quanto stabilito dalla normativa europea, la quale non risolve espressamente questo bilanciamento con la tutela dei diritti, è sottolineato in G. DE MINICO, *Towards an "Algorithm Constitutional by Design"*, in *BioLaw Journal*, 1, 2021, 395.

[368] Cfr. P. ADLER ET AL., *Auditing Black-box Models for Indirect Influence*, in arXiv:1602.07043v2 [stat.ML], novembre 2016; C. SANDVIG, K. HAMILTON, K. KARAHALIOS, C. LANGBORT, *Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms*, in *Semantic Scholar*, 22 maggio 2014 [bit.ly/39U1VkC], ove vengono indicate una serie di tecniche di *auditing*.

[369] M.T. RIBEIRO, S. SINGH. C. GUESTRIN, *Why should I Trust You? Explaining the Predictions of Any Classifier*. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016 [arxiv.org/pdf/1602.04938.pdf].

[370] L. EDWARDS, M. VEALE, *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You are Looking for*, cit., 65. Per inciso, è stato osservato come una situazione analoga si verifica in generale per tutte le forme di *auditing*: ad esempio, quando una impresa viene sottoposta ad *audit*, non si cerca di spiegare il funzionamento delle connessioni sinaptiche o la genetica di coloro che lavorano all'interno dell'impresa, ma ci si basa su elementi indiretti per verificare se le persone abbiano agito secondo le procedure appropriate; cfr. J.J. BRYSON, *The Artificial Intel-*

con metodi diversi dalle tecniche di *audit*[371], salvo però dover verificare la concreta utilità che così ne deriverebbe rispetto alle esigenze di tutela di fronte a decisioni algoritmiche come quelle di riconoscimento facciale.

7. *Le "distorsioni" nel riconoscimento facciale (i c.d.* bias*)*

L'impiego sempre più massiccio di TRF è suscettibile – come visto – di originare fenomeni discriminatori a partire dagli stessi elementi che la Costituzione ritiene non dovrebbero fondare distinzioni, secondo la formulazione del principio di eguaglianza formale; oppure a risolversi in fattori che possono limitare di fatto la libertà e l'eguaglianza di persone maggiormente bisognose di tutela, in contrasto con il principio di eguaglianza sostanziale[372]. È giunto il momento di guardare più da vicino una delle principali ragioni che danno origine a queste forme di violazione del principio di eguaglianza, riconducibili ai c.d. *bias*.

Nella letteratura informatica, con il termine *bias* ci si riferisce a quelle "distorsioni"[373] presenti all'interno dei sistemi informatici che hanno l'effetto di "discriminare sistematicamente e ingiustamente de-

ligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation, in M. DUBBER, F. PASQUALE, S. DAS (a cura di), *The Oxford Handbook of Ethics of Artificial Intelligence*, Oxford University Press, Oxford, 2019, 7.

[371] Si tratta di tecniche che permettono di sottoporre a verifica l'algoritmo e tenerne segreti i dati o una parte del software, ma al contempo garantiscono che il software e gli input soddisfino determinate regole o determinati requisiti di regolarità procedurale, o consentono di verificare che la stessa "policy" venga usata per ciascuna decisione, o che la medesima "policy" sia stata predeterminata prima che gli input vengano conosciuti, o che i risultati siano riproducibili; cfr. J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YU, *Accountable Algorithms*, cit., 662 ss. V. anche S. WACHTER, B. MITTELSTADT, C. RUSSELL, *Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR*, in *Harvard Journal of Law & Technology*, 31, 2, 2018, 841 ss.

[372] V. *retro* Cap. II, par. 8. Il riferimento, in particolare, è rivolto a quelle violazioni perpetrate nei confronti di donne, minoranze etniche, minori, anziani e disabili.

[373] Nella traduzione offerta ad es. in GRUPPO DI ESPERTI AD ALTO LIVELLO SULL'INTELLIGENZA ARTIFICIALE, *Orientamenti etici per un'IA affidabile*, cit., 14.

terminati individui o gruppi in favore di altri". Un sistema discrimina ingiustamente "se nega un'opportunità o un bene o se assegna un risultato indesiderato ad un individuo o ad un gruppo di individui per motivi che sono irragionevoli o inappropriati"[374].

L'intera storia delle immagini è segnata da questo tipo di distorsioni. Fin dal XIX° secolo, con la nascita della fotografia, i reagenti chimici fotosensibili, la meccanica delle macchine fotografiche e le procedure per sviluppare le pellicole erano più adatte a rappresentare pelli chiare, mentre risultavano molto meno efficaci nel riprodurre le sfumature delle pelli scure[375]. Nel passaggio alle foto digitali – ovvero alla registrazione elettronica delle griglie di pixel tramite sequenze di valori numerici computabili, conservabili e trasmissibili tramite internet – alcuni di questi "pregiudizi tecnologici" sono rimasti pressoché impregiudicati[376]. Nel primo decennio degli anni 2000 hanno fatto molto scalpore il caso della blogger asioamericana che denunciò come la videocamera acquistata, dotata di TRF, equivocasse la forma stretta e allungata del proprio occhio con un ammiccamento[377]; o il caso della *webcam* in grado asseritamente di tracciare i volti, capace sì di rilevare le persone dalla pelle chiara, ma del tutto insensibile a quelle dalla pelle più scura[378]. Si tratta di esempi da cui si evince che le soluzioni video-fotografiche vengono studiate per ottenere risultati ottimali nei confronti di persone con certe caratteristiche, fra cui pelli bianche in grado meglio di riflettere le luce e di distinguersi per intensità di contrasto, e molto meno per i c.d. BAME (*black*, *Asian* e *minority ethnic*).

Anche le più moderne TRF non sono indenni da analoghi *bias*. Questi fenomeni possono avere diverse origini e integrare una casistica molto varia. Rinviando alla letteratura informatica specialistica che ha

[374] B. FRIEDMAN, H. NISSENBAUM, *Bias in computer systems*, in *ACM Transactions on Information Systems (TOIS)*, 14, 3, 1996, 332, traduzione nostra.

[375] Cfr. S. LEWIS, *The Racial Bias Built into Photography*, in *The New York Times*, 25 aprile 2019 [nyti.ms/3sYF1zZ].

[376] D. LESLIE, *Understanding bias in facial recognition technologies: an explainer*, cit., 13.

[377] G. SHARP, *Nikon Camera Says Asians are always Blinking*, in *TheSocietyPages.org*, 29 maggio 2009, [bit.ly/2R5ZFQw].

[378] B.X. CHEN, *HP Investigates Claims of 'Racist' Computers*, in *Wired*, 22 dicembre 2009 [bit.ly/2R5ZTXS].

indagato approfonditamente sul punto[379], è più utile qui richiamare le forme di distorsioni differenziabili in base ai momenti in cui possono venire in essere[380], ovvero dalla progettazione sino al concreto svolgersi del procedimento di riconoscimento facciale.

I *bias* possono avere origine, innanzitutto, nel momento della costruzione del modello algoritmico. Gli algoritmi, infatti, possono produrre effetti discriminatori a causa delle scelte con cui il modello è progettato o delle variabili che vengono prese in considerazione[381].

In questo caso si possono produrre "discriminazioni dirette" nella misura in cui fa uso di "etichette" (c.d. *labels*) come "razza", "etnia", "genere", per categorizzare i dati e consentire agli algoritmi di distinguerli ai fini delle decisioni prodotte. Alcune ricerche empiriche dimostrano come i più grandi *dataset* usati dalle TRF sono stati costruiti usando tecniche di classificazione dei dati che riescono con difficoltà a "leggere" il colore della pelle, rendendo invisibili a chi utilizza questi dati le relative differenze[382]. Anche la scelta delle etichette, inoltre, si espone a criticità, a causa della mutevolezza delle categorie cui rinviano, o del rischio di riflettere pregiudizi culturali e classificazioni soggettive[383], che possono sfociare in forme di "razzismo scientifico"[384].

[379] Cfr. su tutti M. VEALE, R. BINNS, *Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data*, in *Big Data & Society*, 4, 2017, 3, cui si rinvia anche per i richiami bibliografici relative a: «'disparate impact' or 'statistical/demographic parity', which considers classification rates between groups; 'accuracy equity', which considers the overall accuracy of a predictive model for each group; 'conditional accuracy equity', which considers the accuracy of a predictive model for each group, conditional on their predicted class; 'equality of opportunity', which considers whether each group is equally likely to be predicted a desirable outcome given the actual base rates for that group; and 'disparate mistreatment', a corollary which considers differences in false positive rates between groups».

[380] Analogamente, P. ZUDDAS, *Intelligenza artificiale e discriminazioni*, in *Consulta Online - Liber amicorum per Pasquale Costanzo*, 16 marzo 2020, 5.

[381] Cfr. J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YU, *Accountable Algorithms*, cit., 680 s.

[382] M. MERLER, N. RATHA, R.S. FERIS, J.R. SMITH, *Diversity in faces*, in *arXiv:1901.10436v6*, 2019, spec. 4 ss.

[383] Cfr. S. BAROCAS, A.D. SELBST, *Big Data's Disparate Impact*, cit., 681.

[384] D. LESLIE, *Understanding bias in facial recognition technologies: an explainer*, cit., 6. Si osserva in O. KEYES, *The Misgendering Machines: Trans/HCI Implications of*

Ad esempio, una ricerca pubblicata nel 2017 ha dimostrato come in un famoso *database*, contenente pià di ventimila immagini, all'interno della categoria "razza" fossero utilizzate solo quattro classificazioni, ovvero "bianchi", "neri", "asiatici", "indiani" e "altri"[385].

Tuttavia, è possibile anche incorrere in discriminazioni c.d. *proxy*[386], che non originano dal modo con cui vengono presi direttamente in considerazione dati "sensibili", ma che si risolvono indirettamente in un diverso trattamento in base a tali elementi. Si pensi a quei modelli algoritmici più evoluti di *deep learning*, che individuano autonomamente le caratteristiche (c.d. *features*) con cui costruire il modello biometrico, prendendo in considerazione elementi come la *texture* della pelle, la geometria del volto o i caratteri di determinati tratti fenotipici. Il sistema, in questo caso, potrebbe rivelarsi maggiormente sensibile in ordine a determinate varianti corrispondenti ad una certa fascia di età o ad una determinata etnia, e non ad altre.

Inoltre, ulteriori distorsioni possono prodursi nella scelta delle categorie di dati che l'algoritmo deve elaborare[387]. Si pensi a quei modelli di riconoscimento facciale in cui tale scelta viene stabilita dall'essere umano (c.d. *handcrafted*), così da risultare elaborati solamente alcuni tratti biometrici, corrispondenti ad altrettante caratteristiche localizzate del volto, e non altri. La stessa selezione dei tratti potrebbe risultare discriminatoria nella misura in cui si riveli più efficace nei confronti di determinate categorie di soggetti e non altre.

Altra fase nella quale i *bias* possono venire in essere è al momento della scelta dei dati e immagini con cui vengono "allenati" i modelli algoritmici (*training set*)[388]. I sistemi di *machine learning* possono veder

Automatic Gender Recognition, *Proceedings of the ACM on Human-Computer Interaction,* 2, novembre 2018, come le TRF fatichino a riconoscere il genere di una persona soprattutto quando questa non si riconosce nel sesso maschile o femminile.

[385] K. CRAWFORD, T. PAGLEN, *Excavating AI: The Politics of Training Sets for Machine Learning*, 19 settembre 2019.

[386] S. BAROCAS, A.D. SELBST, *Big Data's Disparate Impact*, cit., 691 ss.; F.Z. BORGESIUS, *Discrimination, artificial intelligence, and algorithmic decision-making*, Study for the Council of Europe, 2018, 13.

[387] S. BAROCAS, A.D. SELBST, *Big Data's Disparate Impact*, cit., 688; F.Z. BORGESIUS, *Discrimination, artificial intelligence, and algorithmic decision-making*, cit., 12.

[388] CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Report on Artificial In-*

compromessa la propria accuratezza e portare a risultati discriminatori se "allenati" con dati storici che riflettono pregiudizi impliciti, o se le immagini campionate offrono una rappresentazione statisticamente distorta di gruppi rispetto al complesso della popolazione[389]. Da questo punto di vista, le immagini impiegate nel riconoscimento facciale e le metriche utilizzate dovrebbero rispecchiare la varietà dei tratti fenotipici delle persone, in relazione a sesso, età, origine etnica: maggiore è il "pluralismo" dei dati utilizzati, tendenzialmente maggiore sarà l'accuratezza del sistema[390].

Recenti studi, tuttavia, dimostrano come le persone dalla pelle nera e le donne risultino fortemente sottorappresentate nella costruzione dei *dataset*, al punto che le donne dalla pelle scura originano tassi di errore nel riconoscimento facciale fino al 34,7%, a differenza degli uomini dalla pelle chiara che si fermano allo 0,8%[391].

telligence, by A. Mantelero, T-PD(2018)09rev, gennaio 2019, 9; G. SARTOR, F. LAGIOIA, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, cit., 21.

[389] J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YU, *Accountable Algorithms*, cit., 680 s.; M. VEALE, R. BINNS, *Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data*, cit., 2.

[390] B.F. KLARE, M.J. BURGE, J.C. KLONTZ, R.W. VORDER BRUEGGE, A.K. JAIN, *Face recognition performance: Role of demographic information*, in *IEEE Transactions on Information Forensics and Security*, 7, 6, 2012, 1789 ss.

[391] J. BUOLAMWINI, T. GEBRU, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proceedings of Machine Learning*, 81, 2018, 77 ss.; a partire da una indagine avente ad oggetto i sistemi di classificazione di Microsoft, IBM, e Face++; I.D. RAJI, J. BUOLAMWINI, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, gennaio 2019; C.M. COOK, J.J. HOWARD, Y.B. SIROTIN, J.L. TIPTON, A.R. VEMURY. *Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems*, in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 1, 1, 2018, 32 ss. V. inoltre P. GROTHER, M. NGAN, K. HANAOKA, *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*, cit., 3 ss., ove sono riportati i risultati in esito ad una valutazione massiva di ben 189 algoritmi sviluppati da 99 tra i maggiori e più famosi produttori, tenendo ferma la soglia di falsi-positivi e falsi-negativi accettabili, in modo da verificare l'accuratezza dell'algoritmo rispetto a differenti gruppi demografici. Con foto di alta qualità, i falsi-positivi nei dispositivi di verifica sono tra le 2 e le 5 volte superiori nelle donne che negli uomini, maggiori nelle

Le ragioni alla base di questo tipo di *bias* possono essere rintracciate nella circostanza che i primi e più usati *database* con cui allenare gli algoritmi sono stati costruiti solo in parte attraverso una selezione deliberatamente oculata e rappresentativa di immagini, eventualmente con il contributo di soggetti volontari o remunerati. Il più delle volte, tale costruzione è avvenuta raccogliendo immagini da internet in maniera casuale, magari ricorrendo a professionisti come i citati *data broker* e *data consultant*, molto spesso senza il consenso degli interessati o delle piattaforme *social* nelle quali venivano ospitate[392]. Di conseguenza, le immagini campionate riflettono le relazioni di potere, le gerarchie sociali e le strutture di privilegio delle realtà socioculturali da cui sono attinte[393].

Quand'anche la scelta delle immagini con cui allenare gli algoritmi non avvenisse in modo casuale da internet, vi è comunque il rischio che la selezione produca un *dataset* di dati incompleti, nella misura in cui il campione scelto non fosse rappresentativo, così per produrre ugualmente una rappresentazione parziale della realtà[394].

persone di origine africana o asiatica rispetto a quelle di origine est-europea; quanto ai falsi-negativi, nel caso di fototessere con immagini di buona qualità vi è una percentuale maggiore per gli asiatici rispetto ad europei e africani, ma con foto di minore qualità i falsi-negativi sono generalmente maggiori per gli africani. A differenza della metodologia impiegata nelle ricerche i cui risultati sono riportati nei contributi dottrinali citati sopra, la ricerca da ultimo richiamata non si limita a verificare il prodotto degli algoritmi, ma offre una valutazione più articolata, in relazione alla tipologia di algoritmo e alla sua finalità (identificazione o verifica). Tuttavia, in questa indagine non si approfondisce quali siano gli elementi tecnici che specificatamente causano una discriminazione in termini di causa-effetto (*ivi*, 9). Diversamente, i contributi dottrinali sopra citati si limitano a uno studio basato su pochi algoritmi, ma si spingono fino a valutare la relazione di causa-effetto rispetto alle decisioni prodotte; cfr. anche U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, cit., 33.

[392] Cfr. M. MERLER, N. RATHA, R.S. FERIS, J.R. SMITH, *Diversity in faces*, cit., 4, ove si dimostra che da un controllo su otto dei *dataset* più famosi, ben sei di essi comprendevano tra 81.2% e 94.6% di individui dalla pelle bianca. V. anche *retro* par. 5.3.

[393] D. LESLIE, *Understanding bias in facial recognition technologies: an explainer*, cit., 18. In questo caso si rientrerebbe in una ipotesi di "*biased samples*", in cui il campione di dati risulta distorsivo, più che di "*biased data*", ovvero dati già affetti da pregiudizi; per questa distinzione, cfr. F.Z. BORGESIUS, *Discrimination, artificial intelligence, and algorithmic decision-making*, cit., 11.

[394] Come osserva P. ZUDDAS, *Intelligenza artificiale e discriminazioni*, cit., 9.

In queste ipotesi, i *bias* che sorgono al momento della creazione dei *training set* possono interessare sia la fonte dei dati, ed è il caso dei "*bias* di selezione", oppure la persona responsabile delle analisi, ed è il caso dei "*bias* di conferma"[395].

Ma i *bias* possono riguardare anche la "qualità" del dato, poiché, come osservato anche dal Parlamento europeo, «l'utilizzo di dati di scarsa qualità, obsoleti, incompleti o inesatti, nelle diverse fasi del trattamento dei dati, può portare a previsioni e valutazioni inadeguate e, a sua volta, a distorsioni»[396]. Nelle TRF ciò può dipendere innanzitutto dalle condizioni di acquisizione delle immagini, a seconda, ad esempio, che essa avvenga in ambienti controllati o meno. Ma a pesare è anche la presenza stessa dei *bias* sopra descritti: il riflesso della luce, l'inclinazione del volto o il movimento dell'immagine, sono infatti destinati a interferire maggiormente con un sistema che già ottiene risultati peggiori – magari con un maggior numero di falsi-positivi – nei confronti di persone dalla pelle scura, accentuando così le disparità conseguenti alla presenza di distorsioni pregresse[397].

Si comprende, dunque, come nelle TRF, e più in generale nelle decisioni algoritmiche, le distorsioni non nascano necessariamente da intenti consapevolmente discriminatori, ma anche da ipotesi accidentali legate alla progettazione dell'algoritmo[398], salvo incorrere in ipotesi di "camuffamento", ovvero di *bias* intenzionali spacciati invece come accidentali[399].

Quanto detto fa comprendere come la scelta e la selezione delle immagini a monte sia decisiva per la qualità del riconoscimento atteso a valle – quello che in gergo tecnico prende il nome di "*garbage in, garbage out*". La costruzione dei *dataset*, tuttavia, non è mai un proces-

[395] CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Report on Artificial Intelligence*, cit., 9.

[396] PARLAMENTO EUROPEO, *Una politica industriale europea globale in materia di robotica e intelligenza artificiale*, cit., punto 177.

[397] FRA, *Under watchful eyes – biometrics, EU IT-systems and fundamental rights*, cit., 90.

[398] T.Z. ZARSKY, *Incompatible: The GDPR in the Age of Big Data*, cit., 1014.

[399] J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YU, *Accountable Algorithms*, cit., 680 s.; F.Z. BORGESIUS, *Discrimination, artificial intelligence, and algorithmic decision-making*, cit., 13 s.

so statico, ma occorre mantenere sempre aggiornati i dati e i campioni utilizzati, verificando nel tempo il livello di accuratezza del riconoscimento per intervenire, se del caso, a integrazione con immagini nuove e più differenziate[400]. Ciononostante, questa opera di continuo aggiornamento può risultare difficoltosa, dal momento che la correzione dei *dataset* di immagini o la costruzione di nuovi, una volta rilevata la presenza di distorsioni, può comportare costi molto rilevanti per le imprese[401]. Per gli informatici, inoltre, può essere difficile intervenire per correggere eventuali errori una volta che i modelli algoritmici vengono venduti a terze parti, le quali spesso non offrono agli sviluppatori *feedback* sul rendimento del software, indispensabili per aggiornare e rendere più accurato il modello[402].

La panoramica svolta sul piano tecnologico impone di rintracciare una base giuridica che offra tutela nei confronti dei *bias*. Il riferimento principale va alla legislazione antidiscriminatoria, volta a creare un sistema integrato per proteggere singoli individui e gruppi all'interno di settori specifici, avente origine in direttive dell'UE[403], per come recepite a livello nazionale[404]. Il perno su cui si muove l'intera disciplina vi-

[400] Cfr. CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on Facial Recognition*, cit., 9.

[401] P. HACKER, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law*, in *Common Market Law Review*, 55, 4, 2018, 1150.

[402] Cfr. P.T. KIM, *Data-Driven Discrimination at Work*, in *William & Mary Law Review*, 58, 3, 2016-2017, 857 ss.

[403] Si tratta di direttiva 2000/43/EC, che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica in una serie di ambiti, fra cui il mercato del lavoro, istruzione, formazione professionale, protezione sociale, accesso ai beni e servizi; la direttiva 2000/78/EC, relativa al principio di parità di trattamento in materia di occupazione e di lavoro (c.d. direttiva quadro), a tutela di discriminazioni fondate sulla religione o le convinzioni personali, gli handicap, l'età o le tendenze sessuali; la direttiva 2004/113/EC, che attua il principio della parità di trattamento tra uomini e donne per quanto riguarda l'accesso a beni e servizi e la loro fornitura; la direttiva 2006/54/EC, riguardante l'attuazione del principio delle pari opportunità e della parità di trattamento fra uomini e donne in materia di occupazione e impiego.

[404] Per una panoramica sul punto, v. EUROPEAN COMMISSION, *A comparative analysis of non-discrimination law in Europe 2019*, report preparato da I. Chopin e C. Germaine per lo *European network of legal experts in gender equality and non-*

gente è la distinzione tra "discriminazione diretta" e "discriminazione indiretta"[405], la quale, però, non risulta del tutto adeguata a fronteggiare i citati "*algorithmic bias*".

Si ha *discriminazione diretta* quando «una persona è trattata meno favorevolmente di quanto sia, sia stata o sarebbe trattata un'altra in una situazione analoga»[406]. Nell'ambito delle TRF, tuttavia, non è frequente che si verifichi questo tipo di discriminazione[407]. Stando alle ipotesi di *bias* all'interno del procedimento decisionale riportate sopra, si integra una discriminazione diretta quando viene riconosciuto peso inferiore a variabili riferite a dati "sensibili", o si verificano distorsioni nell'algoritmo in dipendenza dell'uso delle etichette. Viceversa, è più difficile invocare una discriminazione diretta quando i modelli sono "allenati" con dati che offrono una rappresentazione statisticamente distorta di un gruppo o una realtà.

Le ipotesi che fuoriescono dal perimetro della discriminazione diretta dovrebbero ricadere nelle *discriminazione indiretta*, che si verificano quando «una disposizione, un criterio o una prassi apparentemente neutri possono mettere in una posizione di particolare svantag-

discrimination, Bruxelles, 2020. In Italia, tale pacchetto di direttive è stato attuato principalmente con il d.lgs. 9 luglio 2003, n. 215, recante "Attuazione della direttiva 2000/43/CE per la parità di trattamento tra le persone indipendentemente dalla razza e dall'origine etnica", e il d.lgs. 9 luglio 2003, n. 216, recante "Attuazione della direttiva 2000/78/CE per la parità di trattamento in materia di occupazione e di condizioni di lavoro".

[405] Cfr. P. CARETTI, G. TARLI BARBIERI, *I diritti fondamentali Libertà e diritti sociali*, cit. 205 ss.; M. D'AMICO, *Articolo 3*, in F. CLEMENTI, L. CUOCOLO, F. ROSA, G.E. VIGEVANI (a cura di), *La Costituzione italiana. Commento articolo per articolo*, I, cit., 29 s.; E. CONSIGLIO, *Che cosa è la discriminazione? Un'introduzione teorica al diritto antidiscriminatorio*, Giappichelli, Torino, 2020, spec. 77 ss.; L. GIACOMELLI, *Ripensare l'eguaglianza. Gli effetti collaterali della tutela antidiscriminatoria*, Giappichelli, Torino, 2018, spec. 130 ss. Ulteriori specificazioni settoriali dei concetti di discriminazione diretta e indiretta per ragioni di sesso si hanno al d.lgs. 11 aprile 2006, n. 198, "Codice delle pari opportunità tra uomo e donna" (es. art. 25 nell'ambito dei rapporti di lavoro o art. 55-*bis* nell'accesso a beni e servizi).

[406] Art. 2, c. 1, lett. a, d.lgs. n. 215/2003.

[407] Più in generale, con riguardo al *machine learning*, cfr. P. HACKER, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law*, cit., 1151 ss.

gio le persone che professano una determinata religione o ideologia di altra natura, le persone portatrici di un particolare handicap, le persone di una particolare età o di una particolare tendenza sessuale, rispetto ad altre persone»[408]. Tuttavia, anche questo schema normativo – peraltro, oramai risalente nel tempo e ben antecedente agli sviluppi tecnologici in questione – può mostrarsi inadatto rispetto alle ipotesi di distorsioni richiamate sopra, nella misura in cui si limiti a sanzionare *ex post* eventuali fenomeni discriminatori: la valutazione sul carattere discriminatorio di una decisione è infatti sottoposta ad un test di proporzionalità per il quale, in termini pratici, gli interessati che vogliano lamentare in giudizio una discriminazione devono soddisfare un onere della prova a dir poco diabolico[409], trovandosi nella difficile posizione di chi, per offrire una dimostrazione di quanto lamentato, deve aprire *black box* che celano gli algoritmi, i *database*, o tecnologie (come quelle basate su reti neurali artificiali), che rimangono inintelligibili alla logica causale.

Una impostazione differente è stata accolta dalla normativa europea fin qui discussa, che da questo punto di vista, più che adottare un approccio rimediale al pari della legislazione antidiscriminatoria[410], cerca di intervenire a monte per evitare che si verifichino distorsioni con un approccio basato sul rischio[411]. Sebbene non sia previsto un vero e proprio "divieto di *bias*", si incarica il titolare del trattamento di attivarsi per garantire il "*principio di esattezza*" dei dati, il quale pone in correlazione diretta la "qualità" di questi ultimi con le finalità per i

[408] Art. 2, c. 1, lett. b, d.lgs. n. 215/2003.

[409] Cfr. P. HACKER, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law*, cit., 1160 ss.; F.Z. BORGESIUS, *Discrimination, artificial intelligence, and algorithmic decision-making*, cit., 19 s. Le fasi di tale test si distinguono in termini di valutazione della legittimità, idoneità della misura, necessità in senso stretto e proporzionalità in senso stretto (cfr. anche *retro* par. 4.3).

[410] È un punto sottolineato da P. ZUDDAS, *Intelligenza artificiale e discriminazioni*, in *Consulta Online - Liber amicorum per Pasquale Costanzo*, 16 marzo 2020, 12.

[411] Spunti in P. HACKER, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law*, cit., 1170 ss. V. anche *retro* par. 2.

quali vengono trattati[412], imponendo così di verificare la presenza o meno di distorsioni negli algoritmi e nei *dataset*, oltre che di approntare le "*misure tecniche e organizzative*" necessarie per garantire e dimostrare che il trattamento sia conforme alla disciplina a protezione dei dati e per tutelare i diritti dell'interessato[413]. Tali previsioni – si potrebbe dire – vengono compendiate nel principio di protezione dei dati "*by design*", con il quale – come si vedrà meglio più avanti[414]– la costruzione del sistema algoritmico deve integrare scelte e valori che impediscano queste distorsioni.

L'impostazione così espressa trova chiara sintesi nel già ricordato considerato 71 del GDPR, che appare indicativo di quello che può essere definito come un "principio di non discriminazione per via algoritmica"[415], ossia il dovere di rettificare i dati in "ingresso" per evitare effetti discriminatori nell'output decisionale[416]. Questa lettura, inoltre, trova conferma anche nelle pronunce della Corte di giustizia con cui si sollecita la necessità di sottoporre a riesame periodico i modelli e i cri-

[412] Più in particolare, i dati personali devono essere «esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati» (cfr. art. 5, par. 1, lett. d, del GDPR; art. 4, par. 1, lett. d, della LED). V. anche art. 5, lett. d, della Convenzione 108 e i principi al punto 5.5 della Raccomandazione n. R(87) 15.

[413] L'obbligo di garantire e dimostrare la conformità del trattamento trova menzione tra le responsabilità del titolare del trattamento (art. 22 GDPR; art. 24 LED), mentre la garanzia dei diritti trova menzione, oltre che nella formulazione del principio di esattezza, anche – per quanto rileva qui – a proposito del trattamento di categorie particolari di dati personali (art. 9 GDPR) o sui processi decisionali completamente automatizzati (art. 22 GDPR; art. 11 LED).

[414] V. *infra* Cap. V, par. 5.

[415] A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, cit., 101.

[416] Nel considerato 71 del GDPR si prevede che «al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento [...] metta in atto misure tecniche e organizzative adeguate [...] al fine di garantire la sicurezza dei dati personali secondo una modalità [...] che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti».

teri prestabiliti su cui si fondano le decisioni automatizzate, nonché le banche dati utilizzate, per verificare che i dati siano limitati allo stretto necessario e non affetti da distorsioni che producano risultati di natura discriminatoria[417].

In aggiunta, e in termini complementari rispetto alle misure di intervento a monte, vale sempre il meccanismo di salvaguardia offerto dall'intervento dell'essere umano nei procedimenti decisionali interamente automatizzati, per poter riscontrare eventuali distorsioni e, nella misura del possibile, intervenire a correggerle[418]. Al limite, in presenza della lesione di un diritto provocata da una presunta distorsione, l'interessato ha la possibilità di esercitare le proprie prerogative relative alla "conoscibilità" del sistema.

Questa panoramica sulle diverse tipologie di *bias* che possono annidarsi all'interno delle TRF, e sui rimedi che si possono esperire, induce conclusivamente a riflettere su due aspetti fondamentali.

Il primo è che queste tecnologie manifestano la propria utilità confermando l'ordine sociale *esistente.* Le inferenze statistiche su cui si basano gli algoritmi, capaci di generare modelli e esplicitare tendenze di dati, comportamenti o immagini, si limitano a perpetuare situazioni di fatto preesistenti, sul presupposto che statisticamente determinate correlazioni tenderanno a ripetersi nel tempo[419]. Questa conseguenza appare insostenibile quando la realtà di partenza è affetta da discriminazioni o da situazioni di svantaggio[420]. Per un verso, dunque, si ha la riprova di come il principio di eguaglianza, nell'accezione formale e sostanziale, rimanga al di fuori dell'orizzonte algoritmico[421]. Per l'altro, si comprende bene l'accusa di "idiozia"[422] mossa agli algoritmi, in quanto del tutto privi della capacità valutati-

[417] CGUE, parere 1/15 (Accordo PNR UE-Canada), cit., p. 174.

[418] V. *retro* par. 6.3.

[419] D. CARDON, *Che cosa sognano gli algoritmi*, cit., 74.

[420] Rileva C. O'NEIL, *Armi di distruzione matematica*, Giunti-Bompiani, Firenze-Milano, 2017, 16, come i ricchi vengono considerati nella loro individualità, mentre i poveri subiscono una «gestione all'ingrosso».

[421] Cfr. A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, cit., 17, secondo cui «appare molto più complicato educare un algoritmo a perseguire logiche sostanziali di eguaglianza».

[422] D. CARDON, *Che cosa sognano gli algoritmi*, cit., 70.

va e della duttilità cognitiva – in una parola, della ragionevolezza – propria delle persone[423].

Il secondo aspetto che occorre sottolineare è la debolezza dell'assunto per cui tecnologie algoritmiche come quelle di riconoscimento facciale sarebbero "neutrali"[424]. Una delle ragioni con cui si giustifica l'impiego delle TRF nell'operare valutazioni, ad esempio circa la personalità di un individuo, o nell'assumere decisioni, ad esempio durante un colloquio di lavoro, è che queste siano "*noise free*"[425], ovvero al riparo dagli umori o dalle emozioni che minano il raziocinio degli esseri umani, e dunque si possano considerare più oggettive dell'intelligenza naturale. Tuttavia, il fatto che gli algoritmi si limitino fondamentalmente a replicare la realtà preesistente, o i *bias* che affliggono i loro procedimenti decisionali, valgono pienamente a sconfessare tale assunto. Non esistono algoritmi che riflettono neutralmente la realtà; essi, viceversa, propongono una loro rappresentazione dei problemi da risolvere ricavata dalle variabili scelte, dalle formule classificanti, dal peso attribuito ai singoli parametri inseriti, dalle procedure che determinano il risultato, allo scopo di ottenere i risultati attesi[426].

8. Law in action: *le TRF portate di fronte ad un giudice*

Per apprezzare come i principi fin qui trattati possano operare "in azione" vale la pena richiamare uno dei pochi casi in cui – a quanto costa – le TRF siano state portate davanti ad un tribunale per dar conto delle limitazioni ai diritti fondamentali che sono in grado di provocare[427].

[423] V. *retro* Cap. II, par. 3.1.

[424] B.A. GREENBERG, *Rethinking Technology Neutrality*, in *Minnesota Law Review*, 100, 2016, 1495 ss.; M. AIROLDI, D. GAMBETTA, *Sul mito della neutralità algoritmica*, in *The Lab's Quarterly*, 4, 2018, 25 ss.

[425] J.N. MATHIAS, *Bias and Noise: Daniel Kahneman on Errors in Decision-Making*, in *Medium*, 17 ottobre 2017, [bit.ly/3mJuI0p].

[426] A.C. AMATO MANGIAMELI, *Algoritmi e big data. Dalla carta sulla robotica*, in *Rivista di filosofia del diritto*, 1, 2019, 109.

[427] Altra vicenda è quella legata all'uso di TRF all'interno delle scuole con finalità di tutela della sicurezza, su cui il *Tribunal administratif de Marseille*, con sentenza del

L'inquadramento offerto dai giudici risulta particolarmente interessante ai fini della presente analisi perché restituisce una ricostruzione di alcune delle principali problematiche giuridiche fin qui emerse e offre un esempio dei delicati bilanciamenti tra interessi di rilevanza costituzionale da tenere in considerazione nel decidere se e come impiegare le tecnologie in questione, anche in ragione delle molteplici variabili e soluzioni tecniche a disposizione.

Le autorità giudiziarie in questione sono la *Queen's Bench Division* della *High Court of Justice*, giudice amministrativo con sede in Cardiff, il quale ha adottato in data 4 settembre 2019 una pronuncia successivamente impugnata innanzi alla *Civil Division* della *Court of Appeal*, e riformata con sentenza dell'11 agosto 2020[428]. La circostanza che la vicenda processuale si snodi su più gradi di giudizio e veda contrapporre valutazioni divergenti offre la riprova di come sia possibile dare origine ad applicazioni differenti dei principi giuridici in gioco, entro uno spazio che per molti versi appare ancora inesplorato.

Il *casus quo* ha origine nel Regno Unito e riguarda l'uso delle TRF da parte delle forze di polizia per le ordinarie attività di prevenzione, indagine e repressione dei reati. Protagonista è la *South Wales Police*, che dal 2017 ha fatto sperimentalmente impiego di queste tecnologie, maturando un'esperienza tanto significativa nel panorama europeo da essere fatta oggetto anche di ricerche e analisi da parte di studiosi indipendenti[429]. La vicenda, in particolare, interessa il progetto-pilota

27 febbraio 2020, si è pronunciata per annullare la deliberazione del Consiglio della *Provence-Alpes-Côte d'Azur* che aveva autorizzato la sperimentazione di queste tecnologie, nonostante l'avviso contrario della CNIL; su alcuni dei motivi v. *retro* par. 4.1. Si poi consideri il contenzioso scaturito dalla decisione del Commissario per la protezione dei dati e la libertà di informazione di Amburgo, che ingiungeva alle forze di polizia di cancellare il *database* con le immagini utilizzate per i controlli in occasione del G20 del luglio 2017, su cui v. *retro* par. 6.2.

[428] Nella dottrina italiana, a commento della prima pronuncia, v. A. PIN, *Non esiste la "pallottola d'argento": l'"*artificial face recognition*" al vaglio giudiziario per la prima volta*, in *DPCE online*, 4, 2019, 3175 ss.; J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della* High Court of Justice, in *Diritto Penale Contemporaneo*, 1, 2020, 231 ss.

[429] B. DAVIES, M. INNES, A. DAWSON, *An evaluation of South Wales Police's use of Automated Facial Recognition*, Cardiff University, settembre 2018, ove si descrivono ampiamente le due modalità di impiego dell'*AFR*, ovvero l'*AFR Locate*, richiamata nel

denominato "*Automated Facial Recognition (AFR) Locate*", con il quale la polizia gallese impiega videocamere di sorveglianza ad uso "*live*", ovvero per riprendere immagini digitali di persone tra la folla e identificarle sul momento. Tali immagini vengono processate e comparate con le immagini presenti in gallerie (c.d. *watchlist*) confezionate – asseritamente – per specifici utilizzi, ricomprendenti fotografie sia di soggetti all'attenzione delle forze dell'ordine, in quanto ricercati, aventi precedenti penali, in fuga, o la cui presenza in certe aree o a determinate tipologie di eventi può risultare pericolosa, sia di soggetti che non hanno avuto precedenti rapporti con le forze dell'ordine, ma ritenuti vulnerabili o di possibile interesse per scopi di *intelligence*.

Il sistema *AFR Locate* funzionata grossomodo tramite il processo di riconoscimento strutturato nelle fasi ricostruite all'inizio dell'analisi[430] e, tramite una comparazione tra le immagini catturate dal vivo e quelle presenti nelle *watchlist*, propone una ipotesi di identificazione che deve essere confermata da un operatore umano, ossia un agente di polizia adeguatamente formato all'uso del sistema. In caso non vi sia nessuna corrispondenza – ovvero la stragrande maggioranza delle ipotesi – l'immagine acquisita viene immediatamente cancellata[431]; in caso di corrispondenza positiva, l'immagine viene conservata al massimo per 24 ore e, su conferma da parte dell'operatore, fa seguito il riscontro di un altro agente che interviene sul campo per fermare il soggetto in questione.

L'*AFR Locate*, inoltre, non viene impiegato per indagini segrete, dato che, per informare i cittadini sullo specifico utilizzo, le forze di polizia danno preventiva notizia sui *social network* e, nei luoghi in cui

testo, e l'*AFR Identify*, con il quale si analizzano le immagini di sospettati non identificati di precedenti reati attraverso la comparazione con un *database* di circa 450.000 immagini, a disposizione delle forze dell'ordine, di soggetti sottoposti a provvedimenti limitativi della libertà personale.

[430] V. *retro* Cap. I, par. 2.

[431] Il sistema *AFR Locate* è in grado di scansionare 50 immagini di volti (non necessariamente corrispondenti a persone differenti) al secondo. Nei circa 50 utilizzi del sistema tra il 2017 e il 2018, sono stati scansionati attorno ai 500.000 volti; cfr. High Court of Justice, Queen's Bench Division, Divisional Court Cardiff, *The Queen (OTAO) Bridges v. The Chief Constable of South Wales Police and others*, [2019] EWCH 2341 (Admin), 4 settembre 2019, p. 35-36.

il sistema è all'opera, provvedono ad esporre cartelloni con adeguata informativa nel raggio di circa un centinaio di metri, oltre che a distribuire volantini.

La vicenda giudiziaria vede coinvolto un soggetto che lamenta di essere stato ripreso e identificato dalle videocamere della polizia in due occasioni, ovvero durante lo *shopping* natalizio in un'area affollata di Cardiff e, circa un anno dopo, durante una manifestazione pacifica.

Dei profili toccati dalle pronunce segnalate interessa qui mettere in luce alcuni aspetti riguardanti, rispettivamente, la lamentata violazione: del diritto al rispetto della vita privata di cui all'art. 8 della CEDU, per il tramite dello *Human Rights Act* del 1998; della disciplina sui dati personali di cui al *Data Protection Act 2018*, adottato dal Regno Unito in attuazione del GDPR, della LED e della Convenzione 108; del dovere delle autorità pubbliche di verificare che non vengano prodotti effetti discriminatori ai sensi dell'*Equality Act* del 2010.

Venendo allo specifico del primo aspetto, entrambi i giudici sono concordi nel ritenere che l'uso del sistema *AFR Locate* interferisca con il *diritto al rispetto della vita privata*, alla luce anche dell'ampia portata che la giurisprudenza EDU accorda a tale nozione[432]. A risultare controversa, però, è la dimostrazione che l'uso sperimentale del sistema di riconoscimento facciale possa essere considerato legittimo in quanto "*previsto dalla legge*" ai sensi dell'art. 8, par. 2, CEDU, secondo i criteri elaborati dalla Corte EDU[433]. In assenza di una specifica legislazione che, in generale, disciplini l'uso delle TRF da parte delle forze di polizia, la *Divisional Court* è ferma nel ritenere che l'uso specifico dell'*AFR Locate* rientri nei «*common law powers*» della polizia[434]. Divergente, invece, è la valutazione dei due giudici sulla sussistenza di un quadro normativo che risponda ai requisiti di "qualità" della legge richiesti dall'art. 8, par. 2, CEDU[435] e idoneo a fondare l'uso specifico del sistema. Con ciò il rispetto della Convenzione si fonde anche con il rispetto della *disciplina sulla protezione dei dati personali*, la quale concorre a formare proprio tale quadro.

[432] Cfr. *retro* Cap. II, nota 46.

[433] Su tale nozione, più approfonditamente, v. *retro* par. 4.2.

[434] [2019] EWCH 2341 (Admin), cit., p. 78.

[435] V. *retro* par. 4.3.

Su un versante, la *Divisional Court* ritiene che la normativa attualmente in vigore sia adeguata allo scopo, dal momento che occorre concentrarsi non tanto sulla novità dell'impiego di una tecnologia innovativa, quanto sulla sostanza dell'attività che ne origina, la quale comunque ricade entro la portata della disciplina vigente[436]. Quest'ultima è costituita da normativa primaria, ossia il richiamato *Data Protection Act 2018*, dalla normativa secondaria[437], e dalle "*local policies*" della *South Wales Police*[438]. La Corte aggiunge inoltre che per la disciplina giuridica non sarebbe necessario, e neppure pratico, definire *a priori* le precise circostanze entro cui il riconoscimento facciale debba essere impiegato, come ad esempio specificare precisamente quali reati possano giustificare un'identificazione tramite tale sistema o quanto questi debba essere sensibile dal punto di vista tecnico[439].

Sull'altro versante, la *Court of Appeal* muove da differenti presupposti, ovvero che la tecnologia in questione sia innovativa; che la stragrande maggioranza delle persone sottoposte a sorveglianza non sia di alcun interesse per la polizia; che si stia discorrendo di un trattamento che coinvolge dati sensibili; che si abbia riguardo a trattamenti automatizzati[440]. Di conseguenza, la normativa attualmente in vigore non pare sufficientemente specifica per rispondere alla "*who question*", ovvero all'interrogativo su chi possa essere inserito nelle *watchlist*, e alla "*where question*", ovvero in quale luogo il sistema possa essere impiegato; ne consegue che all'operatore di polizia sarebbe rimessa una eccessiva discrezionalità su questi profili. In particolare, quanto al *Data Protection Act 2018*, non risulta che nella vicenda in discussione sia integrato il requisito della "stretta necessità" per il trattamento dei

[436] [2019] EWCH 2341 (Admin), cit., p. 84.

[437] Si tratta del *Surveillance Camera Code of Practice*, adottato in attuazione del *Protection of Freedoms Act 2012*, per disciplinare l'uso dei sistemi di videosorveglianza, anche da parte delle forze di polizia, approvato dal *Secretary of State*, con il concorso attivo dei soggetti destinatari dei doveri stabiliti dal codice stesso, della *Association of Chief Police Officers*, dell'autorità garante per la protezione dei dati.

[438] Ovvero la "*Standard Operating Procedure*", i "*Deployment Reports*" e la "*Policy on Sensitive Processing*", adottati con lo scopo di regolare la sperimentazione dell'*AFR Locate*.

[439] [2019] EWCH 2341 (Admin), cit., p. 96.

[440] Court of Appeal, Civil Division, *R (OTAO) Bridges v. The Chief Constable of South Wales Police and others*, [2020] EWCA Civ 1058, 11 agosto 2020, p. 86-89.

dati sensibili richiesto dall'art. 10 della LED[441], secondo cui tale trattamento è ammissibile solamente «se strettamente necessario» rispetto alle finalità di polizia – da intendersi, lo si ricorda, come presenza di giustificazioni precise e particolarmente solide per il trattamento di tali dati[442]. Per questo motivo la *Court of Appeal* riforma la pronuncia di I grado stabilendo che la legislazione vigente non sia sufficiente ad integrare la previsione legislativa richiesta dall'art. 8, par. 2, CEDU.

Interessante – anche per le valutazione svolte sopra in merito alla tutela della libertà personale nel nostro ordinamento[443] – è anche il riferimento fatto dalle due Corti alla necessità dell'intervento di un magistrato nell'autorizzare l'uso dell'*AFR Locate*: mentre per la *Divisional Court* ciò non sarebbe necessario, in quanto si tratta di una identificazione che non implica contatto fisico o uso della forza, a differenza di quanto accade invece con l'ingresso nella proprietà privata o l'acquisizione di impronte dattiloscopiche[444], per la *Court of Appeal* l'inserimento nelle *watchlist* di persone sospettate o accusate di reati assieme a persone vulnerabili o per le quali si ritiene necessaria attività di *intelligence* pare irragionevole, dato che la sorveglianza segreta delle prime categorie richiede l'autorizzazione di un giudice, mentre l'uso di *AFR Locate* per le seconde no[445]. Sul punto, l'*Information Commissioner's Office* (ICO), Garante della *privacy* del Regno Unito, ha parimenti sollevato perplessità circa il rispetto del principio di minimizzazione dei dati, il quale si ritiene possa trovare applicazione anche nella creazione delle *watchlist*[446].

[441] [2020] EWCA Civ 1058, cit., 91. Quanto al *Surveillance Camera Code of Practice*, non pare vi siano indicazioni precise per stabilire quali requisiti occorre soddisfare per essere inseriti nelle *watchlist* o per stabilire in quali luoghi impiegare il sistema; gli stessi documenti relativi alle "*local policies*" della *South Wales Police* rimettono eccessiva discrezionalità alle forze dell'ordine su questi stessi aspetti (p. 90-130).

[442] Così GRUPPO DI LAVORO ARTICOLO 29, *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, WP 258, 29 novembre 2017, 7 s.

[443] Cfr. *retro* cap. II, par. 5.

[444] [2019] EWCH 2341 (Admin), cit., p. 75.

[445] [2020] EWCA Civ 1058, cit., p. 126. Il riferimento è al *Regulation of Investigatory Powers Act 2000*. Dubbi sul punto sono espressi anche in INFORMATION COMMISSIONER'S OFFICE, *ICO investigation into how the police use facial recognition technology in public places*, cit., 14 ss.

[446] *Ibidem*.

La vicenda giudiziaria in discussione interessa anche per un secondo profilo relativo alla violazione del diritto al rispetto della vita privata all'art. 8 CEDU, ovvero la sottoposizione dell'*AFT Locate* al *test di proporzionalità* per stabilire se le limitazioni ai diritti fondamentali da questo prodotte soddisfino le condizioni al par. 2 del citato art. 8. È un punto su cui la *Divisional Court* dedica particolare attenzione, a differenza – lo si anticipa – della *Court of Appeal*.

Il giudice di primo grado, in particolare, ritiene che l'uso dell'*AFR Locate* superi tale test[447] e quindi il bilanciamento sia corretto e non sproporzionato, dal momento che, schematicamente: il sistema risulta essere stato utilizzato in modo trasparente e aperto, con un significativo coinvolgimento della cittadinanza; in ogni occasione sia stato impiegato con un impatto contenuto e per un periodo limitato di tempo; sarebbe stato adoperato allo scopo specifico e limitato – «*specific and limited purpose*» – di identificare soggetti definiti (fra cui non il ricorrente) che potessero trovarsi nelle aree sorvegliate o la cui presenza giustificherebbe un allarme delle forze dell'ordine; nessuno è stato arrestato per errore; la limitazione del diritto alla vita privata del ricorrente è stata contenuta al trattamento istantaneo dei suoi dati da parte dell'algoritmo e alla loro immediata cancellazione; nessuna sua informazione è stata conservata o portata all'attenzione della polizia; non è stato identificato o approcciato dalle forze dell'ordine[448]. Si aggiunge[449], inoltre, che l'uso del sistema apparirebbe giustificato anche in ragione dello scopo, ovvero la tutela della sicurezza pubblica, a causa dei precedenti disordini verificatisi in occasioni analoghe da parte di soggetti adesso ricompresi nella *watchlist* che potevano essere nuovamente presenti nei medesimi luoghi; che la realizzazione delle *watchlist* non hanno interessato il ricorrente; che l'uso del sistema non risultasse meramente «*speculative*», in quanto le *watchlist* hanno coinvolto persone per la cui identificazione ricorrevano "*good reasons*" e la scelta del luogo di impiego appariva ragionevolmente giustificata; all'atto pratico, questa tecnologia ha consentito di arrestare soggetti che in

[447] A questo proposito la *Divisional Court* applica il test definito nel precedente della Corte suprema *Bank Mellat v Her Majesty's Treasury (No 2)* [2014] AC 700.

[448] [2019] EWCH 2341 (Admin), cit., p. 101.

[449] *Ivi*, p. 102-106.

precedenza non si era riusciti a catturare con altri metodi, favorendo anche un risparmio di risorse economiche e di tempo.

Un complesso bilanciamento, dunque, rispetto al quale la *Court of Appeal* si limita a respingere le censure dei ricorrenti senza sovrapporre alcuna valutazione o dichiarare errata l'analisi della *Divisional Court*[450]. Sul punto, tuttavia, l'ICO ha sollevato perplessità in ragione della prassi della *South Wales Police* di impiegare le TRF durante eventi di massa, per i quali, in genere, manca una idonea attività preparatoria di *intelligence*, risulta che le *watchlist* siano costruite senza ricorrere a parametri adeguati e non pare che si miri specificatamente a ricercare persone definite[451]. In questi casi, quindi, si può dubitare che possa davvero esservi quello «*specific and limited purpose*» di cui sopra, e non si verifichi piuttosto un impiego meramente «*speculative*».

In ragione delle diverse ricostruzioni sul profilo del rispetto della vita privata di cui alla CEDU, dunque, i due giudici si collocano su posizioni antitetiche anche circa la conformità alla normativa sulla *protezione dei dati personali*, sia con riguardo alla valutazione sul rispetto delle condizioni di liceità dei trattamenti[452], sia con riguardo all'onere di esperire una valutazione di impatto[453].

[450] [2020] EWCA Civ 1058, cit., p. 131-143.

[451] INFORMATION COMMISSIONER'S OFFICE, *ICO investigation into how the police use facial recognition technology in public places*, cit., 22.

[452] Il giudice di secondo grado, invero, non entra nel merito di questo profilo, non essendo motivo di appello. Interessante al riguardo è la parte della pronuncia con cui il giudice di primo grado chiarisce di non dubitare come il citato sistema di RF implichi il trattamento di dati biometrici, non soltanto delle persone presenti nelle *watchlist*, ma anche di coloro le cui immagini vengono catturate dal vivo; cfr. [2019] EWCH 2341 (Admin), cit., p. 133.

[453] Il *Data Protection Act* del 2018, all'art. 64, impone che venga svolta una valutazione di impatto, analogamente a quanto accade con gli artt. 35 del GDPR e 27 della LED. Da quest'ultimo punto di vista, mentre la *Divisional Court* giudica sufficiente la valutazione svolta dalla *South Wales Police*, non spettando alla Corte di sostituirsi al titolare del trattamento in questa attività, bensì di operare un controllo "esterno" secondo le indicazioni fornite anche dall'*Information Commissioner* (cfr. [2019] EWCH 2341 (Admin), p. 146-148), la *Court of Appeal* ravvisa un difetto nella valutazione di impatto nella misura in cui non sono stati previsti i pericoli per la tutela della vita privata derivanti dalla eccessiva discrezionalità di cui godono le forze di polizia, secondo quanto appena chiarito ([2020] EWCA Civ 1058, cit., p. 152). Con ciò trova conferma

Da ultimo, viene in rilievo il dovere delle autorità pubbliche di garantire pari opportunità ed evitare *effetti discriminatori*[454]. La *Divisional Court* respinge la censura rivolta ai presunti effetti discriminatori indiretti derivanti dall'uso del sistema *AFR Locate* per motivi di sesso e razza, basata sul presunto maggiore tasso di falsi-positivi nelle identificazioni che coinvolgono donne, persone dalla pelle nera e appartenenti a minoranze etniche. A sostegno, il giudice di primo grado formula sostanzialmente tre argomenti: non ci sono prove evidenti che il "*Neo-Face Watch software*" alla base del sistema di riconoscimento facciale – sviluppato dall'azienda privata NEC e messo a disposizione delle forze di polizia con licenza di software proprietario – produca tali effetti e che non vi sono riscontri atti a dimostrare che i *dataset* usati per allenare gli algoritmi fossero affetti da *bias*[455]; non risulta esservi un tasso di falsi-positivi tra donne maggiore di quello riscontrabile tra gli uomini[456]; vale sempre la salvaguardia offerta dal controllo di un operatore umano a conferma dei riscontri suggeriti dalla macchina[457].

Anche su questo punto, tuttavia, la *Court of Appeal* si dimostra di ben diverso avviso, giudicando tutt'altro che assolto l'obbligo in questione delle autorità pubbliche. Queste ultime – a detta del giudice di

come la DPIA costituisca uno strumento rilevante ai fini della tutela giurisdizionale dei diritti, in grado di fornire elementi significativi a sostegno del percorso argomentativo dei giudici – ricevendo, anche nella vicenda in parola, approfonditi richiami in sede di motivazione – e, di converso, non costituisca affatto un obbligo da assolvere come mera formalità da parte delle autorità responsabili. Sulla valutazione di impatto sui dati, cenni *infra* Cap. V, par. 2.

[454] Nello specifico, si tratta del "*Public Sector Equality Duty*" all'art. 149 dell'*Equality Act 2010*, che stabilisce che un'autorità pubblica debba, nell'esercizio delle sue funzioni, avere la dovuta considerazione circa la necessità di: eliminare discriminazioni, molestie, persecuzioni e qualsiasi altra condotta proibita dalla legge; far progredire le pari opportunità e i buoni rapporti tra persone che condividono caratteristiche giuridicamente tutelate e persone che non le condividono.

[455] [2019] EWCH 2341 (Admin), cit., p. 153.

[456] Se tra il maggio 2017 e il giugno 2018 vi sono stati falsi-positivi maggiori nel caso delle donne, ciò è dovuto, in base alle informazioni rese dalle forze di polizia, a causa della presenza nelle *watchlist* delle immagini di due donne con un alto numero di caratteristiche generiche comuni (c.d. *lamb*) che tendono a confondere il software; [2019] EWCH 2341 (Admin), cit., p. 154.

[457] [2019] EWCH 2341 (Admin), cit., p. 156.

II grado – devono compiere tutti i passi che ragionevolmente si rendono necessari per prendere in considerazione l'impatto potenziale di una nuova *policy* che potrebbe produrre effetti sproporzionati verso determinate categorie di persone. Si tratta di un obbligo "di processo" e non "di risultato", che produce l'effetto di responsabilizzare i soggetti che ricorrono a simili tecnologie e di rassicurare la popolazione interessata che i propri interessi siano stati presi in debita considerazione[458]. Il fatto che si tratti di una tecnologia innovativa e che – come ritiene il giudice di I grado – non vi siano prove evidenti su effetti discriminatori non esime dall'assolvere tale obbligo positivo, anzi dovrebbe indurre ad una maggiore attenzione[459].

La *Court of Appeal* prende posizione, innanzitutto, sul meccanismo di salvaguardia sopra richiamato, stabilendo che la necessità che un essere umano confermi le decisioni della macchina non sia di per sé sufficiente ad assolvere il citato obbligo delle autorità pubbliche, dato che "anche gli esseri umani possono commettere errori"[460]. L'argomento, tuttavia, prova troppo nella misura in cui rischia di svalutare eccessivamente l'intervento umano, quand'anche possa rivelarsi sostanzialmente determinante[461].

La Corte, inoltre, dichiara che occorrerebbe poter dimostrare esplicitamente l'assenza di una sproporzione nei falsi-positivi tra donne e uomini, ma ciò non è documentabile, visto che i dati vengono eliminati istantaneamente o dopo poco tempo[462]. Anche questo rilievo si espone a critiche, dal momento che sembra difficilmente raccordabile con il principio di limitazione nella conservazione dei dati che, da una parte, impone la cancellazione dei dati non rilevanti e, dall'altra, riduce i termini temporali di conservazione di quelli per i quali il sistema segnala una corrispondenza[463].

Decisive sembrano invece le considerazioni sulla mancanza di controlli sul *dataset* impiegato per allenare l'algoritmo. In particolare, il

[458] [2020] EWCA Civ 1058, cit., p. 176.
[459] *Ivi*, p. 182.
[460] *Ivi*, p. 185.
[461] V. *retro* par. 6.3.
[462] [2020] EWCA Civ 1058, cit., p. 191.
[463] V. *retro* par. 5.3.

fatto che tali dati siano coperti da segreto commerciale impedisce di verificare la consistenza demografica del campione utilizzato. In questo modo, le forze di polizia non hanno potuto constatare, direttamente o per mezzo di una verifica indipendente, se siano o meno presenti inaccettabili *bias* che possano determinare discriminazioni per motivi di sesso o razza. Si tratta, quest'ultimo, di un obbligo inderogabile che grava sulle autorità pubbliche e che non può essere pretermesso a causa di interessi commerciali[464]. Per questo, si ritiene che la *South Wales Police* non abbia compiuto tutto ciò che ragionevolmente può essere richiesto prima di utilizzare simile «*novel and controversial technology*»[465].

In ragione degli indirizzi giurisprudenziali emersi, dunque, l'utilizzo delle TRF dal vivo è stato interdetto alle autorità gallesi ed occorrerà valutare, da una parte, se vi saranno futuri sviluppi sul piano normativo in grado di fornire copertura sufficiente all'*AFR Locate* e, dall'altra, se la *South Wales Police* sarà in grado di sottoporre ad *audit* il sistema attualmente utilizzato, superando le barriere opposte dal segreto, o sarà costretta a ricorrere ad algoritmi differenti su cui riprogettare il sistema di riconoscimento facciale. Nel frattempo, non è escluso che la *South Wales Police* possa continuare ad impiegare questa tecnologia[466], ad esempio, per finalità mirate di indagine[467], lasciando irrisolto il dibattito circa i costi e i benefici di questi mezzi innovativi. Per contribuire a porre rimedio a questo stato di incertezza, a seguito della pronuncia di secondo grado è intervenuto il *Surveillance Camera Commissioner*, autorità garante di settore che ha formulato alcuni indirizzi per orientare l'impiego di tali strumenti da parte delle forze dell'ordine[468].

[464] [2020] EWCA Civ 1058 cit., p. 199.

[465] *Ivi*, p. 201.

[466] Cfr. *UK judges: police use of facial ID is unlawful, but not banned*, in *Biometric Technology Today*, 8, settembre 2020, 3.

[467] Da ultimo, v. J. REES, *Facial recognition: How South Wales Police caught a sexual predator*, in *BBC News*, 20 febbraio 2021 [bbc.in/3mpcZv2], ove si riporta la vicenda dell'arresto a seguito di un tentativo di violenza sessuale, reso possibile grazie all'identificazione ottenuta dal confronto automatizzato tra l'immagine ripresa su un autobus pochi minuti prima del tentativo di stupro e la foto segnaletica della persona in questione raccolta più di 15 anni prima.

[468] A seguito della pronuncia di appello, il *Surveillance Camera Commissioner*, au-

9. (segue) …e alcuni spunti sull'esperienza italiana: il caso S.A.R.I.

In conclusione, tuttavia, occorre sottolineare come la vicenda appena ricostruita abbia qualcosa da dire anche all'ordinamento italiano. Il sistema utilizzato dalla *South Wales Police*, infatti, richiama molto da vicino il S.A.R.I. (Sistema Automatico di Riconoscimento Immagini) a disposizione – come già accennato[469] – in Italia del Ministero dell'interno[470]. Anche il SARI presenta due modalità simili a quelle dell'AFR. La prima è il SARI *Real Time*, non ancora in uso, ma che, analogamente al *AFR Locate*, offrirebbe una funzione di supporto a operazioni di controllo sul territorio in occasione di eventi e manifestazioni; le immagini riprese dal vivo verrebbero infatti confrontate con delle *watchlist* create in corrispondenza dell'evento in questione, generando degli *alert* in caso di eventuali corrispondenze. La seconda è il SARI *Enterprise*, in uso dal settembre 2018, attraverso il quale viene confrontata un'immagine con le fotografie presenti nell'"A.F.I.S. – S.S.A.", il sistema automatizzato di identificazione delle impronte digitali, integrato dal "Sottosistema anagrafico" contenente circa una decina di milioni di foto segnaletiche con le relative informazioni anagrafiche e descrittive – sistema che in futuro potrà essere integrato con una serie di altre banche dati gestite a livello di Unione europea, ampliando enormemente il volume delle immagini processabili[471]. In entrambi i casi spetta ad un operatore di polizia il compito di convalidare i risultati proposti dal confronto automatizzato, giudicando a partire

torità indipendente istituita ai sensi del *Protection of Freedoms Act 2012*, con la funzione di favorire il rispetto e fornire pareri in ordine all'attuazione del "*Surveillance Camera Code of Practice*" – il quale, lo si ricorda, secondo la *Divisional Court*, contribuiva ad offrire una base normativa sufficiente alle pratiche della *South Wales Police* –, nel novembre 2020 ha adottato il documento "*Facing the Camera*", recante "*Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales*".

[469] V. *retro* par. 6.3.

[470] Più ampiamente, v. R.V.O. VALLI, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati da immagini*, cit.; R. LOPEZ, *La rappresentazione facciale tramite* software, in A. SCALFATI (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2019, 239 ss.

[471] V. *infra* Cap. IV, par. 6.

dal punteggio riportato dal *set* di immagini proposte, ovvero la percentuale di somiglianza individuata dal sistema in ordine decrescente.

A fronte del riserbo sulle specifiche tecniche di funzionamento del SARI, la cui conoscenza potrebbe comprometterne l'efficacia e la sicurezza[472], e per quanto quindi si può ricavare dalle informazioni contenute nel capitolato tecnico della gara di appalto per la realizzazione del sistema stesso[473], è possibile osservare come alcuni aspetti del SARI sollevino qualche perplessità, anche alla luce delle ragioni sottostanti gli indirizzi giurisprudenziali sopra riportati.

La criticità principale è dovuta all'assenza di un fondamento legislativo che nell'ordinamento italiano disciplini adeguatamente le condizioni di utilizzo di tale strumento. Il Garante della *privacy* – si ricorda – ha già avuto occasione di pronunciarsi sul SARI *Enterprise*[474], stabilendo come il relativo impiego non costituisca un nuovo trattamento di dati personali, diverso da quello previsto e disciplinato al d.m. del 24 maggio 2017, bensì «una diversa modalità di trattamento di dati biometrici» disciplinata dalla normativa vigente[475]. Diversamente è andata per il SARI *Real Time*, sul quale pure il Garante si è più di recente pronunciato, con un parere però di tutt'altro avviso[476].

Chiamato dal Ministero dell'interno a dare il via libera su un suo possibile impiego nel prossimo futuro, il Garante ha chiarito come simile «trattamento di immagini volte ad identificare le persone nel contesto pubblico [sia] di estrema delicatezza», risolvendosi in un trattamento che coinvolge non solo i dati biometrici di chiunque sia sotto-

[472] Secondo quanti riportato in R. COLUCCINI, *Lo scontro Viminale-Garante della privacy sul riconoscimento facciale in tempo reale*, in *Irpi*, 13 gennaio 2021 [bit.ly/3wEpXcT], a seguito di una richiesta di accesso civico *ex* d.lgs. n. 33/2013 ai documenti in possesso del Ministero dell'interno.

[473] Gara che si è aggiudicata l'azienda Parsec 3.26. Per il documento in questione, cfr. MINISTERO DELL'INTERNO, DIPARTIMENTO DELLA PUBBLICA SICUREZZA, *Capitolato tecnico. Procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini S.A.R.I. Lotto n° 1*, disponibile su: [bit.ly/2Rajq9D]

[474] V. *retro* par. 6.3.

[475] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell'identità di un volto*, cit.

[476] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, 25 marzo 2021, sulla base dei documenti trasmessi relativi alla valutazione di impatto sulla protezione dei dati.

posto a riconoscimento tra la folla, seppure non oggetto di attenzione da parte delle forze dell'ordine, ma anche i dati "particolari" idonei a rivelare, ad esempio, le opinioni politiche o l'appartenenza sindacale di chi venisse identificato in occasione di manifestazioni pubbliche. Come tale, occorre un solido fondamento normativo che disciplini tale trattamento e soddisfi così i requisiti imposti dall'art. 7 della CEDU e l'art. 52 CDFUE, oltre che dall'art. 10 della LED, l'art. 9 del GDPR e l'art. 7 del d.lgs. n. 51/2018, il quale prevede che il trattamento sia «specificatamente previsto» dal diritto dell'UE o da legge. Le molteplici disposizioni invocate dal Ministero a supporto dell'impiego del SARI *Real Time* vengono giudicate dal Garante inadatte allo scopo: né l'art. 1 del t.u.l.p.s., che stabilisce in generale i compiti dell'autorità di pubblica sicurezza; né il più volte richiamato d.P.R. n. 15/2018, che – come detto, oltre a generare non semplici questioni ermeneutiche e di compatibilità con il nuovo quadro legislativo[477] – reca sì una disciplina specifica sui sistemi di sorveglianza e le riprese video-fotografiche, i quali però vengono definiti «sistemi ontologicamente diversi da quelli dei dati biometrici»[478]; né le previsioni del codice di procedura penale, parimenti ritenute inconferenti[479].

Viceversa, secondo il Garante, occorrerà adottare una base legislativa che, «in esito alla ponderazione di tutti i diritti e le libertà coinvolti», valga fra l'altro a «rendere adeguatamente prevedibile l'uso di tali sistemi, senza conferire una discrezionalità così ampia che il suo utilizzo dipenda in pratica da coloro che saranno chiamati a disporlo»[480] –

[477] V. *retro* nota 41.

[478] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, cit., p. 2.

[479] Si ha riguardo agli artt. 134 c. 4, 234, 266, 431 c. 1, lett. b, e agli artt. 55, 348, 354 e 370 del c.p.p., riguardanti, rispettivamente, la documentazione degli atti per riproduzione audiovisiva, l'acquisizione di scritti o altri documenti mediante fotografia, cinematografia, fonografia ed altri mezzi, l'intercettazione di comunicazioni tra presenti mediante dispositivi elettronici portatili, l'intercettazione di flussi di comunicazioni telematiche, le funzioni di polizia giudiziaria nell'assicurare le fonti di prova e nel condurre accertamenti su luoghi o persone, di iniziativa o su delega dell'autorità giudiziaria.

[480] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, cit., p. 3.

una chiara assonanza rispetto al verdetto in appello sopra ricostruito reso dalla *High Court of Justice*.

Allo stato, si potrebbe dire, non risulta esservi una disciplina che consenta di rispondere alla "*who question*", ovvero che specifichi i criteri per comporre le *watchlist* o determinare le tipologie di illecito verso cui può essere utilizzato il sistema[481]; parimenti, anche la "*where question*", riguardante i luoghi nei quali impiegare il sistema, rimane inevasa.

In assenza di un riferimento normativo tarato sulle peculiarità di queste tecnologie, dunque, il riconoscimento facciale potrebbe essere impiegato dalle forze dell'ordine in circostanze e per finalità molto differenti, con forti dubbi in punto di rispetto del principio di proporzionalità: un conto, infatti, è utilizzare tali tecnologie a scopo mirato per identificare una persona già sottoposta a fermo, operando un confronto con una galleria di immagini riguardanti soggetti, ad esempio, noti per determinati reati; altro è impiegare queste tecnologie dal vivo o tramite telecamere a circuito chiuso, come accade ad esempio all'interno degli stadi[482], per identificare soggetti tra la folla, operando eventualmente un confronto con un *database* contenente milioni di immagini[483]. La disponibilità di tali strumenti, quindi, getta una luce diversa anche sulla disciplina relativa alla flagranza per i reati commessi in occasione di manifestazioni sportive, secondo cui si è considerati in stato di flagranza anche a distanza di giorni, qualora il soggetto che ha compiuto il reato, «sulla base di documentazione video fotografica o di altri elementi oggettivi dai quali emerga inequivocabilmente il fatto, ne risulta autore»[484].

[481] Come rilevato anche *ibidem*.

[482] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema di videosorveglianza presso lo Stadio Olimpico. Verifica preliminare*, 28 luglio 2016. Più ampiamente, v. anche S. CARAVACA, *Il riconoscimento facciale negli stadi di calcio, tra privacy e sicurezza*, in *Risk Management 360*, 2 aprile 2021 [bit.ly/32qjdRX], anche per una serie di esempi di società sportive estere che fanno ricorso a queste tecnologie.

[483] Sono i due scenari qualificati come "a rischio moderato" e "a rischio molto alto" in C. GARVIE ET AL., *The Perpetual Line-Up. Unregulated Police Face Recognition in America*, cit., 19 ss.

[484] Art. 1, d.l. 24 febbraio 2003, n. 28, convertito con modificazioni dalla legge 24 aprile 2003, n. 88. Sul punto, v. P. CARETTI, G. TARLI BARBIERI, *I diritti fondamentali. Libertà e diritti sociali*, cit., 268.

Vi sono però ulteriori rilievi che possono essere mossi al SARI: si pensi alle incertezze legate a possibili effetti discriminatori in mancanza di verifiche circa l'assenza di *bias* negli algoritmi da esso integrati[485]; ad un difetto di trasparenza in ordine all'accuratezza del sistema[486] e alle eventuali conseguenze per gli interessati in caso di falsi-positivi[487]; alla mancata diffusione dei risultati di una analisi dei rischi condotta tramite una puntuale valutazione di impatto sui dati personali[488].

Non solo, ma tali strumenti di riconoscimento facciale sono suscettibili di essere ulteriormente implementati, sia come possibilità di ampliare il *database* attraverso ulteriori dati biometrici con i quali operare il confronto[489], sia come possibili utilizzi in ambiti e per finalità ulteriori, come l'identificazione dei migranti durante le operazioni di sbarco[490]. Non stupisce, quindi, che il SARI sia stato oggetto di alcuni atti di sindacato ispettivo in Parlamento per chiedere chiarimenti al Ministero dell'interno e valutare la possibilità di una moratoria sul relativo impiego[491], ai quali ha fatto seguito anche la presentazione di una pro-

[485] Profilo rilevato anche in GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, cit., p. 3.

[486] Cfr. J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della* High Court of Justice, cit., 243.

[487] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, cit., p. 3.

[488] Riferimenti *infra* Cap. V, par. 5.

[489] Sul punto, a proposito del SARI *Enterprise*, il capitolato fa riferimento ad un sistema di ricerca automatico «per mezzo di uno o più algoritmi di riconoscimento facciale, all'interno di una banca dati di grandi dimensioni (dell'ordine di milioni di immagini) di soggetti foto segnalati o *di altre banche dati*» (6, enfasi aggiunta). Cfr. R.V.O. VALLI, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati da immagini*, cit., che sottolinea i rischi legati alla possibilità di integrare la banca dati utilizzata da SARI *Real time* con immagini reperite dai social network, in mancanza di standard minimi qualitativi.

[490] Più in particolare, come riportato da in R. COLUCCINI, *Lo scontro Viminale-Garante della privacy sul riconoscimento facciale in tempo reale*, cit., si tratta della possibilità di utilizzare SARI *Enterprise* anche per verificare l'autenticità delle foto nei documenti e SARI *Real Time* come «sistema tattico per monitorare le operazioni di sbarco e tutte le varie tipologie di attività illegali correlate, video riprenderle ed identificare i soggetti coinvolti».

[491] Cfr. CAMERA DEI DEPUTATI, XVIII legislatura, Interpellanza urgente 2/01109, 22 febbraio 2021; Interrogazione a risposta immediata in Assemblea 3/02074, 3 marzo

posta di legge al riguardo[492]. Riprendendo le parole del Garante della *privacy* nell'ultima pronuncia sopra richiamata, il rischio è che tali sistemi siano in grado di produrre una «evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui»[493].

2021, con le repliche del Ministro dell'interno.

[492] Cfr. CAMERA DEI DEPUTATI, XVIII legislatura, A.C. 3009, *Sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici in luoghi pubblici o aperti al pubblico*.

[493] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, cit., p. 3.

CAPITOLO IV

TRF E NUOVE FRONTIERE DI SVILUPPO: I SISTEMI DI INFORMAZIONE EUROPEI

SOMMARIO: 1. Considerazioni introduttive: fronteggiare gli effetti del c.d. *function creep*. – 2. Il Sistema d'informazione Schengen (SIS). – 3. Il Sistema *European dactylographic* (EURODAC). – 4. Il Sistema di informazione visti (VIS). – 5. Il Sistema di ingressi/uscite (EES). – 6. I c.d. regolamenti "interoperabilità": verso una sempre maggiore integrazione dei dati… – 7. (*segue*) …e una maggiore integrazione delle criticità.

1. *Considerazioni introduttive: fronteggiare gli effetti del c.d.* function creep

Quella ricostruita nel Capitolo precedente è la regolamentazione dei dati personali che assume una portata trasversale rispetto a tutti i settori materiali e alle singole applicazioni con cui le TRF possono essere impiegate. Essa, dunque, funge da *lex generalis* sulla quale costruire ogni ulteriore disciplina giuridica che riguardi queste tecnologie. È sempre a livello di UE, tuttavia, che è possibile rintracciare i riferimenti normativi quantitativamente più consistenti alle TRF e che fungono da *leges speciales* rispetto al GDPR e alla LED[1].

Si tratta della disciplina riguardante i principali sistemi di scambio di dati e informazioni all'interno dell'UE. Questi sistemi sono strutturati in *database* gestiti a livello centralizzato e in *network* che pongono in collegamento istituzioni e organismi dell'Ue con gli Stati membri[2].

[1] Questo inquadramento tra *lex generalis* e *lex specialis* è offerto dal Garante europeo della protezione dei dati, ad esempio, nel parere relativo alle proposte di riforma del SIS II (2006/C 91/11), p. 2.2, su cui v. *infra*.

[2] V. COMMISSIONE EUROPEA, comunicazione al Parlamento europeo ed al Consiglio, *Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia*, 20.07.2010 COM(2010) 385 def., ove si distingue tra sistemi centralizzati, quali SIS, VIS, EURODAC, SID (Sistema Informativo Doganale), Europol e Eurojust, e sistemi decentralizzati, come quelli ai sensi della Convenzione di Prüm e della

In particolare, ai fini del presente discorso, vale la pena concentrarsi proprio su quei sistemi che trattano immagini del volto da sottoporre a TRF, o che lo faranno in un futuro prossimo in forza delle modifiche oggi in discussione[3]. Non saranno oggetto di attenzione, invece, quei sistemi decentralizzati che si basano solamente sulla trasmissione di informazioni tra Stati, a partire da quello istituito dal Trattato di Prüm, oggi europeizzato[4]: anche quest'ultimo, in prospettiva, potrà integrare lo scambio di immagini facciali, sebbene la discussione in proposito si trovi ancora ad uno stato non sufficientemente avanzato[5].

"Swedish initiative". La distinzione tra strumenti "interni" ed "esterni" all'UE, in chiave politologica, è affermata anche da T. BALZACQ, *The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies*, in *Journal of Common Market Studies*, 46, 1, 2008, 83 ss., ove si indica come strumenti "interni" EURODAC, SIS e VIS e come strumenti esterni gli *Europol-USA Agreements* e il PNR. All'interno dello spazio di libertà, sicurezza e giustizia, opera una distinzione dei sistemi di scambio tra Ue e Stati membri anche M. TZANOU, *The EU as an emerging "Surveillance Society": The function creep case study and challenges to privacy and data protection*, in *Vienna Journal on International Constitutional Law*, 4, 3, 2010, 411 s., che li differenzia dai sistemi basati su scambi tra Stati a partire da accordi intergovernativi, come il Trattato di Prüm, su cui v. *infra* nota 4.

[3] Una prima ricognizione è offerta in FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., 13 ss.

[4] Il sistema istituito dal Trattato di Prüm favorisce lo scambio su larga scala di impronte digitali, profili ricavati dal DNA e dati di immatricolazione dei veicoli a scopi di polizia e sicurezza nazionale. Sottoscritto a Prüm il 27 maggio 2005, da Belgio, Germania, Spagna, Francia, Lussemburgo, Paesi Bassi e Austria, questo accordo internazionale ha infatti ad oggetto «l'approfondimento della cooperazione transfrontaliera, in particolare al fine di lottare contro il terrorismo, la criminalità transfrontaliera e la migrazione illegale». Ratificato dal Parlamento italiano con la legge 30 giugno 2009, n. 85, esso prevede l'istituzione di una banca dati nazionale del DNA (art. 5 ss.) e la disciplina per il prelievo e il trattamento dei campioni biologici (artt. 9 ss.) (v. *retro* Cap. II, par. 5). Con le decisioni 2008/615/GAI e 2008/616/GAI del 23 giugno 2008, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera, il Trattato di Prüm e stato poi integrato nel diritto UE. In dottrina, v. O. SALLAVACI, *Strengthening cross-border law enforcement cooperation in the EU: the Prüm network of data exchange*, in *European Journal on Criminal Policy and Research*, 24, 2018, 219 ss.

[5] Sul punto, v. L. SCAFFARDI, Next Generation Prüm *e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, in *Federalismi.it*, 8, 2021, 200 ss.; N. VAVOULA, *Police Information Exchange*

Ciò che accomuna tutti questi sistemi, oltre al trattamento di questa particolare tipologia di dati biometrici, è anche la tendenza, riscontrata fin dalla loro istituzione, a quello che in ambito tecnologico viene definito come "*function creep*", o "scorrimento di funzioni", ovvero un incremento di funzionalità che ne ha arricchito o, sotto diversi punti di vista, snaturato lo scopo iniziale. Questa apertura, che in particolare è andata a beneficio delle forze dell'ordine, solleva problematiche giuridiche di non poco conto che occorre approfondire per cogliere gli sviluppi futuri che interesseranno le TRF.

Tale scorrimento verso nuove funzioni può essere distinto in diverse periodizzazioni, scandite grossomodo da eventi terroristici o emergenze che hanno indotto le istituzioni europee e gli Stati membri a do-

The future developments regarding Prüm and the API Directive, PE 658.542, *Study Requested by the LIBE committee*, settembre 2020, spec. 25 ss. Le inefficienze, i ritardi e le difficoltà operative che hanno caratterizzato l'attuazione delle citate decisioni 2008/615/GAI e 2008/616/GAI, unitamente al progresso tecnologico al sevizio sia delle tecniche investigative, sia del terrorismo e della criminalità, hanno indotto le istituzioni europee ad avviare alcune iniziative volte a modernizzare tali decisioni, come emerso nelle "Conclusioni del Consiglio sull'attuazione delle "Decisioni Prüm" a dieci anni dall'adozione" (Conclusioni n. 11227/18 del 8 luglio 2018). L'intenzione è quella di innovare le regole in materia di circolazione e scambio di dati per estenderne l'ambito di applicazione; implementare le connessioni tra il sistema Prüm e altri meccanismi di cooperazione transfrontaliera in materia di indagine e lotta alla criminalità (fra cui quelli discussi nel presente Capitolo); ampliare le categorie di dati incluse nel meccanismo di scambio, includendovi anche le immagini facciali. Più ampiamente, si veda lo studio di fattibilità commissionato dalla Commissione a Deloitte, che su quest'ultimo profilo sollecita una serie di misure: l'adozione di standard comuni di qualità; la definizione di un numero minimo e massimo di immagini da trasferire per ciascuna ricerca, in rapporto alla soglia di errore impostata negli algoritmi; la necessità che in caso di "*no match*" i dati vengano cancellati in tempi brevi; stabilire un set di dati statistici in relazione a ciascuno scambio di informazioni (cfr. DELOITTE, *Study on the Feasibility of Improving Information Exchange under the Prüm Decisions. Advanced technical report*, maggio 2020, 77 ss.). Viene inoltre richiamata l'attenzione sullo stato dell'arte in queste tecnologie, soprattutto in punto di condizionamenti derivanti dalla qualità dei dati, a partire dagli effetti del decorso del tempo dei soggetti ripresi e la minor accuratezza nei confronti delle persone nere e delle donne (*ivi*, 143 ss.). Si sollecita inoltre l'importanza di rivedere il sistema di scambio dei dati ove, attualmente, prevede un sistema di *hit/no hit* basato in due fasi (per questo sistema v. *infra*), in quanto giudicato troppo dispendioso di tempo e risorse (*ivi*, 61 ss.).

tarsi, in risposta, di strumenti tecnologici di sorveglianza più penetranti, basati soprattutto sul trattamento di dati biometrici[6]. Dal momento che questi sistemi informativi vengono concepiti inizialmente per scopi differenti, ma vivono poi una sostanziale convergenza verso obiettivi comuni, sarà opportuno procedere ad una loro disamina distinta per comprendere le ragioni e la portata di questo percorso evolutivo. Il risultato finale ha contribuito a quella che è stata definita efficacemente come la "digitalizzazione della politica europea di immigrazione"[7], ma anche alla confusione tra gestione dell'immigrazione e contrasto al crimine e al terrorismo[8].

Già introduttivamente, però, merita segnalare anche una seconda traiettoria che muove lo sviluppo e la gestione di questi sistemi, che va nella direzione di una progressiva integrazione e interoperabilità delle rispettive banche dati. Sebbene non ancora pienamente portata a termine, questa imponente architettura dell'informazione, una volta a regime, consentirà di confrontare le immagini facciali catturate dalle forze dell'ordine nei più disparati contesti di vita – come visto introduttivamente – con i dati contenuti nei diversi *database* a livello europeo, ampliando a dismisura le potenzialità di controllo cui ciascuno di essi è preposto, ad esempio, in ambito migratorio, nel rilascio dei visti, nelle richieste di asilo, e persino nella più generale tutela della sicurezza pubblica. Un disegno che, se portato a termine, cambierà il modo stesso di concepire la tutela dei dati personali.

[6] Per una efficace ricostruzione, v. N. VAVOULA, *Databases for Non-EU Nationals and the Right to Private Life: Towards a System of Generalised Surveillance of Movement?*, in F. BIGNAMI (a cura di), *EU Law in Populist Times*, Cambridge University Press, Cambridge, 2020, 227 ss.; E. BROUWER, *Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection*, in *European public law*, 26, 1, 2020, 71 ss. Per una panoramica v. anche V. FERRARIS, *Il migrante datificato nei confini del futuro: senza potere di fronte a un oscuro potere?*, in S. GOZZO, C. PENNISI, V. ASERO, R. SAMPUGNARO (a cura di), *Big Data e processi decisionali. Strumenti per l'analisi delle decisioni giuridiche, politiche economiche e sociali*, Egea, Milano, 2020, 136 ss.

[7] M. BESTERS, F.W.A. BROM, *"Greedy" Information Technology: The Digitalization of the European Migration Policy*, in *European Journal of Migration & Law*, 12, 4, 2010, 462 ss.

[8] A questo proposito si parla efficacemente di "*crimmigration*", secondo il termine coniato da J.P. STUMPF, *The Crimmigration Crisis: Immigrants, Crime, and Sovereign Power*, in *American University Law Review*, 56, 2, 2016, 367 ss.

2. *Il Sistema d'informazione Schengen (SIS)*

Il primo tra i sistemi in questione ad essere stato ideato è il "Sistema d'informazione Schengen" (SIS), concepito contestualmente all'adozione della Convenzione di Schengen. Esso rappresenta la controparte al venir meno delle frontiere fisiche all'interno dell'area Schengen, nella necessità di definire un sistema di previsioni comuni volte a rafforzare i *controlli alle frontiere esterne* dell'Unione e la *sicurezza pubblica al suo interno*[9]. Dopo l'integrazione dell'*acquis* di Schengen in ambito UE con il Trattato di Amsterdam e la modifica della competenza in giustizia e affari interni originariamente introdotta dal Trattato di Maastricht, il fondamento normativo del SIS è stato ripartito tra il "primo" e il "terzo pilastro"[10]. Oggi, con il Trattato di Lisbona, tale sistema si colloca all'interno dello "spazio di libertà sicurezza e giustizia", fondato sull'art. 3 del TUE e al Titolo V del TFUE[11].

Grazie soprattutto alla evoluzione degli strumenti tecnologici con cui identificare i soggetti che transitano dai confini[12], e sotto la pressione degli atti terroristici dell'11 settembre 2001 e degli attentati di Madrid e Londra nel 2004 e 2005[13], il SIS, da strumento creato origi-

[9] Il Titolo IV della Convenzione di Schengen del 19 giugno 1990 è dedicato al "Sistema d'informazione Schengen". Ai sensi dell'art. 93 il suo scopo è quello «di preservare l'ordine pubblico e la sicurezza pubblica, compresa la sicurezza dello Stato e di assicurare l'applicazione, nel territorio delle Parti contraenti delle disposizioni sulla circolazione delle persone stabilite nella presente Convenzione».

[10] Cfr. P.J. KUIJPER, *Some legal problems Associated with the Communitarization of Policy on Visas, Asylum and Immigration under the Amsterdam Treaty and Incorporation of the Schengen Acquis*, in *Common Market Law Review*, 37, 2, 2000, 345 ss.

[11] Più in generale, sulla evoluzione dello spazio di libertà sicurezza e giustizia, v. B. NASCIMBENE, *Riflessioni sullo spazio di libertà, sicurezza e giustizia*, in *Studi sull'integrazione europea*, 3, 2017, 17 ss., e i richiami bibliografici ivi citati. Sul SIS, v. specificatamente anche F. DECLI, G. MARANDO, *Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia*, in F. PERONI, M. GIALUZ (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, EUT, Trieste, 2009, 106 ss., e gli atti ivi citati.

[12] L. MUSSELLI, *Alcune prime considerazioni sui sistemi di scambio di informazioni nello spazio di libertà, sicurezza e giustizia: securitization, function creep e tutela dei diritti*, Centro Studi sul Federalismo, Research Paper, maggio 2013, 10.

[13] A seguito di tali eventi la gestione delle frontiere e il controllo dell'immigrazione si è strettamente intrecciata con la lotta al terrorismo, come rileva

nariamente per il controllo delle frontiere, ha marcato sempre più il carattere di strumento di *indagine a tutela della sicurezza interna* degli Stati[14]. Il regolamento CE n. 1987/2006 del 20 dicembre 2006 e la decisione 2007/533/GAI del 12 giugno 2007, hanno infatti sviluppato un sistema d'informazione Schengen di seconda generazione (c.d. SIS II) con uno scopo caratterizzato maggiormente in quest'ultimo senso[15], accrescendo le relative *funzionalità* e possibilità di *accesso* da parte di autorità pubbliche[16]. Mentre originariamente il SIS ospitava in prevalenza informazioni di carattere alfanumerico, il sistema è andato successivamente ampliandosi con dati biometrici quali impronte digitali e fotografie[17]. Alla sola possibilità di verificazione uno-a-uno, inoltre, è stata aggiunta la possibilità di operare identificazioni secondo la logica uno-a-molti, trasformando il SIS da strumento di controllo a strumento investigativo ad ampio spettro nei confronti di una popolazione indeterminata di possibili sospettati[18].

A. BALDACCINI, *Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases*, in *European Journal of Migration and Law*, 10, 2008, 32 ss.

[14] M. TZANOU, *The EU as an emerging "Surveillance Society": The function creep case study and challenges to privacy and data protection*, cit., 411 s. Cruciale è stata l'esplicitazione del "principio di disponibilità" operata dal *Programma dell'Aia: rafforzamento della libertà, della sicurezza e della giustizia nell'unione europea* (2005/C 53/01), nell'ambito dell'obiettivo del "rafforzamento della sicurezza", secondo cui «in tutta l'Unione, un ufficiale di un servizio di contrasto di uno Stato membro che ha bisogno di informazioni nell'esercizio delle sue funzioni può ottenere tali informazioni da un altro Stato membro, e [...] il servizio di contrasto nell'altro Stato membro che dispone di tali informazioni è tenuto a trasmettergliele per i fini dichiarati, tenendo conto dei requisiti relativi alle indagini in corso nel suddetto Stato» (p. 2.1).

[15] Questa duplice finalità del controllo dell'immigrazione e il mantenimento dell'ordine pubblico e della sicurezza rifletteva la duplice base normativa, costituita sia da uno strumento legislativo appartenente al "primo pilastro" (TCE), sia da un atto del "terzo pilastro" (Titolo VI TUE) cfr. F. DECLI, G. MARANDO, *Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia*, cit., 110.

[16] Come rilevato anche dal Garante europeo della protezione dei dati, nel parere sulle proposte dei due atti citati nel testo (2006/C 91/11, p. 3).

[17] Art. 20, par. 2, lett. e, e art. 22, del regolamento CE n. 1987/2006 e della decisione 2007/533/GAI.

[18] A. BALDACCINI, *Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases*, cit., 37 s.

Gli eventi terroristici in Francia del novembre 2015 e in Belgio nel marzo 2016 hanno impresso una nuova accelerazione nello scivolamento dei sistemi informativi UE verso un carattere schiettamente centralizzato e investigativo[19]. Dopo la riforma del "Codice frontiere Schengen" del 2016[20], il SIS II è stato ulteriormente modificato nel 2018 e il suo ambito di applicazione è ora definito da tre regolamenti distinti, che entreranno in vigore definitivamente prima del 28 dicembre 2021 a sostituzione del SIS II, rispettivamente nei settori della cooperazione di polizia e giudiziaria in ambito penale[21], dei controlli alle frontiere[22], del rimpatrio di cittadini di Paesi terzi il cui soggiorno è irregolare[23].

Il SIS mantiene una architettura complessa[24], che garantisce acces-

[19] Cfr. N. VAVOULA, *Databases for Non-EU Nationals and the Right to Private Life: Towards a System of Generalised Surveillance of Movement?*, cit., 243 ss., che richiama la comunicazione della Commissione "*the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union*", COM/2016/0230 final.

[20] Cfr. regolamento (UE) n. 2016/399, su cui v. in generale G. CELLAMARE, *Schengen (sistema di)*, in *Enc. dir.*, Annali X, 2017, 845 ss.

[21] Regolamento (UE) 2018/1862 del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione.

[22] Regolamento (UE) 2018/1861 del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006.

[23] Regolamento (UE) 2018/1860 del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare.

[24] Il SIS si articola in un network di SIS nazionali (N-SIS), situati presso ciascuno Stato membro e dotati di un'interfaccia nazionale uniforme (NI-SIS), e in un *database* a livello centrale (C-SIS), localizzato a Strasburgo, con il compito di trasferire e standardizzare i dati. Il sistema si articola in un'infrastruttura di comunicazione che fornisce una rete virtuale cifrata dedicata ai dati SIS e provvede allo scambio di informazioni tra gli uffici della rete SIRENE (*Supplementary Information Request at the National Entries*), quale strumento ausiliario del SIS, i cui uffici sono collocati a livello nazionale per fornire tutta una serie di informazioni supplementari in relazione alle se-

so ai dati ad una pluralità di autorità nazionali per il perseguimento delle rispettive finalità: controlli di frontiera, controlli doganali, contrasto ai reati di terrorismo, altri reati gravi o esecuzione di sanzioni penali[25], decisioni in materia di ingresso e soggiorno di cittadini di Paesi terzi, controlli di sicurezza sui cittadini di Paesi terzi che chiedono la protezione internazionale[26] – un ampio spettro di finalità, dalle quali rimane esclusa l'immigrazione, a differenza dei sistemi che si vedranno nel prosieguo.

Quanto alla disciplina sul trattamento dei dati, ciascun regolamento contiene numerose disposizioni di identico tenore[27], a partire dalla necessità di rispettare il principio di proporzionalità per giustificare l'interrogazione del SIS tramite una richiesta di segnalazione[28]; si aggiungono le previsioni su la sicurezza[29], la protezione[30] e la conserva-

gnalazioni. La procedura di interrogazione automatica è fondata su un sistema *hit/no hit*, in forza del quale, una volta accertata la presenza del dato nel sistema, ulteriori informazioni possono essere fornite dai competenti uffici nazionali SIRENE. In Italia, l'ufficio N-SIS e l'ufficio SIRENE sono attualmente collocati presso il Dipartimento della Pubblica Sicurezza del Ministero dell'Interno, rispettivamente Servizio per il Sistema Informativo Interforze e Servizio per la Cooperazione Internazionale di Polizia (d.m. 2 luglio 2019). L'agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) ha la responsabilità sulla gestione del SIS centrale, l'infrastruttura di comunicazione, il coordinamento degli uffici SIRENE, la definizione delle norme di sicurezza (Capo III, entrambi i reg.).

[25] A patto che si applichi la direttiva (UE) 2016/680, su cui v. *infra*.

[26] Altre funzioni sono quelle legate alla attività immatricolazione di veicoli e registrazione di armi da fuoco, squadre della guardia di frontiera e costiera europea, squadre di personale che assolvono compiti attinenti al rimpatrio e dei membri delle squadre di sostegno per la gestione della migrazione, nonché ad Europol ed Eurojust; così artt. 44-50, regolamento (UE) 2018/1862, ma v. anche artt. 34-39 regolamento (UE) 2018/1861.

[27] Nel caso del regolamento (UE) 2018/1860 (SIS-rimpatri), ove non diversamente previsto, si fa ampio rinvio espresso al regolamento (UE) 2018/1861 (SIS-frontiere) quanto a l'inserimento, il trattamento e l'aggiornamento delle segnalazioni, le disposizioni riguardanti le competenze degli Stati membri e di eu-LISA, le condizioni relative all'accesso, il periodo di riesame delle segnalazioni, il trattamento dei dati, la protezione dei dati, la responsabilità, il monitoraggio e le statistiche (art. 19).

[28] Art. 21, che parla di adeguatezza, pertinenza e importanza del caso.

[29] Ovvero per quanto riguarda la sicurezza (art. 10), la tenuta dei registri (art. 12).

zione dei dati[31]. Le autorità nazionali di controllo indipendenti sono preposte al controllo della liceità del trattamento dei dati personali nel SIS da parte degli Stati membri[32].

Rispetto alle categorie dei dati trattati, invece, merita sottolineare come, allo scopo di creare una segnalazione di persone ricercate o di oggetti (SIS-polizia)[33], o di respingimento, rifiuto di soggiorno o provvedimenti restrittivi (SIS-frontiere)[34], o di rimpatrio (SIS-rimpatri)[35], il sistema può adesso archiviare e lanciare ricerche usando come parametro anche le immagini dei volti[36]. Nel rispetto di norme minime di qualità dei dati e specifiche tecniche[37], tali immagini possono essere utilizzate allo scopo di interrogare il SIS per confermare l'identità di una persona reperita grazie ad una prima interrogazione attraverso dati alfanumerici; come elemento di *conferma*, dunque, e non come unico elemento di identificazione[38].

Nel considerando 20 dei regolamenti SIS-polizia e SIS-frontiere,

[30] Artt. 66-71 regolamento (UE) 2018/1862, e art. 51-57 regolamento (UE) 2018/1861, concernenti la legislazione applicabile, il diritto di accesso, la rettifica di dati inesatti e la cancellazione di dati archiviati illecitamente, la possibilità di proporre un reclamo dinanzi a un'autorità di controllo o di proporre ricorso giurisdizionale, i mezzi d'impugnazione.

[31] Le segnalazioni di persone e oggetti sono conservate esclusivamente per il periodo necessario a realizzare le finalità per le quali sono state inserite (artt. 53 e 54 regolamento (UE) 2018/1862; art. 39 regolamento (UE) 2018/1861, nei termini ivi specificati).

[32] Art. 69 regolamento (UE) 2018/1862; art. 55 regolamento (UE) 2018/1861.

[33] Nello specifico, si tratta di persone ricercate per l'arresto, persone scomparse o persone vulnerabili a cui deve essere impedito di viaggiare, persone ricercate per presenziare ad un procedimento giudiziario, persone e oggetti ai fini di controlli discreti, controlli di indagine o controlli specifici, oggetti a fini di sequestro o di prova in un procedimento penale, di ignoti ricercati a fini di identificazione in conformità del diritto nazionale (artt. 26, 32, 34, 36, 38 e 40, regolamento (UE) 2018/1862).

[34] Artt. 24 e 25, regolamento (UE) 2018/1861.

[35] Art. 4, par. 1, lett. u, regolamento (UE) 2018/1860.

[36] Art. 20, par. 2, lett. w, regolamento (UE) 2018/1862.

[37] Art. 42 regolamento (UE) 2018/1862; art. 32 regolamento (UE) 2018/1861.

[38] Art. 43, par. 1, regolamento (UE) 2018/1862; art. 33, par. 1, regolamento (UE) 2018/1861. In questo senso sono state accolti i rilievi formulati dall'European Data Protection Supervisor nella sua *Opinion 7/2017*, *on the new legal basis of the Schengen Information System*, 2 maggio 2017, n. 19.

inoltre, si dà conferma che l'inserimento e l'utilizzo nel SIS delle immagini dei volti «dovrebbe essere limitato a quanto necessario ai fini degli obiettivi perseguiti, dovrebbe essere autorizzato dal diritto dell'Unione, dovrebbe avvenire nel rispetto dei diritti fondamentali, in particolare dell'interesse superiore del minore, e dovrebbe essere conforme alla normativa dell'Unione in materia di protezione dei dati». Quanto propriamente alle tecniche di riconoscimento facciale, si dispone che «non appena ciò diviene tecnicamente possibile, e garantendo al contempo un grado elevato di affidabilità dell'identificazione, è possibile ricorrere a fotografie e immagini del volto per identificare una persona presso valichi di frontiera regolari»[39].

Non appena possibile, dunque, il riconoscimento facciale potrà diventare legittimamente uno degli strumenti principali per realizzare *direttamente* l'identificazione preposta alle molteplici finalità di decisione, controllo e contrasto sopra menzionate. Di fronte a questa eventualità, il Garante europeo ha espresso una serie di preoccupazioni in termini di qualità dei dati utilizzati, necessità e proporzionalità nell'utilizzo di indicatori biometrici per gli scopi indicati[40], rispetto delle previsioni generali del GDPR e della LED[41]; tutti rilievi che verranno ribaditi ogni volta che un sistema di informazione centralizzato subirà questo scorrimento di funzioni e che raggiungeranno il proprio culmine nelle più recenti riforme che coinvolgono trasversalmente tutti i sistemi.

[39] Art. 43, par. 4, regolamento (UE) 2018/1862 (v. anche cons. 22); art. 33, par. 4, regolamento (UE) 2018/1861 (v. anche cons. 22).

[40] "La necessità di usare identificatori biometrici deve essere chiaramente dimostrata e la possibilità di beneficiarne devono dipendere da misure di salvaguardia più stringenti"; così gli "*EDPS Formal comments on the draft Commission Implementing Decisions*" sulla definizione degli standard di qualità dei dati, 26 agosto 2020, p. 2.1.

[41] Il Garante europeo ha sollecitato un più diretto e chiaro collegamento con le varie previsioni generali del GDPR e della LED riferite alla limitazione delle finalità, utilizzo di sistemi di sicurezza all'avanguardia, periodi di tempo proporzionati per la conservazione dei dati, qualità e protezione degli stessi fin dalla progettazione, tracciabilità, supervisione efficace e sanzioni dissuasive per usi impropri; cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 7/2017, on the new legal basis of the Schengen Information System*, 2 maggio 2017, p. 6.

3. *Il Sistema* European dactylographic *(EURODAC)*

Il secondo sistema da prendere in considerazione è l'"*European dactylographic*" (EURODAC), ovvero il database europeo delle impronte digitali per coloro che richiedono asilo e per le persone fermate mentre varcano irregolarmente una frontiera esterna dell'UE[42].

In parallelo all'abolizione delle frontiere interne all'area Schengen e all'istituzione del SIS, il regolamento n. 2725/2000/CE, sotto il "primo pilastro", ha istituito l'EURODAC con lo scopo principale di agevolare l'applicazione della "Convenzione di Dublino", ovvero determinare lo Stato responsabile per l'esame delle domande di protezione internazionale proposte da cittadini di Paesi terzo o da apolidi. Il sistema consente infatti di comparare le impronte digitali dei soggetti richiedenti asilo o degli immigrati che entrano illegalmente nell'area Schengen, i quali solitamente non dispongono di documenti di identificazione, per arginare il rischio che possano essere formulate più domande in diversi Stati (il c.d. fenomeno dell'*asylum shopping*)[43].

Anche questo strumento, che ha acquisito un rilievo centrale per la gestione dei confini e delle crisi migratorie, ha progressivamente ampliato i propri scopi, con utilizzi che producono un impatto sulla società e sulla vita dei singoli ben più incisivo.

Ai fini del presente discorso merita ricordare che con le modifiche del 26 giugno 2013, il regolamento (UE) 603/2013, oggi in vigore, oltre a precisare meglio i diritti dei soggetti sottoposti a rilevamento dei

[42] Più ampiamente, v. E.R. BROUWER, *Eurodac: Its Limitations and Temptations*, in *European Journal of Migration and Law*, 4, 2, 2002, 231 ss.; F. BOEHM, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Springer, Berlin-Heidelberg, 2012.

[43] M. GIALUZ, *Principio di accessibilità e banche dati di "primo pilastro"*, in F. PERONI, M. GIALUZ (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, cit., 145 ss.; L. MUSSELLI, *Alcune prime considerazioni sui sistemi di scambio di informazioni nello spazio di libertà, sicurezza e giustizia: securitization, function creep e tutela dei diritti*, cit., 13. Anche l'EURODAC funzionava come un sistema *hit/no hit*, da interrogare per verificare se le impronte digitali di un soggetto sono state già inserite da un altro Stato membro. Il sistema non associava le impronte con le generalità del soggetto, e pertanto veniva utilizzato solo a scopo di verificazione.

dati[44], ricomprende tra questi scopi anche le politiche di *sicurezza*, consentendo alle autorità di contrasto di accedere ai dati biometrici raccolti[45]. Tale accesso è però presidiato da cautele derivanti dalla necessità che la ricerca su EURODAC abbia carattere residuale rispetto alla ricerca su altre banche dati, che il confronto sia «necessario in un caso specifico (vale a dire non si eseguono confronti sistematici)», in particolare «a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi», e che sussistano «fondati motivi per ritenere che il confronto contribuisca in misura sostanziale»[46].

Questa tendenza espansiva dell'utilizzo dei dati biometrici per i controlli alle frontiere pare ancor più evidente nelle proposte di modifica del regolamento EURODAC presentate dalla Commissione nel 2016[47], nell'ambito di un pacchetto di riforme del "sistema Dublino"[48].

[44] L'art. 29 del regolamento (UE) 603/2013, stabilisce che la persona sia informata «per iscritto e se necessario oralmente, in una lingua che la persona comprende o che ragionevolmente si suppone a lei comprensibile»: della identità del responsabile del trattamento; dello scopo per cui i suoi dati saranno trattati nell'EURODAC e del fatto che è ammesso l'accesso degli Stati membri e di Europol all'EURODAC a fini di contrasto; dei destinatari dei dati; dell'esistenza di un obbligo di rilevamento delle sue impronte digitali; del diritto di accesso ai dati che la riguardano e del diritto di chiedere che i dati inesatti che la riguardano siano rettificati o che i dati che la riguardano trattati illecitamente siano cancellati, nonché del diritto di ottenere informazioni sulle procedure da seguire per esercitare tali diritti.

[45] Secondo l'art. 1, par. 2 del regolamento (UE) 603/2013, vengono disciplinate anche «le condizioni per le richieste di confronto dei dati relativi alle impronte digitali con i dati conservati nel sistema centrale, presentate dalle autorità designate degli Stati membri e dall'Ufficio europeo di polizia (Europol) a fini di contrasto».

[46] Art. 20, par. 2, del regolamento (UE) 603/2013. Si tratta delle banche dati nazionali, di quella disciplinata dalla decisione 2008/615/GAI che incorpora il Trattato di Prüm, e il VIS.

[47] Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), COM(2016)0272 - 2016/0132 (COD)*, 4 maggio 2016.

Per quanto qui rileva maggiormente, si propone, fra l'altro, di utilizzare il sistema anche per il controllo dell'immigrazione clandestina, dei movimenti secondari dei cittadini di Paesi terzi all'interno dell'UE e dell'identificazione degli immigrati irregolari; a questo scopo, viene estesa anche alle immagini facciali la categoria dei dati da raccogliere obbligatoriamente, da archiviare, da trasmettere alle autorità di pubblica sicurezza ai fini della comparazione, ricomprendendo anche i minori fino a sei anni[49].

Già nel 2013 il Garante europeo aveva sollevato pesanti riserve[50], quanto al rispetto dei canoni di proporzionalità e necessità nell'utilizzo di dati contenuti in un sistema creato per ben altre finalità e con una infrastruttura non pienamente compatibile con le nuove funzioni[51]. Si

[48] Sulle proposte di riforma del regolamento (UE) 604/2013 (c.d. Dublino III), e le difficoltà incontrate nel corso dell'*iter* legislativo, v. in dottrina P. DE PASQUALE, *Verso la refusione del regolamento «Dublino III»*, in *Studi sull'integrazione europea*, 2018, 2, 267 ss.; G. MORGESE, *La riforma del sistema Dublino: il problema della condivisione delle responsabilità*, in *Diritto pubblico*, 2, 2020, 103 ss. Per un quadro complessivo del "sistema Dublino", v. C. FAVILLI, *La politica dell'Unione in materia d'immigrazione e asilo. Carenze strutturali e antagonismo tra gli Stati membri*, in *Quad. cost.*, 2, 2018, 361 ss.

[49] V. in particolare l'art. 1, par. 2, lett. b, art. 2 e artt. 10 e 12-16 del regolamento, nella loro ipotetica nuova formulazione. Da notare anche che, in base alla proposta, dovrebbero essere anche raccolte le generalità del soggetto interessato (art. 13), consentendone quindi una chiara identificazione del soggetto cui è associata l'immagine facciale. L'art. 2 stabilisce anche che «taking fingerprints and facial images of minors from the age of six shall be carried out in a child-friendly and child-sensitive manner by officials trained specifically to enrol minor's fingerprints and facial images».

[50] EUROPEAN DATA PROTECTION SUPERVISOR, Op*inion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of "EURODAC" for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] […] (Recast version)*, 5 settembre 2012, p. 25 ss.

[51] Il sistema si compone infatti di una banca dati centrale informatizzata (il c.d. "Sistema centrale") e di una infrastruttura di comunicazione tra il Sistema centrale e gli Stati membri, dotata di una rete virtuale cifrata dedicata ai dati EURODAC. Ogni Stato membro, attraverso un singolo punto di accesso (il c.d. *focal point* nazionale), invia i dati al Sistema centrale che in tempo reale effettua il controllo relativo alla presenza o meno delle impronte inserite nel Sistema. In Italia l'autorità responsabile per EURODAC è la Direzione centrale anticrime – Servizio di polizia scientifica a Roma, investita del ruolo di *focal point* nazionale. A livello decentrato i 14 Gabinetti regionali di polizia scientifica sono i

consideri poi come i richiedenti asilo sottoposti a controllo, per le condizioni in cui si vengono a trovare, siano soggetti in una posizione di particolare vulnerabilità, i quali, peraltro, subiscono una raccolta sistematica dei dati biometrici, a differenza di quanto avviene per tutti gli altri cittadini europei[52]. Le proposte del 2016 accentuano poi le preoccupazioni sul rispetto del principio di limitazione delle finalità, che impone l'utilizzo dei dati per le finalità alle quali sono stati originariamente raccolti, nei confronti di uno strumento in grado di catturare invasivamente dati biometrici e informazioni come quelle ricavabili dalle immagini facciali[53].

4. *Il Sistema di informazione visti (VIS)*

Il terzo strumento che qui assume rilievo è il "Sistema di informazione visti" (VIS), a presidio dei controlli alle frontiere dello spazio Schengen e preposto allo scambio di dati e informazioni sui visti rilasciati dai Paesi membri a cittadini di Paesi terzi.

soggetti deputati all'inserimento delle informazioni relative alle impronte e le trasmettono, attraverso l'interfaccia nazionale AFIS (*Automated Fingerprint Identification System*), al *focal point nazionale*, unico abilitato a trasmettere i dati al Sistema centrale di EURODAC. Quando le impronte sono già presenti nel Sistema, gli Stati membri possono scambiarsi le informazioni relative alla persona attraverso la rete di scambio informativo, denominata "Dublinet" creata appositamente a tale scopo. EURODAC, infatti, non contiene i dati anagrafici della persona, neppure immigrata irregolare, ma esclusivamente le informazioni atte ad identificare la presenza o meno delle impronte nel Sistema (artt. 9, par. 1, e 11, par. 3); solo successivamente è possibile risalire, attraverso Dublinet, all'identità della persona e prendere così i provvedimenti previsti dal regolamento Dublino; cfr. M. GIALUZ, *Principio di accessibilità e banche dati di "primo pilastro"*, cit., 146 s.; V. FERRARIS, *Eurodac e i limiti della legge: quando il diritto alla protezione dei dati personali non esiste*, in *Diritto, Immigrazione e Cittadinanza*, 2, 2017, 5 s.

[52] EUROPEAN DATA PROTECTION SUPERVISOR, Op*inion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of "EURODAC" for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] [.....] (Recast version)*, 5 settembre 2012, p. 38.

[53] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 07/2016, on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)*, 21 settembre 2016, p 15 ss.

A differenza del SIS e di EURODAC, questo sistema è stato concepito all'indomani dell'11 settembre 2001, in un contesto quindi di misure caratterizzate, anche solo indirettamente, da connotazioni antiterroristiche[54]. Se dunque anche il VIS è andato incontro ad un ampliamento di funzionalità, ciò risulta maggiormente compatibile con il suo spirito originario[55].

Il VIS presenta diversi punti in comune rispetto al già citato SIS, tanto a livello organizzativo[56], quanto nel fondamento giuridico, in quanto è stato istituito con uno specifico strumento di "primo pilastro", ossia il regolamento (CE) 767/2008, ed uno di "terzo pilastro", ossia la decisione 2008/633/GAI. Questo dato riflette, anche qui, le due anime del sistema, ovvero, da una parte, costruire una politica

[54] A. BALDACCINI, *Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases*, cit., 39. Per un richiamo agli atti di indirizzo che hanno portato all'istituzione del VIS, v. M. GIALUZ, *Principio di accessibilità e banche dati di "primo pilastro"*, cit., 151 ss., con specifico riguardo al Consiglio europeo di Laeken del dicembre 2001 e la decisione decisione 2004/512/CE, che ha avviato il processo istitutivo.

[55] M. TZANOU, *The EU as an emerging "Surveillance Society": The function creep case study and challenges to privacy and data protection*, cit., 416.

[56] Sotto un profilo organizzativo il sistema VIS è simile al SIS II: ai sensi della decisione 2004/512/CE, esso si compone di un "*Central Visa information system*" (CS-VIS) che ha sede nello stesso luogo fisico ove trova collocazione il Sistema centrale SIS II, ovvero a Strasburgo, con cui si interfacciano le sezioni nazionali ("*The National Interfaces*") (NI-VIS) presso ciascun Stato aderente. Il sistema VIS condivide la stessa infrastruttura tecnologica con SIS II, e non è un caso dunque se la sede fisica del sistema centrale risulta la medesima; cfr. L. MUSSELLI, *Alcune prime considerazioni sui sistemi di scambio di informazioni nello spazio di libertà, sicurezza e giustizia: securitization, function creep e tutela dei diritti*, cit., 16. Il VIS è divenuto operativo solamente nel 2011; il sistema centrale è stato inizialmente sotto la responsabilità della Commissione, per poi passare all'agenzia eu-LISA. In base al d.interm. n. 4516/495 del 6 ottobre 2011, nel nostro Paese l'accesso al VIS è riservato esclusivamente al personale autorizzato del Ministero degli affari esteri, per le finalità connesse all'esame delle domande di visto presentate all'estero e all'adozione delle correlate decisioni, e del Ministero dell'interno, per le richieste di visto presentate in frontiera e per la determinazione dello Stato membro competente per l'esame di una domanda di asilo. Anche il personale autorizzato delle forze di polizia può inoltre consultare il VIS, ai valichi di frontiera esterni e all'interno dell'Italia, per accertare l'identità del titolare del visto e l'autenticità del visto stesso, nonché per verificare se sono soddisfatte le condizioni di ingresso, soggiorno o residenza.

comune in *materia di visti*, a partire da una più stretta cooperazione consolare e nello scambio di informazioni[57], e dall'altra, rafforzare le politiche di *sicurezza pubblica*, tramite maggiori controlli alla frontiera e all'interno degli Stati membri, una più efficace identificazione degli immigrati irregolari, una più serrata prevenzione di minacce alla sicurezza interna[58]; "vantaggi secondari", questi ultimi, che a detta del Garante europeo rischiano di sbilanciare eccessivamente il sistema verso questo secondo ambito[59].

Il sistema, per come originariamente ideato, trattava solamente dati sui visti per soggiorni di breve durata, ovvero sia dati alfanumerici, come generalità, provenienza, scopo del viaggio, sia fotografie e impronte digitali[60]. In relazione all'accesso a tali dati, il regolamento prevede una differenziazione a seconda dello scopo dello stesso[61], in cui le fotografie – anche qui – vengono utilizzate solamente come strumento sussidiario di verifica dell'identità, nella misura in cui l'identificazione

[57] Il citato regolamento definisce la finalità "generica" del VIS nel «migliorare l'attuazione della politica comune in materia di visti, la cooperazione consolare e la consultazione tra le autorità centrali competenti per i visti, agevolando lo scambio di dati tra Stati membri in ordine alle domande di visto e alle relative decisioni».

[58] Rispettivamente, art. 2, par. 1, e par. 2, lett. d, e, g, regolamento (CE) 767/2008.

[59] GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Parere sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (COM(2004) 835 definitivo) (2005/C 181/06)*, 23 luglio 2005, p. 3.2.

[60] Art. 5, par. 1, lett. b, c, regolamento (CE) 767/2008. L'uso di dati biometrici è stato segnalato dal Garante europeo, anche qui, come un aspetto molto delicato, sottolineando la necessità di «porre in atto importanti garanzie», specie in termini di rispetto del principio della limitazione dello scopo, di restrizione dell'accesso e di misure di sicurezza; cfr. GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Parere sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve* durata, cit., p. 3.4.2.

[61] A fini di verifica ai valichi di frontiera esterni (art. 18); di verifica all'interno del territorio degli Stati membri dell'identità del titolare del visto, dell'autenticità del visto o della sussistenza delle condizioni d'ingresso, di soggiorno o di residenza (art. 19); di identificazione delle persone che non soddisfano le condizioni per l'ingresso, il soggiorno o la residenza nel territorio degli Stati (art. 20); per la determinazione della competenza per le domande di asilo (art. 21); per l'esame della domanda di asilo da parte delle autorità competenti (art. 22).

non vada a buon fine tramite altri elementi come le impronte digitali; a questi limitati fini, viene consentito l'accesso alle autorità competenti sui controlli alle frontiere esterne e all'interno degli Stati membri, in materia di immigrazione e di asilo.

Come accennato, il VIS viene utilizzato anche per scopi di *law enforcement*. Ciò pone seri rischi in relazione a dati raccolti con ben altre finalità[62], sebbene il regolamento e la decisione 2008/633/GAI abbiano circondato con molte cautele l'accesso da parte delle autorità di pubblica sicurezza quanto a modalità, scopo e reati perseguiti, analogamente a quanto accade per l'EURODAC[63]. Vengono inoltre riconosciuti i più volte ricordati diritti e garanzie a tutela dei dati personali[64].

A seguito degli attentati terroristici del novembre 2015 e del marzo 2016, la Commissione ha presentato nel maggio 2018 una ulteriore proposta di riforma per potenziare il VIS che rileva direttamente per l'uso di TRF[65]. Si prevede, infatti, che i dati raccolti al momento della domanda del visto rientrino anche le "immagini facciali" in formato digitale, possibilmente scattate dal vivo, con una qualità e risoluzione sufficienti e tali da permettere di utilizzare le immagini in sistemi au-

[62] Rischi messi in luce anche da M. TZANOU, *The EU as an emerging "Surveillance Society": The function creep case study and challenges to privacy and data protection*, cit., 420 ss.

[63] M. GIALUZ, *Principio di accessibilità e banche dati di "primo pilastro"*, cit., 158 ss. Possono interrogare il VIS soltanto le autorità di polizia nazionali appositamente identificate dallo Stato, non direttamente ma soltanto attraverso i punti di accesso (art. 4 decisione), soltanto nei confronti di «un caso specifico», in presenza di «fondati motivi» per ritenere che la consultazione dei dati VIS «contribuisca in misura sostanziale» alla prevenzione, all'individuazione o all'investigazione dei soli «reati di terrorismo e di altri reati gravi» (art. 3 regolamento, art. 5 decisione); parimenti l'Europol può avere accesso «entro i limiti delle sue competenze e laddove ciò sia necessario per l'adempimento delle sue funzioni» (art. 3 regolamento, art. 7 decisione). Ogni autorità competente autorizzata ad accedere al VIS, inoltre, assicura che l'utilizzo del sistema sia «necessario, adeguato e proporzionato all'assolvimento dei compiti dell'autorità competente stessa» (art. 7 regolamento).

[64] L'art. 37 del regolamento (CE) 767/2008, riconosce agli interessati il diritto a essere informati sullo scopo del trattamento, le categorie dei destinatari di tali dati, il periodo della loro conservazione, sul diritto di accesso, rettifica e cancellazione.

[65] EUROPEAN COMMISSION, *Proposal for a Regulation of the European Parliament and of the Council on upgrading the Visa Information System (VIS)*, COM/2018/302 final 2018/0152(COD), 16 maggio 2018.

tomatizzati di confronto[66]. Si comprende la portata di tale aggiunta, però, solo se si considerano gli ulteriori profili di modifica destinati a incidere profondamente sulle funzioni del sistema.

Viene infatti previsto un ampliamento dello scopo del VIS, con una estensione, tra l'altro, alla prevenzione delle minacce alla sicurezza interna e ad assicurare in generale la corretta identificazione delle persone, consentendo quindi un accesso al sistema da parte delle forze dell'ordine molto più strutturato[67].

La raccolta dei dati viene estesa anche ai minori fino a sei anni e ai titolari di visti per soggiorno di lunga durata e di permessi di soggiorno, includendo quindi l'unica categoria di cittadini di Paesi terzi che attualmente non rientra in nessuno dei sistemi su larga scala dell'UE nello spazio di libertà, sicurezza e giustizia[68]. Inoltre, viene previsto un controllo incrociato delle domande di visto con altri sistemi di informazione dell'UE, segnatamente con i dati raccolti e conservati a fini di cooperazione di polizia e giudiziaria[69].

Nel contesto delle novità normative riguardanti l'interoperabilità dei sistemi su larga scala dell'UE, di cui si dirà a breve, la proposta contribuirebbe quindi alla creazione di una rete centralizzata a livello UE che darebbe accesso a una quantità considerevole di informazioni su tutti i cittadini di Paesi terzi che hanno attraversato o stanno prendendo in considerazione l'attraversamento delle frontiere dell'UE[70].

[66] Rispettivamente, nella nuova formulazione, art. 5, par. 1, art. 22c, art. 9, par. 8. A questo scopo vengono previste specifiche regole per l'inserimento dei dati di cui all'art. 29a.

[67] Art. 2, par. 1, secondo la nuova formulazione.

[68] Art. 13, par. 7, lett. a e artt. 22a ss.; EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 9/2018 on the Proposal for a new Regulation on the Visa Information System*, 12 dicembre 2018, p. 32.

[69] Art. 9a e art. 22b; segnatamente: SIS, EURODAC, l'*Entry/Exit System* (EES), il sistema ECRIS-TCN, lo *European Travel Information and Authorisation System* (ETIAS), l'*Interpol Stolen and Lost Travel Document database* (SLTD), e l'*Interpol Travel Documents Associated with Notices database* (Interpol TDAWN).

[70] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 9/2018 on the Proposal for a new Regulation on the Visa Information System*, 12 dicembre 2018, p. 32.

5. *Il Sistema di ingressi/uscite (EES)*

Il "Sistema di ingressi/uscite" (*Entry/exit System* - EES) ha preso forma all'interno del pacchetto denominato "Frontiere Intelligenti" del 2013, per trovare disciplina nel regolamento (UE) 2017/2226, del 30 novembre 2017[71]; in concomitanza e sulla falsariga, quindi, delle ultime modifiche o proposte di modifica dei sistemi di informazione richiamati in precedenza.

L'EES presenta infatti obiettivi riconducibili, da una parte, al controllo dei cittadini dei Paesi extra-UE che transitano nello spazio Schengen per soggiorni di breve durata o che sono esenti dall'obbligo del visto, garantendo così una sistematica identificazione anche dei c.d. soggiornanti fuoritermine; dall'altra, a finalità di *law enforcement*, quali supporto alla lotta al terrorismo e ai crimini gravi[72].

L'EES sostituisce così il metodo tradizionale di apposizione manuale del timbro sul passaporto per introdurre forme di controllo più efficaci[73]. È uno strumento rivolto ai cittadini che entrano *legalmente* sul territorio, complementare quindi al VIS, per la durata della permanenza dei cittadini extra-UE che richiedono il visto, e al sistema EURODAC, col quale differisce per il titolo di ingresso e la legittimità della permanenza dei cittadini[74].

[71] L'EES era già stato ipotizzato nella comunicazione della Commissione del 13 febbraio 2008 su "*Gestione delle frontiere dell'UE: le prossime fasi*", COM(2008) 69 definitivo. Il regolamento (UE) 2017/2226 si accompagna al regolamento (UE) 2017/2225, che modifica il codice frontiere Schengen per quanto riguarda l'uso del sistema di ingressi/uscite. Nella sua prima versione del 2013, il pacchetto "Frontiere Intelligenti" comprendeva anche la realizzazione di un programma per viaggiatori registrati (RTP), poi abbandonato.

[72] Questa la triplice finalità esplicitata dalla Commissione nel suo *Explanatory Memorandum* alla proposta [COM(2016) 194 final 2016/0106(COD), p. 1].

[73] Considerando 7 regolamento (UE) 2017/2226. Più in particolare, il sistema consente di registrare il momento e il luogo d'ingresso e di uscita dei soggetti sopra richiamati, di calcolare automaticamente la durata del soggiorno autorizzato, generare segnalazioni allo scadere del soggiorno e registrare il momento e il luogo di coloro che sono stati respinti per diniego del visto (art. 1, par. 1 regolamento (UE) 2017/2226).

[74] Coloro che fanno ingresso legalmente nell'area Schengen e ottengono un visto di breve durata sono registrati sull'EES, mentre coloro che presentano richiesta di asilo o fanno ingresso illegalmente sono registrati in EURODAC.

L'EES, che presenta una struttura organizzativa complessa analoga agli altri strumenti sopra visti[75], crea per ciascun transitante un fascicolo individuale entro cui sono conservati i dati sull'identità, i documenti di viaggio e i dati biometrici[76]. Tra questi dati vi è anche l'immagine del volto, qualificata espressamente come "dato biometrico"[77]. Si dà quindi per implicito che ad essa vengano applicate tecniche di riconsocimento facciale, tanto che l'immagine, rilevata sul posto o estratta dal documento di viaggio elettronico, deve possedere una sufficiente risoluzione e qualità per essere «utilizzata nel confronto biometrico automatizzato»[78].

In accordo con le finalità suindicate, all'EES possono avere accesso, innanzitutto, le sole autorità autorizzate dagli Stati e competenti circa i controlli di frontiera, i visti e l'immigrazione[79], per il solo svolgimento delle proprie attività istituzionali o a soli scopi identificativi[80]. In questi casi la protezione dei dati personali è garantita dalla espressa applicazione del GDPR[81].

Al sistema possono accedere anche le autorità di contrasto designate dagli Stati membri, ma solamente nel rispetto di una serie di cau-

[75] L'architettura di EES comprende, fra l'altro, un sistema centrale, che gestisce una banca dati centrale informatizzata di dati biometrici e alfanumerici; un'interfaccia uniforme nazionale in ciascun Paese dell'Unione partecipante; un'infrastruttura di comunicazione sicura e criptata tra il sistema centrale dell'EES e le interfacce uniformi nazionali; un canale di comunicazione sicuro tra il sistema centrale dell'EES e il sistema centrale del VIS (art. 7). L'agenzia eu-LISA è responsabile dello sviluppo e della gestione del sistema (art. 5), nonché di attuare gli adeguamenti al VIS al fine di garantire l'interoperabilità tra il sistema centrale dell'EES e il sistema centrale del VIS (art. 37). Il sistema non è ancora operativo, ai sensi dell'art. 66.

[76] Artt. 16-17 regolamento (UE) 2017/2226. I dati dei viaggiatori che rispettano le norme di durata del soggiorno breve autorizzato vengono conservati per un periodo di tre anni, mentre quelli dei viaggiatori che hanno superato lo scadere del periodo di soggiorno autorizzato vengono conservati per cinque anni (art. 34, salvo le regole di modifica e cancellazione anticipata all'art. 35).

[77] Rispettivamente art. 3, par. 1, nn. 17 e 18, regolamento (UE) 2017/2226.

[78] Art. 15, parr. 2 e 4, regolamento (UE) 2017/2226.

[79] Art. 9 regolamento (UE) 2017/2226.

[80] Art. 27 regolamento (UE) 2017/2226.

[81] Art. 49, par. 2 regolamento (UE) 2017/2226. Si assicura anche che l'utilizzo dell'EES sia necessario, adeguato e proporzionato (art. 10).

tele riguardanti le tipologie di reato e le ragioni giustificative, al pari dell'EURODAC e del VIS[82]. In questi casi è consentita l'interrogazione del sistema a fini di identificazione di un soggetto direttamente tramite immagini del volto[83]. Conseguentemente, deve trovare applicazione la LED e la normativa nazionale attuativa[84].

Anche a tutela dei diritti legati alla protezione dei dati viene fatto richiamo del GDPR e della LED, cui si aggiungono le previsioni *ad hoc* del regolamento che rafforzano il diritto di informazione, il diritto di accesso ai dati personali, di rettifica, integrazione e cancellazione e di limitazione del trattamento degli stessi, nonché i mezzi di ricorso[85]. Sulla liceità del trattamento dei dati personali da parte degli Stati e degli organismi dell'UE vigilano le autorità nazionali di controllo previste dal GDPR e dalla LED e il Garante europeo[86].

L'EES, unitamente al neoistituito "Sistema europeo di informazione e autorizzazione ai viaggi" (ETIAS)[87], fa parte di un sistema com-

[82] Il ricorso è consentito «al fine di prevenire, accertare e indagare reati di terrorismo o altri reati gravi» (art. 29, par. 1, regolamento (UE) 2017/2226), purché ciò risulti «necessario e proporzionato in un caso specifico», suffragato da «prove o ragionevoli motivi per ritenere che la consultazione dei dati dell'EES contribuisca alla prevenzione, all'accertamento o all'indagine di uno dei reati in questione», in particolare laddove sussista il «fondato sospetto che la persona sospettata, l'autore oppure la vittima di un reato di terrorismo o di un altro reato grave» rientri in una delle categorie contemplate dal regolamento (art. 32, par. 1); maggiori cautele sono previste se la persona in questione è sconosciuta, fra cui l'obbligo di consultare prima le altre banche dati nazionali (art. 32, par. 2).

[83] Art. 32, par. 4, lett. b, regolamento (UE) 2017/2226.

[84] Art. 49, par. 3, regolamento (UE) 2017/2226. All'EES può accedere anche una unità operativa designata di Europol (art. 30). In questo caso trova applicazione il regolamento (UE) 2016/794 (art. 49, par. 4).

[85] Così rispettivamente artt. 50, 52 e 54 del regolamento (UE) 2017/2226.

[86] Artt. 55-58 del regolamento (UE) 2017/2226.

[87] L'ETIAS è stato istituito dal regolamento (UE) 2018/1240, allo scopo di imporre ai viaggiatori che entrano in area Schengen senza la necessità di un visto di sottoporsi a regole di esame per ottenere una autorizzazione prima della partenza, allo scopo di valutare se vi siano rischi per la sicurezza, l'immigrazione illegale o un alto rischio epidemico. Più approfonditamente, v. S. ALEGRE, J. JEANDESBOZ, N. VAVOULA, *European Travel Information and Authorisation System (ETIAS): Border Management, Fundamental Rights and Data Protection*, *Study for the LIBE Committee*, PE 583.148, 2017; E. BROUWER, *Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection*, cit., 80 ss.

plessivo di sorveglianza biometrica rivolto a quasi tutti i viaggiatori che attraversano legalmente – occorre sottolinearlo – i confini dell'area Schengen. Nonostante il richiamo alle due discipline portanti sulla protezione dei dati personali, il caso dell'EES pone in risalto la questione fondamentale se un simile sistema di raccolta massiva e particolarmente intrusiva dei dati personali sia rispettoso dei principi di necessità e proporzionalità imposti dall'art. 52, par. 1 della CDFUE[88]. In questa valutazione pesano il numero delle persone coinvolte[89], la tipologia dei dati processati, le condizioni e i mezzi attraverso cui ciò avviene, il carattere obbligatorio della raccolta, la molteplicità di scopi perseguiti.

L'EES, inoltre, può essere utilizzato sia come un mezzo generalizzato per identificare i sospettati anonimi, responsabili o vittime dei crimini, sia come uno strumento di *intelligence* per ricostruire la storia dei viaggiatori sospettati di crimini. Il rischio latente è che – al pari di quanto può accadere per i sistemi richiamati in precedenza – le autorità di contrasto accedano a queste informazioni anche se le persone non siano sospettate di condotte illecite o sottoposte ad indagine. Nuovamente vengono in rilievo gli indirizzi della Corte di giustizia che impongono vi sia un «nesso evidente» tra i dati delle persone il cui comportamento viene sorvegliato e la commissione di un reato o una situazione suscettibile di dar luogo ad azioni penali[90]. Parimenti, occorre che vengano rispettate le diverse condizioni esplicitate dalla giurisprudenza affinché possa ritenersi giustificato l'accesso ai dati conservati da parte di altre autorità nazionali, segnatamente di contrasto[91].

[88] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 06/2016 on the Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System*, 21 settembre 2016, 7.

[89] La valutazione d'impatto della Commissione rileva come ci si aspetti che gli ingressi e le uscite dall'area Schengen aumentino del 57% entro il 2025, raggiungendo la soglia di 850 milioni di attraversamenti, di cui 1/3 da parte di Paesi terzi; EUROPEAN COMMISSION, *Impact Assessment Report on the establishment of an EU Entry Exit System*, cit., 5.

[90] CGUE, C-293-12 e C-594/12, *Digital Rights Ireland,* cit., p. 58; CGUE, C-203/15 e C-698/15, *Tele2 Sverige AB*, cit., p. 105. La misura dovrebbe essere limitata da criteri oggettivi, che prendano in considerazione «un pubblico i cui dati sono idonei a rivelare una connessione, almeno indiretta, con atti di criminalità grave, a contribuire in un modo o in un altro alla lotta contro la criminalità grave, o a prevenire un grave rischio per la sicurezza pubblica» (p. 111).

[91] CGUE, C-203/15 e C-698/15, *Tele2 Sverige AB*, cit., p. 114 ss.

Da qui le serie preoccupazioni espresse dal Garante europeo, che ha chiaramente qualificato come "inaccettabile" che l'EES possa essere direttamente e principalmente sfruttato per finalità di polizia e non per la gestione dei confini e la semplificazione dei controlli[92]. Preoccupazioni che – come visto – si sono rivelate ricorrenti nell'ultimo quindicennio.

6. *I c.d. regolamenti "interoperabilità": verso una sempre maggiore integrazione dei dati …*

Nella comunicazione del 6 aprile 2016 su "Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza"[93], la Commissione ha sollecitato la necessità di migliorare l'architettura della gestione dei dati dell'UE per il controllo delle frontiere e la sicurezza, per porre rimedio così alla frammentazione e alla complessità dovuta all'esistenza di sistemi gestiti diversamente e tra loro incomunicanti. Tale comunicazione ha impresso quindi uno slancio per il completamento di un processo mirante alla realizzazione dell'interoperabilità fra tali sistemi, entro un percorso di discussione già in progresso da molti anni e su cui gli eventi terroristici in Europa del 2015-2016, gli stessi che – come visto in precedenza – hanno giustificato le ultime proposte di modifica dei vari sistemi di informazione, avevano provocato una decisiva accelerazione[94].

L'interoperabilità può essere genericamente definita come la capa-

[92] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 06/2016 on the Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System*, cit., 19.

[93] Comunicazione della Commissione, *Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza*, COM(2016) 205 final, 6 aprile 2017.

[94] Cfr. N. VAVOULA, *Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?*, cit., 136 ss., per una ricostruzione complessiva di questo percorso, iniziato con il già citato *Programma dell'Aia: rafforzamento della libertà, della sicurezza e della giustizia nell'unione europea* (2005/C 53/01), che sollecitava a «l'accesso reciproco o l'interoperabilità di basi di dati nazionali, oppure l'accesso diretto (on-line), anche per l'Europol, alle basi di dati centrali dell'UE già esistenti» (2.1).

cità che differenti sistemi di informazione possiedono di comunicare, di scambiare tra loro dati e di farne utilizzo[95]. Come osserva il Gruppo di esperti ad alto livello istituito *ad hoc* dalla Commissione, interoperabilità non significa accumulare dati o raccogliere categorie ulteriori di informazioni, e neppure condividere automaticamente i dati tra i diversi sistemi: l'interoperabilità riguarderebbe un modo mirato e intelligente di usare i dati esistenti per ottenere i risultati ottimali allo scopo di proteggere più efficacemente e, allo stesso tempo, assicurare il pieno rispetto dei diritti fondamentali[96].

Si comprende quindi come l'interoperabilità non sia esclusivamente o prevalentemente una scelta tecnica, ma piuttosto costituisca una *scelta politica*, tale da avere profonde conseguenze sociali e giuridiche[97]. Basti pensare alla circostanza che in passato, al contrario, era stata la compartimentalizzazione ad essere considerata un mezzo privilegiato per salvaguardare il diritto alla *privacy* e alla protezione dei dati[98]. L'interoperabilità, dunque, non è mai la somma delle singole parti

[95] EUROPEAN DATA PROTECTION SUPERVISOR, *Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice*, 17 novembre 2017, p. 7. Essa costituisce uno dei fattori chiave per garantire l'efficienza dei sistemi informatici su vasta scala, consentendo di ridurre i costi complessivi e di evitare ridondanze naturali di elementi eterogenei. Potrebbe addirittura favorire anche la protezione dei dati, nella misura in cui l'integrazione tra sistemi aventi lo stesso scopo eviti che il medesimo dato venga richiesto più volte ai cittadini (p. 9).

[96] HIGH-LEVEL EXPERT GROUP ON INFORMATION SYSTEMS AND INTEROPERABILITY, *Final report*, maggio 2017, 8. Ad esempio, si osserva in FRA, *Opinion 1/2018. Interoperability and fundamental rights implications*, cit., 16, come un minore non accompagnato che si presenti alla frontiera vedrebbe le proprie impronte digitali registrate su EURODAC. Al momento della sua eventuale scomparsa verrebbe registrato sul SIS II. I due sistemi, però, per come strutturati fino ad ora, non interloquirebbero.

[97] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, 16 aprile 2018, p. 143. Sottolinea questo aspetto anche F. GALLI, *Interoperable Databases: New Cooperation Dynamics in the EU AFSJ?*, in *European public law*, 26, 1, 2020, 113.

[98] Cfr. COMMISSIONE EUROPEA, Comunicazione *Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia* COM(2010) 385 final, 20 luglio 2010, ove si leggeva che «Una gestione compartimentata delle informazioni come quella delineatasi negli ultimi decenni contribuisce alla tutela del diritto del cittadino al rispetto della vita privata più di qualsiasi alternativa centralizzata».

e non è mai "un fine in sé": pertanto non si può eludere la valutazione se ciò sia necessario, politicamente desiderabile e giuridicamente possibile[99].

Il quadro dell'interoperabilità dei sistemi di larga scala a livello UE è definito adesso dai due regolamenti "gemelli" (Ue) 2019/817 e (Ue) 2019/818, entrambi del 20 maggio 2019, riguardanti frontiere e visti, da una parte, e cooperazione di polizia e giudiziaria, asilo e migrazione, dall'altra. Essi tuttavia contengono previsioni di analogo tenore e, pertanto, possono essere trattati congiuntamente[100].

Grazie a questa riforma saranno resi disponibili alle autorità nazionali i dati, comprese le immagini facciali, di cittadini europei e soprattutto di Stati extra-Ue contenute nei sistemi richiamati in precedenza, ovvero il Sistema d'informazione Schengen (SIS), l'EURODAC, il Sistema di informazione visti (VIS), il Sistema di ingressi e uscite (EES), oltre che il Sistema europeo di informazione sui casellari giudiziali di cittadini di paesi terzi (ECRIS-TCN)[101], conte-

[99] Come si osserva in EUROPEAN DATA PROTECTION SUPERVISOR, *Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice*, cit., pp. 7 e 12, l'interoperabilità deve essere al servizio di "uno scopo genuino di pubblico interesse".

[100] La scelta di un duplice atto è dovuta alle differenti basi giuridiche nei Trattati: il primo negli artt. 78, par. 2, lett. e; 79, par. 2, lett. c; 82, par. 2, lett. d; 85, par. 1; 87, par. 2, lett. a; 88, par. 2 TFEU; il secondo negli art. 77, par. 2, lett. a, b, d, e TFUE.

[101] Il sistema informativo del casellario giudiziale europeo (*European Criminal Records Information System* - ECRIS) è un sistema decentralizzato istituito nel 2012 per consentire lo scambio di informazioni tra gli Uffici dei casellari giudiziali di ciascuno degli Stati europei, permettendo così alle autorità giudiziarie dei Paesi europei di tenere in considerazione i precedenti compiuti in altri Stati membri. Per integrare la mancanza di informazioni sui cittadini di Paesi extra-UE, il regolamento (UE) 2019/816, del 17 aprile 2019, ha istituito un sistema centralizzato denominato ECRIS-TCN, gestito da eu-LISA, che raccoglie anche i precedenti di questi ultimi cittadini. Tale regolamento. si accompagna alla direttiva (UE) 2019/884, del 17 aprile 2019, che modifica la decisione quadro 2009/315/GAI, sull'ECRIS, e sostituisce la decisione 2009/316/GAI del Consiglio. Il sistema, che dovrebbe essere operativo nel 2022, consentirà di individuare lo Stato membro che dispone delle informazioni sul casellario giudiziale del cittadino di paese terzo (art. 7, par. 7). Per ciascun cittadino condannato è presente una registrazione che contiene dati alfanumerici, le impronte digitali e anche le immagini del volto, ove consentito dallo Stato terzo (art. 5). Tali immagini possono essere utilizzate, in un primo momento, a scopo di conferma di interrogazioni del

nente le immagini facciali dei cittadini extra-UE che hanno riportato condanne penali, e il Sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), unico invece a non contenere dati biometrici.

Tra gli obiettivi dei regolamenti "interoperabilità" figurano, sullo stesso piano, sia migliorare i controlli alle frontiere esterne, la politica comune in materia di visti, l'esame delle domande di protezione internazionale, l'identificazione di persone ignote, nonché la prevenzione e la lotta all'immigrazione illegale, sia mantenere la sicurezza pubblica e l'ordine pubblico, la prevenzione e lotta ai reati di terrorismo o altri reati gravi[102].

Il nuovo sistema ha una architettura molto complessa, destinata a modificare i sistemi informativi preesistenti. A questi ultimi, infatti, si aggiungono un portale di ricerca europeo (*European search portal* - ESP) e le ulteriori tre nuove banche dati centralizzate che dovranno essere istituite, ovvero un servizio comune di confronto biometrico (*shared biometric matching service* - BMS), un archivio comune di dati di identità (*common identity repository* - CIR) e un rilevatore di identità multiple (*multiple-identity detector* - MID).

L'ESP è uno strumento che dovrebbe fungere da "*message broker*", ovvero da interfaccia unica in grado di consentire l'interrogazione parallela di tutti i citati sistemi di informazione dell'UE, dei dati Europol e delle banche dati Interpol, da parte degli Stati membri e delle agenzie dell'Unione[103]. Dato l'ampio spettro di archivi e informazioni consultabili, risultano cruciali le regole poste per l'accesso a questa interfaccia. Possono ricorrere all'ESP e ai dati ivi contenuti solo i soggetti autorizzati ad accedere ad uno dei sistemi di informazione interconnessi, nei limiti e per le finalità stabilite dalle rispettive normative[104]. In aggiunta, si precisa che a tali discipline distin-

sistema a partire da dati alfanumerici. La Commissione potrà decidere, quando sarà tecnicamente possibile, se implementare il sistema permettendo l'uso di immagini del volto a scopo direttamente identificativo (art. 6). Il Capitolo V del regolamento è dedicato a "Diritti e controllo sulla protezione dei dati". In dottrina, v. G. DI PAOLO, *Novità. Verso una nuova architettura di gestione dei dati contenuti nei sistemi di informazione dell'Unione*, in *Cass. pen.*, 9, 2019, 3380 ss.

[102] V. art. 1, par. 1, regolamenti "interoperabilità".

[103] Art. 6 regolamenti "interoperabilità".

[104] Art. 7, par. 1, regolamenti "interoperabilità".

te occorre fare riferimento anche per stabilire le categorie di dati con cui è possibile interrogare l'ESP e a cui le autorità interroganti possono avere accesso[105].

Il BMS comune è invece un sistema in grado di raccogliere tutti i *template* biometrici conservati nei sistemi interconnessi, comprese le immagini facciali e le impronte digitali, nel rispetto di norme minime di qualità[106]. Il BMS consente di effettuare interrogazioni tramite i dati biometrici e realizzare un confronto trasversale con i *template* contenuti nei diversi sistemi interconnessi, senza dover ricorrere a ricerche separate[107]. I dati originari da cui sono estratti i *template* dovrebbero invece rimanere conservati nei *database* di ciascun sistema[108].

Al centro del sistema vi è poi il CIR, ovvero un *database* comune entro cui confluiscono i dati personali provenienti dal VIS, EURODAC, EES, ETIAS e ECRIS-TCN, nel quale vengono creati e conservati fascicoli individuali contenenti i dati alfanumerici e biometrici di ciascuna persona[109]; un sistema, dunque, in grado di creare in maniera generalizzata e sistematica i profili di milioni di cittadini provenienti da Paesi UE ed extra-UE.

Al CIR, tramite l'ESP, possono accedere le autorità di polizia a scopo identificativo e di verificazione in una serie di ipotesi in cui l'identificazione è resa più complicata[110], beneficiando del confronto e

[105] Rispettivamente art. 9, parr. 2 e 6, regolamenti "interoperabilità".

[106] Art. 13, par. 1 regolamenti "interoperabilità".

[107] Art. 12, par. 1 regolamenti "interoperabilità".

[108] Il BMS riunisce e conserva tutti i template biometrici, separati per logica in base al sistema di informazione di provenienza. È composto da una infrastruttura centrale che sostituisce i sistemi centrali rispettivamente dell'EES, del VIS, del SIS, dell'EURODAC e dell'ECRIS-TCN nella misura in cui registrino *template* biometrici e consentano di effettuare ricerche con dati biometrici (art. 12, par. 2, lett. a, regolamenti "interoperabilità").

[109] Art. 18 regolamenti "interoperabilità". Il SIS dovrebbe rimanere separato dall'archivio comune, sebbene entrambi CIR e SIS dovrebbero utilizzare il BMS comune per individuare eventuali collegamenti sulla base dei dati biometrici e dovrebbero utilizzare l'ESP per individuare eventuali collegamenti sulla base dei dati alfanumerici (cons. 41).

[110] L'art. 20, par. 1, regolamenti "interoperabilità" indica: se l'autorità di polizia non è in grado di identificare una persona in ragione dell'assenza di un documento di viaggio o di un altro documento credibile che ne provi l'identità; se sussistono dubbi

dell'abbinamento automatizzato dei dati già conservati separatamente nei singoli sistemi di informazione di provenienza. A questo proposito, i regolamenti fanno rinvio alla legislazione nazionale per la necessità di specificare le finalità esatte, le procedure, le condizioni e i criteri di tali verifiche[111].

Le autorità di polizia possono altresì interrogare il CIR qualora sussistano fondati motivi per ritenere che l'acceso ai sistemi di informazione integrati possa contribuire alla prevenzione, all'accertamento o all'indagine di "reati di terrorismo" o di altri "gravi reati"[112].

Le cautele verso questo strumento di ricerca hanno indotto a strutturare il sistema in due fasi, per le quali le autorità di pubblica sicurezza dovranno prima interrogare il sistema per verificare se vi siano dati rilevanti circa un soggetto (*hit/no hit*), e solo successivamente potranno accedere a tali dati presentando richiesta agli Stati o alle autorità competenti sulla base delle singole discipline dei sistemi integrati[113]. In questo modo si dovrebbe eliminare il meccanismo "a cascata" che impone, nel caso di EURODAC ed EES, di consultare le banche dati nazionali prima di interrogare i sistemi gestiti a livello UE.

Questa complessa architettura informativa è completata dal MID, che si configura come un sistema in grado di creare un fascicolo sull'identità di ciascun soggetto, all'interno del quale vengono segnalati i collegamenti problematici tra i dati delle persone fisiche presenti nei vari sistemi d'informazione dell'UE, allo scopo di rilevate i casi di identità multiple, per agevolare le verifiche di identità e contrastare la frode o i furti di identità[114].

quanto ai dati di identità forniti dall'interessato; se sussistono dubbi quanto all'autenticità del documento di viaggio o di un altro documento credibile fornito dall'interessato; se sussistono dubbi quanto all'identità del titolare del documento di viaggio o di un altro documento credibile; ovvero se l'interessato non è in grado o rifiuta di cooperare. Le forze di polizia, inoltre, potranno interrogare il CIR con i dati biometrici dell'interessato acquisiti sul posto durante una verifica d'identità, solamente «a condizione che la procedura sia stata avviata in presenza dell'interessato» (art. 20, par. 2).

[111] Art. 20, par. 5, regolamenti "interoperabilità".

[112] Art. 22, par. 1, regolamenti "interoperabilità", che aggiunge la necessità che vi sia il sospetto che i dati richiesti siano contenuti nell'EURODAC.

[113] Art. 22, par. 2, regolamenti "interoperabilità".

[114] Art. 25 regolamenti "interoperabilità". I collegamenti che possono instaurarsi

Si assiste, dunque, alla convergenza di sistemi che muovono da punti di partenza e scopi profondamente diversi, quali il SIS per i controlli alle frontiere, l'EURODAC per individuare lo Stato responsabile AD esaminare le richieste di asilo, il VIS per la circolazione di informazioni relativi ai visti e permessi di soggiorno, l'EES per individuare i casi di soggiornanti fuoritermine, l'ECRIS-TCN per rendere accessibili informazioni sulle condanne penali; ciascun sistema oggetto di specifica regolazione in termini di finalità, regole di trattamento e di protezione dei diritti. Questa complessa architettura dovrebbe essere predisposta, secondo quanto previsto dalla Commissione, entro la fine del 2023[115], con un considerevole sforzo tecnico e organizzativo da parte dell'agenzia "eu-LISA" e degli Stati membri[116].

7. (segue) *… e una maggiore integrazione delle criticità*

Volendo esprimere un giudizio su questi sviluppi occorre osservare, innanzitutto, come una integrazione che dovrebbe facilitare la fruizione dei dati rischia, per una paradossale eterogenesi dei fini, di complicare esponenzialmente il quadro non solo tecnico, ma soprattutto giuridico esistente, aggiungendo nuove regole ad uno scenario – come visto sopra – già complesso ed iper-frammentato[117].

Che la decisione di muovere verso l'interoperabilità non sia affatto

tra i dati dei diversi sistemi di informazione integrati vengono ricondotti in diverse classificazioni, distinte in giallo (art. 30), verde (art. 31), rosso (art. 32) e bianco (art. 33), a seconda del livello di intensità di corrispondenza delle informazioni registrate. La verifica automatizzata delle identità diverse è suffragata da una verifica manuale (art. 29).

[115] Così nella relazione della Commissione sullo stato di avanzamento dei preparativi per la piena attuazione dei regolamenti sull'interoperabilità, ai sensi dei rispettivi art. 74, par. 4, e art. 78, par. 5, COM(2020) 428 final, 28 agosto 2020.

[116] Sotto il profilo delle responsabilità, i regolamenti distinguono la responsabilità di eu-LISA, per quanto attiene alla fase preliminare di progettazione e sviluppo (art. 54) e a quella successiva all'entrata in funzione di ciascuna componente dell'interoperabilità (art. 55), da quella degli Stati membri (art. 56) e di Europol (art. 57).

[117] H. ADEN, *Interoperability Between EU Policing and Migration Databases: Risks for Privacy*, in *European Public Law*, 26, 1, 2020, 93, 100 ss.

neutrale, inoltre, si evince dalle conseguenze che, sul piano giuridico, sono destinate non solo ad amplificare quanto accennato per i singoli sistemi circa il rispetto dei canoni di proporzionalità, necessità e dei principi giuridici a protezione dei dati, ma a porre problematiche nuove e ancor più significative.

Questa impressione è evidente pensando al CIR, ovvero un sistema che potenzialmente potrebbe consentire alle autorità nazionali di polizia di effettuare un accesso routinario per scopi identificativi ad un *database* contenente una quantità ineguagliabile di profili personali. Non appena il CIR sarà operativo, potrà essere interrogato per il perseguimento di finalità descritte in termini piuttosto generici, quali quelle indicate in apertura al regolamento con riferimento a sicurezza e ordine pubblico, prevenzione e indagini di reati gravi e di terrorismo. La consultazione di questo strumento, peraltro, consente di eludere alcuni profili nelle valutazioni da svolgere necessariamente prima di consultare i singoli sistemi, come quella relativa alla sussistenza di «fondati motivi per ritenere che il confronto contribuisca in misura sostanziale» alla prevenzione, all'individuazione o all'investigazione di un reato grave o di terrorismo, come richiesto per l'EURODAC, il VIS e l'EES.

Si comprendono allora le preoccupazioni espresse dal Comitato europeo per la protezione dei dati e dal Garante europeo, ove dichiarano che la sola disponibilità dei dati non possa valere a giustificare il loro utilizzo tramite simili sistemi[118]. È pur vero che le autorità di polizia debbano disporre degli strumenti più adeguati per identificare rapidamente gli autori di atti terroristici e altri reati gravi. Tuttavia, facilitare l'accesso di queste autorità a sistemi estranei al settore del contrasto, anche se in misura limitata dalle regole citate sopra, ha implicazioni tutt'altro che insignificanti in termini di diritti fondamentali[119]. Sul punto vengono in rilievo i più volte citati indirizzi della Corte di giustizia, che, a partire dal caso *Digital Rights Ireland*, ha deprecato i

[118] ARTICLE 29 WORKING PARTY, *Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration*, WP266, 11 aprile 2018, 11.

[119] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, 16 aprile 2018, p. 62.

fenomeni di sorveglianza generalizzata, dal momento che anche la mera raccolta e conservazione dei dati per un certo periodo, a prescindere dal loro utilizzo, costituisce una ingerenza al diritto alla vita privata (art. 7 CDFUE) e alla protezione dei dati personali (art. 8 CDFUE)[120]. Pertanto, come viene ricordato nel caso *Tele2 Sverige*, simili misure di sorveglianza devono presupporre la presenza di «criteri oggettivi per definire le circostanze e le condizioni in presenza delle quali deve essere concesso alle autorità nazionali competenti l'accesso» ai dati, con un rapporto "diretto" e di "stretta necessità" tra i dati da conservare e l'obiettivo perseguito[121]. La Corte EDU – si ricorda – nel caso *S. e Marper* ha poi calcato la necessità di avere regole chiare e dettagliate sulla portata e le modalità di applicazione delle misure di sorveglianza[122].

Se tuttavia le ragioni che giustificano il ricorso a tale strumento sono così ampie, allora, più in generale, la creazione di un *database* contenente informazioni dalla così varia provenienza fa sorgere seri interrogativi in termini di superamento del test di proporzionalità elaborato dalla Corte di giustizia[123]. L'accesso a questi sistemi finirebbe per coinvolgere contestualmente cittadini extra-UE che transitano in buona fede per motivi turistici (EES), che sono stati condannati penalmente (ECRIS-TCN), o cittadini europei sottoposti a segnalazione nel settore della cooperazione in materia di polizia o giudiziaria (SIS II)[124]. Il mezzo supererebbe senza dubbio il test quanto alla sua "idoneità" al raggiungimento degli obiettivi perseguiti, sebbene la sua concreta implementazione non sia affatto esente da incognite e difficoltà. Maggiori dubbi sorgono nella valutazione sull'*an* e sul *quantum* tale mezzo "ec-

[120] CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 34-35.

[121] CGUE, C-203/15 e C-698/15, *Tele2 Sverige AB*, cit., p. 110.

[122] Corte EDU, *S. e Marper*, cit., p. 99; anche, *M.M.*, cit., p. 195; *M.K.*, cit., p. 32.

[123] V. *retro* Cap. III, par. 4.3. Sul punto, v. anche le considerazioni in E. BROUWER, *Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection*, cit., 87 ss.

[124] ARTICLE 29 WORKING PARTY, *Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration*, cit., 6 ss.

ceda" quanto necessario per raggiungere tali obiettivi[125]. I settori in questione, i diritti in gioco – si pensi solamente al diritto di asilo all'art. 10, c. 3 Cost. e all'art. 18 CDFUE, anche solo per lo stato di "incertezza istituzionale"[126] in cui potrebbe versare la posizione giuridica del migrante a fronte dei ritardi maturati nell'ottenere l'accesso alla protezione internazionale (come già avviene, e come ancor più potrebbe avvenire) a causa di una erronea o mancata identificazione –, la capacità invasiva di questi mezzi e la gravità dell'ingerenza dovrebbero imporre molta cautela da parte del legislatore[127]. Tale valutazione – aggiunge la Corte di giustizia – dovrebbe essere condotta «in termini rigorosi» trattandosi di dati biometrici[128], da conservare e impiegare per di più a scopi sensibili come la prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali[129].

Parimenti, è tutta da dimostrare la necessità di disporre di strumenti di ricerca così incisivi e potenti, quando i dati sono già contenuti e reperibili, seppur con le difficoltà tecniche e organizzative finora manifestate, nei sistemi che si vuole interconnettere[130].

L'architettura del sistema a due fasi è una scelta che vale senza dubbio a limitare l'accesso delle forze di polizia alle informazioni, ma di fronte a dati di questa natura anche un metadato costituito dalla

[125] Si ricorda che il principio di proporzionalità esige, secondo costante giurisprudenza della CGUE, che gli atti delle istituzioni dell'Unione siano idonei a realizzare gli obiettivi legittimi perseguiti dalla normativa e non superino i limiti di ciò che è idoneo al conseguimento degli obiettivi stessi o eccedano più di quanto necessario a raggiungerli; cfr. CGUE, C-291/12, *Schwarz*, cit., p. 45-46. CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 46-47. V. retro Cap. III, par. 4.3.

[126] Cfr. P. PANNIA, *"Institutional uncertainty" as a technique of migration governance. A comparative legal perspective*, *in DPCE Online*, 41, 4, 2019, 5136 ss., e la bibliografia ivi citata.

[127] Elementi da tenere in considerazione, come chiarito in CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 46-47.

[128] Si consideri quanto stabilito a proposito dell'autorizzazione al rilascio di documenti biometrici idonei a evitarne la falsificazione o l'uso fraudolento; cfr. CGUE, C-291/12, *Schwarz*, cit., p. 36.

[129] Cfr. CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 38.

[130] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, 16 aprile 2018, p. 55.

presenza o meno dell'informazione richiesta in uno dei sistemi (*hit/no hit*) è significativo nella prospettiva della tutela dei diritti fondamentali, perché rivelatore del fatto che i dati cercati sono già stati processati, ad esempio, per ottenere un visto o un permesso di soggiorno[131].

Anche il rinvio alla legislazione nazionale lascia troppo indefinite le regole di accesso al sistema[132]. Non solo, ma la mancanza di chiarezza nella disciplina, derivante dall'assenza di criteri e scopi predefiniti, rimette l'uso di simili strumenti alle regole e alle prassi di ciascun Paese, aprendo così a potenziali divergenze e, soprattutto, a pratiche discriminatorie basate su controlli estensivi concentrati su categorie determinate di stranieri, a partire da sospetti e pregiudizi legati, ad esempio, alla razza o alla religione[133].

Ai rilievi che, in termini generali, si appuntano sulla proporzionalità e necessarietà nell'utilizzo di questi sistemi, si aggiungono poi le cautele da adoperare per il trattamento specifico dei dati biometrici. Ciò vale tanto per il CIR quanto per il BMS comune, il cui trattamento dei *template* biometrici rientra sotto la disciplina delle categorie parti-

[131] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, 16 aprile 2018, cit., 62. Ad esempio, se i dati di un soggetto proveniente dall'Afghanistan, Iraq o Siria sono stati raccolti, è probabile che siano contenuti nell'EURODAC e che il soggetto in questione sia un richiedente asilo; se i dati di un soggetti proveniente dalla Cina o dall'India sono stati raccolti, è probabile che questi abbia richiesto un visto; cfr. FRA, *Opinion 1/2018. Interoperability and fundamental rights implications*, cit., 27. Da qui il suggerimento, non accolto, di considerare il CIR come uno strumento "sussidiario", con l'obbligo per le forze di polizia di consultare prima i propri *database*, o il *database* contenente le impronte digitali previsto dalla decisione 2008/615/GAI che incorpora il trattato di Prüm; così la lettera congiunta inviata dai SIS II, VIS e EURODAC Supervision Coordination Group al Presidente del Parlamento europeo in data 22 giugno 2018 [bit.ly/3rZFn7W].

[132] ARTICLE 29 WORKING PARTY, *Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration*, cit., 12.

[133] V. anche N. VAVOULA, *Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?*, cit., 148, che sottolinea anche come la designazione delle autorità competenti spetti ai singoli Stati membri, dando adito a potenziali abusi, incomprensioni, scelte arbitrarie e poco chiare.

colari di dati all'art. 9, par. 2, lett g, del GDPR, per motivi di interesse pubblico rilevante, e all'art. 10 della LED, per finalità di polizia[134]. Quanto al regolamento, è molto discutibile che il trattamento di tali dati, derivante dalla integrazione di questi sistemi, sia «proporzionato alla finalità perseguita» di identificazione e verificazione, come pure si può dubitare che i trattamenti così originati rispettino «l'essenza del diritto alla protezione dei dati»[135]. Analoghi rilievi valgono anche per la direttiva, la quale impone che il trattamento sia «strettamente necessario».

Tra gli altri capisaldi della normativa generale sulla protezione dei dati che l'interoperabilità pone a rischio vi è innanzitutto il principio di limitazione delle finalità[136]. Quello che è in gioco è l'uso dei dati personali e il loro "meta-uso", derivante dalla combinazione e aggregazione con ulteriori dati contenuti negli altri sistemi, che si arricchirà di finalità ulteriori a quelle per le quali erano stati raccolti e che non potrà poggiare sui fondamenti giuridici originari[137]. In passato tale principio veniva salvaguardato proprio dalla separazione logica dei dati originati o appartenenti a differenti sistemi informatici[138]. Nel momento in cui questa separazione non esisterà più e che, in termini evidenti per il CIR, i requisiti di accesso saranno così ampi, pare evidente il rischio di eludere tale principio nella misura in cui – come sottolinea il Garante europeo – il cittadino che presta il consenso a trattare i propri dati per ottenere un visto veda utilizzati i propri dati a scopo, ad esempio, di indagine assieme a dati raccolti e processati chiaramente per finalità di polizia, come avviene nell'ECRIS-TCN[139].

[134] V. *retro* Cap. III, par. 3.

[135] Si ricordi che in CGUE, C-362/14, *Maximillian Schrems*, cit., p. 94, si legge come «una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata».

[136] V. *retro* Cap. III, par. 5.1.

[137] N. VAVOULA, *Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?*, cit., 144.

[138] ARTICLE 29 WORKING PARTY, *Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration*, cit., 4 s.

[139] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2018 on the Proposals*

Pare inoltre difficile collocare la soglia di incompatibilità delle finalità originarie di raccolta dei dati, dal momento che anche «i limiti di questi sistemi sono lungi dall'essere raggiunti»[140]. La stessa proposta di regolamenti della Commissione preconizzava la possibilità di rendere interoperabili anche sistemi e banche dati ulteriori entro questa infrastruttura comune, secondo un processo di integrazione tecnologica e giuridica che pare difficilmente arrestabile[141].

Tutto ciò è destinato anche a creare attriti con il principio di minimizzazione dei dati[142]. Si pensi ai profili realizzati nel CIR o ai *template* biometrici elaborati nel BMS, ossia in *database* diversi dai sistemi di origine. Ciascun profilo verrà realizzato con i dati indicati nei regolamenti, ossia una quantità di dati che non è detto affatto siano "adeguati", "pertinenti" e "limitati" o "non eccedenti"[143] rispetto alle finalità del trattamento di riconoscimento facciale – identificazione o verificazione – operate nei più diversi contesti.

Come in parte già emerso, inoltre, l'interoperabilità potrebbe accentuare i rischi di discriminazione legati all'uso di TRF[144]. Queste ultime, come visto, presentano margini di errori legati alla qualità dei dati o alle caratteristiche dei soggetti coinvolti nei controlli, legate ad esempio all'età, al sesso o al colore della pelle[145]. L'implementazione di sistemi come il MID che sfruttano sistematicamente il riconoscimento facciale potrebbe incrementare il tasso di falsi-negativi o di falsi-positivi nel rilevamento di casi di frodi di identità.

for two Regulations establishing a framework for interoperability between EU large-scale information systems, 16 aprile 2018, cit., 62.

[140] G. CAGGIANO, *L'interoperabilità fra le banche dati dell'Unione sui cittadini degli Stati terzi*, in *Diritto, Immigrazione e Cittadinanza*, 1, 2020, 180.

[141] Cfr. 2017/0351(COD) COM(2018) 478 final, ove si legge che «i sistemi decentrati quali quelli previsti dal quadro di Prüm, dalla direttiva sul codice di prenotazione (PNR) e dalla direttiva riguardante le informazioni anticipate sui passeggeri potranno essere collegati in un secondo tempo a una o più componenti proposte nel quadro della presente iniziativa, *purché se ne dimostri la necessità*» (enfasi aggiunta). Rischi rilevati anche in FRA, *Opinion 1/2018. Interoperability and fundamental rights implications*, cit., 12.

[142] V. *retro* Cap. III, par. 5.2.

[143] Cfr. art. 5, par. 1, let. c, GDPR; art. 4, par. 1, let. c, LED.

[144] V. *retro* Cap. III, par. 7.

[145] Come rilevato anche in FRA, *Opinion 1/2018. Interoperability and fundamental rights implications*, cit., 14.

A questo riguardo, l'art. 5 dei regolamenti contengono una clausola di non discriminazione e di protezione dei diritti fondamentali, compreso il diritto al rispetto della vita privata e alla protezione dei dati personali, all'interno della quale trova spazio una specifica tutela riservata ai minori, alle persone anziane, con disabilità o bisognose di protezione internazionale. Si tratta di una menzione più che opportuna, ma che può non essere sufficiente alla luce delle tecnologie impiegate e del bisogno di tutele da parte di queste categorie di soggetti. Risulta quindi condivisibile il suggerimento – non accolto – del Gruppo di lavoro "Articolo 29" che incitava ad introdurre, con esplicita menzione, l'esclusione di questi soggetti dalla raccolta dei dati biometrici, l'inaffidabilità di tali dati nei loro confronti, o il divieto di assumere nei loro confronti decisioni basate unicamente su questi dati[146].

Cruciale, a questo proposito, risulterà quindi la qualità dei dati e delle immagini processate dai sistemi, che dovrà essere garantita da eu-LISA attraverso meccanismi automatizzati di controllo[147]. Ambiziosamente, inoltre, i regolamenti si propongono di istituire un formato universale dei messaggi (UMF), che funga da standard comunicativo per lo scambio transfrontaliero di dati tra i sistemi di informazione, le autorità o le organizzazioni del settore di giustizia e affari interni[148].

I regolamenti, inoltre, qualificano le autorità dei singoli Stati come titolari del trattamento per i dati presenti in ciascun sistema e, al contempo, per il trattamento dei dati di BMS, CIR e MID ai sensi del GDPR o della LED[149]. Nei confronti di tali autorità, dunque, può essere esercitato il diritto di informazione, sebbene non si preveda espressamente che, nel contesto dell'interoperabilità, i dati potrebbero

[146] ARTICLE 29 WORKING PARTY, *Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration*, cit., 18.

[147] In base all'art. 37 dei regolamenti "interoperabilità", spetta a eu-LISA di istituire meccanismi automatizzati di controllo della qualità dei dati e di elaborare indicatori comuni, che includano indicatori comuni della qualità dei dati e norme minime di qualità per la conservazione all'interno dei sistemi di informazione dell'UE o delle componenti dell'interoperabilità.

[148] Art. 38 regolamenti "interoperabilità".

[149] Art. 40 regolamenti "interoperabilità". Il successivo art. 41 qualifica l'agenzia eu-LISA responsabile del trattamento ai sensi del regolamento (UE) 2018/1725.

essere trattati differentemente anche per ogni altra finalità potenzialmente consentita dai regolamenti e dalle autorità pubbliche contemplate[150]. La complessità che inoltre dovrebbe raggiungere simile informativa rischierebbe ancor più di inficiarne l'utilità di uno strumento che – come visto[151] – solleva comunemente perplessità quanto alla relativa efficacia[152].

Nonostante ciò, una corretta informazione sul trattamento sarebbe prodromica all'esercizio degli ulteriori diritti di accesso, rettifica e cancellazione dei propri dati personali conservati nel MID e di limitazione del loro trattamento, per come stabiliti dal GDPR e dalla LED[153]. Tali diritti sono tanto più importanti quanto più i *database* interconnessi contengono dati inesatti[154]. Dato che tali inesattezze sono destinate a originare segnalazioni nei collegamenti operati dal MID e a produrre falsi-positivi in ordine a episodi di frodi di identità, i cittadini devono avere la possibilità di intervenire sui propri dati contenuti nei diversi sistemi di informazione, viste anche le difficoltà che si riscontrano nell'esercitare effettivamente questi diritti nei confronti dei singoli sistemi informativi[155],[156]. In caso di diniego alla richiesta di eserci-

[150] Art. 47 regolamenti "interoperabilità". Rilievo sollevato in FRA, *Opinion 1/2018. Interoperability and fundamental rights implications*, cit., 46.

[151] V. *retro* Cap. III, par. 4.1.

[152] Come riscontrato anche dai risultati della ricerca di cui si dà conto in FRA, *Under watchful eyes – biometrics, EU IT-systems and fundamental rights*, cit., 29 ss.

[153] Art. 48 regolamenti "interoperabilità". V. *retro* Cap. III, par. 6.2.

[154] Come dimostra, ad esempio, la *Relazione della Commissione sull'attuazione del regolamento (CE) n. 767/2008 (VIS), l'impiego delle impronte digitali alle frontiere esterne e il ricorso ai dati biometrici nella procedura relativa alle domande di visto*, COM(2016) 655 final, 14 ottobre 2016, p. 3.1.

[155] Come attestato in FRA, *Under watchful eyes – biometrics, EU IT-systems and fundamental rights*, cit., 2018, 100, a fronte di 5 milioni di dati contenuti nell'EURODAC, nel 2016 sono state presentate 156 richieste di accesso; su 800.000 segnalazioni sul SIS II, nel 2010-2011 sono state presentate 6072 richieste di accesso.

[156] A questo riguardo, i regolamenti prevedono appositamente la creazione di un "Portale web", contiene informazioni sui diritti e sulle procedure di cui sopra e un'interfaccia utente che consente alle persone i cui dati sono trattati nel MID e che sono state informate della presenza di un collegamento rosso, di ricevere le informazioni di contatto dell'autorità competente dello Stato membro competente per la verifica manuale delle identità diverse (art. 49, par. 2, regolamenti "interoperabilità").

zio dei diritti summenzionati vengono messi a disposizione i mezzi di ricorso alle autorità giudiziarie o alle autorità competenti da parte delle norme istitutive dei singoli sistemi informativi[157].

Anche a garanzia dei diritti degli interessati, inoltre, si stabilisce che le autorità di controllo previste dal GDPR e dalla LED verifichino la legittimità del trattamento dei dati personali da parte degli Stati membri, anche in collaborazione con il Garante europeo della protezione dei dati[158], potendo accedere alle registrazioni delle operazioni effettuate tramite le componenti del sistema[159].

In definitiva, a conclusione di questa analisi, si può affermare che la decisione del legislatore dell'UE di realizzare sistemi di informazione su larga scala interoperabili non avrà soltanto conseguenze permanenti e profonde sulla struttura di questi sistemi e sulle modalità del loro funzionamento, ma cambierà il modo con cui i principi giuridici in questo settore sono stati tradizionalmente interpretati, segnando un «punto di non ritorno»[160]. È una scelta tecnica e organizzativa che cambierà i termini con cui i dati personali vengono trattati a livello europeo e statale[161]. Per cogliere la portata di questo cambiamento si pensi a quanto chiarito dalla Corte di giustizia nella sua opinione 1/2015, riguardante il trasferimento dei dati concernenti il PNR dall'UE al Canada a scopi di polizia, secondo cui tale trattamento non costituisce un sistema diffuso e illegittimo di sorveglianza nella misura in cui venga limitato a questa categoria di viaggiatori e solo per il periodo di permanenza nel Paese in questione[162]. Contrariamente, nelle

[157] Cfr. art. 67, par. 3, regolamento SIS-polizia e art. 53, par. 3, regolamento SIS-frontiere; art. 29 regolamento EURODAC; art. 40 del regolamento VIS; art. 54 regolamento EES.

[158] Artt. 51-53 regolamenti "interoperabilità".

[159] Art. 10, par. 3 (ESP), art. 16, par. 3 (BMS commune), art. 24, par. 7 (CIR), art. 36, par. 3 (MID), regolamenti "interoperabilità".

[160] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, cit., p. 143.

[161] Così la lettera congiunta inviata dai *SIS II*, *VIS* e *EURODAC Supervision Coordination Group* al Presidente del Parlamento europeo in data 22 giugno 2018 [bit.ly/3rZFn7W].

[162] CGUE, parere 1/15 (Accordo PNR UE-Canada), cit., 196 ss., ove si specifica anche che la conservazione dei dati oltre il periodo di permanenza degli interessati, o

pronunce *Digital Rights Ireland* e *Tele2 Sverige*, la Corte è stata chiara nel condannare come «sorveglianza continua» la conservazione generalizzata e senza limitazioni di dati concernenti le telecomunicazioni[163]. La nuova architettura di banche dati interoperabili, che combina informazioni provenienti dai diversi sistemi, si avvicina molto ad uno strumento di sorveglianza di massa dei movimenti dei cittadini extra-UE ed europei[164]. Come introduttivamente accennato, le forme di sorveglianza digitale praticate nelle società contemporanee hanno oramai superato l'immagine del Panopticon di Bentham. Trattando di interoperabilità, si ha la conferma di trovarsi di fronte ad un sistema in grado non solamente di osservare le persone, ma di fornire una "conoscenza" approfondita delle loro identità, abitudini e comportamenti[165].

la loro trasmissione ad altre autorità, «dovrebbe essere subordinato, salvo casi di urgenza debitamente giustificati, ad un controllo preventivo effettuato o da un giudice, o da un ente amministrativo indipendente la cui decisione che autorizzi l'uso intervenga a seguito di una richiesta motivata di tali autorità presentata, in particolare, nell'ambito di procedure di prevenzione, di accertamento o di esercizio dell'azione penale» (p. 208).

[163] CGUE, C-293-12 e C-594/12, *Digital Rights Ireland*, cit., p. 37; CGUE, C-203/15 e C-698/15, *Tele2 Sverige AB*, cit., p. 100.

[164] G. CAGGIANO, *L'interoperabilità fra le banche dati dell'Unione sui cittadini degli Stati terzi*, cit., 172.

[165] Cfr. N. VAVOULA, *Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?*, cit., 142, che osserva come "pan-opticon", derivante dal greco antico 'πάν' (tutto) + 'οπτικόν' (visivo), sia stato progressivamente sostituito da un "pan-gnosticon", 'πάν' (tutto) + 'γνωστικόν' (conoscenza).

CAPITOLO V

LA REGOLAZIONE GIURIDICA DELLE TRF: NUOVE FORME E APPROCCI

SOMMARIO: 1. Considerazioni introduttive: il rischio di una "*disruption*" delle regole giuridiche. – 2. La *risk-regulation* delle TRF: la rilevanza complessiva del principio di precauzione. – 3. La *self-regulation* delle TRF: virtù e vizi dei principi etici. – 4. La *co-regulation* delle TRF: standard tecnici, codici di condotta e oltre. – 5. La valenza regolativa del *design* delle TRF. – 6. La maggior flessibilità normativa richiesta dalle TRF. – 6.1. Regolare le TRF tramite sperimentazioni normative. – 6.2. TRF e *soft-regulation*. – 7. Spunti sul ruolo delle norme giuridiche nella regolazione delle TRF.

1. *Considerazioni introduttive: il rischio di una "*disruption*" delle regole giuridiche*

In assenza di una disciplina esplicitamente riferita alle TRF, il quadro delle norme giuridiche in vigore, prevalentemente riferite alla protezione dei dati personali, consente di individuare una serie di principi e di riconoscere alcuni diritti che assumono una portata generale e che sono invocabili anche a seguito di sottoposizione a riconoscimento facciale, pur con tutti i limiti sottolineati. Le numerose iniziative votate a sospendere la ricerca e sviluppo di queste tecnologie di ultima generazione, tuttavia, dimostrano la necessità di una riflessione più mirata da parte dei legislatori, specie sulle opzioni percorribili, sui contenuti e sui mezzi con cui approntare una regolazione adeguata[1]. Occorre

[1] Osserva C. SALAZAR, *Umano troppo umano… o no?*, in *BioLaw Journal*, 1, 2014, 257, con riguardo agli sviluppi della robotica – ma lo stesso discorso potrebbe valere per le TRF – come «le norme giuridiche già esistenti siano inadeguate e insufficienti per regolare *in tutte le sue implicazioni* l'interazione tra gli uomini e *queste* macchine, all'evidenza "diverse" da tutte le altre». Anche in A. IANNUZZI, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale Scientifica, Napoli, 2018, 2, si sottolinea che di fronte all'evoluzione tecnologica nell'universo giuridico

adesso interrogarsi su quali potrebbero essere gli strumenti normativi a disposizione per offrire una disciplina alle tecnologie in questione e regolare quindi le interferenze sui diritti fondamentali sopra descritte.

La risposta a tale interrogativo non è affatto immediata, se solo si considera come, nelle società contemporanee, le innovazioni tecnologiche stanno riconfigurando gli equilibri tra poteri e stanno ponendo sotto stress numerose categorie che la scienza giuridica tradizionalmente dà per presupposte[2]. Anche i metodi di regolazione si incrinano sotto il peso delle innovazioni tecnologiche, come è emerso progressivamente, e sempre più impetuosamente, a partire dagli anni '90 con l'avvento prima di internet[3], poi di *big data*[4], IA[5], robotica[6], e quindi – potremmo dire – anche delle TRF.

Quello che emerge dall'impiego sempre più diffuso e dalla inedita capacità pervasiva dispiegata dalle TRF è che c'è bisogno di *nuovi approcci* alla regolamentazione. La stessa normativa fin qui ritenuta rilevante, infatti, dà conto di come non si possa ricorrere solamente al paradigma tradizionale della "*hard law*", intesa come regolamentazione tipicamente ispirata allo schema delle imposizioni assistite da sanzioni ("*command and control*"), che segue una traiettoria di pura eteronomia ("*top-down*"), in cui il destinatario delle norme si vede

occorre verificare «quali principi si stanno flessibilizzando, quali canoni tradizionali rischiano di finire stravolti (o travolti), quali altri sembrano avere la forza di resistere».

[2] Cfr. V. ZENO ZENCOVICH, Big data *e epistemologia giuridica*, in S. FARO, T.E. FROSINI, G. PERUGINELLI (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, cit., 20. V. anche R. KENNEDY, *Algorithms and the Rule of Law*, in *Computers and Law*, aprile/maggio 2017, 23 ss.

[3] Si rinvia qui alle considerazioni in E. MAESTRI, *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, cit., 24 ss. e alla letteratura ivi citata.

[4] Cfr. G. DE MINICO, Big Data *e la debole resistenza delle categorie giuridiche*. Privacy *e* lex mercatoria, in *Diritto pubblico*, 1, 2019, 89 ss. secondo cui, di fronte all'imporsi dei *big data*, «gli antichi paradigmi cedono il posto ai nuovi che il decisore politico disegnerà in coerenza con gli obiettivi della regolazione» (89).

[5] Cfr. W. BARFIELD, *Towards a Law of Artificial Intelligence*, in W. BARFIELD, U. PAGALLO (a cura di), *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar, Cheltenham, 2018, 2 ss.; W. HOFFMANN-RIEM, *Artificial Intelligence as a Challenge for Law and Regulation*, in T. WISCHMEYER, T., RADEMACHER (a cura di), *Regulating Artificial Intelligence*, Springer, 2020, 1 ss.

[6] R. CALO, *Robotics and the Lessons of Cyberlaw*, cit., 513 ss.

calata dall'alto una disciplina che può risultare essere estranea e inadatta alle esigenze sue e del settore[7]. Il rischio complessivo non è solo che metodi e strumenti giuridici tradizionali vengano condannati alla ineffettività[8], ma soprattutto – prendendo in prestito un termine riferito alla tecnologia e alla teoria economica – che si vada incontro ad una "*disruption*" delle regole giuridiche, ovvero una sorta di "distruzione creatrice"[9] con la quale le regole di diritto verrebbero superate da altre forme di regolazione, in maniera incontrollata[10]. Il diritto, nella regolamentazione delle TRF, si trova infatti ad affrontare una vera e propria competizione con altri sistemi normativi, quali derivanti dall'etica, la tecnica o il mercato: a volte questi sistemi possono funzionare sinergicamente, altre volte invece possono rendere le pretese regolative degli altri sistemi inefficaci o ininfluenti[11]. A questo proposito, ad esempio, si parla di "*technological management*", entro

[7] R. BROWNSWORD, *Law, Technology and Society. Re-Imagining the Regulatory Environment*, Routledge, New York, 2019, 37 ss. Analogamente E. STRADELLA, *La regolazione della Robotica e dell'Intelligenza artificiale: il dibattito, le proposte, le prospettive. Alcuni spunti di riflessione*, in *Media Laws*, 1, 2019, 77 ss.

[8] Che i tentativi di regolazione delle tecnologie algoritmiche non provengano dai circuiti tradizionali della regolazione giuridica è sottolineato anche da A. CELOTTO, *Come regolare gli algoritmi. Il difficile bilanciamento tra scienza, etica e diritto*, cit., 56 s.

[9] Nella teoria economica si fa riferimento alla concezione di Schumpeter del processo di "distruzione creatrice", nel quale le innovazioni prendono il posto delle tecnologie preesistenti rendendole obsolete, e alla nota costruzione riferita alla intrinseca dinamicità del capitalismo e al suo carattere rivoluzionario, elaborata in polemica con la teorica di Karl Marx. Si tratta di un processo di innovazione che «incessantly revolutionizes the economic structure from within, incessantly destroying the old one, incessantly creating a new one. This process of Creative Destruction is the essential fact about capitalism»; cfr. J.A. SCHUMPETER, *Capitalism, Socialism and Democracy*, Harper, New York, 1950, 83 ss. Più approfondimente, sul pensiero dei due AA., v. J.E. ELLIOT, *Marx and Schumpeter on Capitalism's Creative Destruction: A Comparative Restatement*, in *The Quarterly Journal of Economics*, 95, 1, 1980, 45 ss.

[10] In generale, v. N.K. KATYAL, *Disruptive Technologies and the Law*, in *The Georgetown Law Journal*, 102, 2014, 1685 ss. Osserva R. BROWNSWORD, *Law, Technology and* Society, cit., 181 ss., come vi sia una duplice *disruption*, ovvero nella sostanza e nei contenuti della legge, ma anche nelle forme di regolazione, ovvero nell'uso e nel mancato uso delle regole giuridiche.

[11] Così, in generale, U. PAGALLO, M. DURANTE, *The Pros and Cons of Legal Automation and its Governance*, in *European Journal of Risk Regulation*, 2, 2016, 331.

cui concorrono una "dimensione normativa" e una tipicamente "non normativa"[12].

Per provare a tracciare qualche coordinata sugli elementi di cui tener conto per delineare questi nuovi approcci alla regolamentazione giuridica, sarà quindi utile attingere agli strumenti offerti dalla più ampia categoria della "*regolazione*", intesa come «the intentional influencing of someone's or something's behaviour»[13]. Dalla analisi fin qui svolta, infatti, emerge come la prassi più recente in tema di TRF dia conto dell'emergere di forme di regolazione più variegate e fra loro complementari. Nel presente Capitolo si vuole offrire una sistematizzazione di questa prassi, da cui cogliere alcuni spunti che potrebbero risultare utili ad evitare la paventata "*disruption*". L'obiettivo di fondo non vuole essere quello di difendere a oltranza il ruolo del diritto, bensì assumere consapevolezza di questo concorso tra sistemi normativi, trovando le forme più proficue di interazione e integrazione dei rispettivi strumenti di regolazione, facendo leva sui relativi punti di forza e ovviando ai punti di debolezza. Attraverso questa combinazione verrà composto un quadro complesso, ma si pensa più efficace, destinato a definire la normazione giuridica delle TRF.

[12] Cfr. R. BROWNSWORD, *Law, Technology and Society*, cit., 39, che sottolinea come occorra riconoscere «*the channelling and constraining effect of technological management*», inteso come «*regulatory environment that accommodates both normative and non-normative approaches*», i primi facendo salva la possibilità di trasgredire una norma, i secondi rendendo ciò estremamente più difficile (*ivi*, 58).

[13] Quella citata è l'ampia definizione in B.-J. KOOPS, *Ten dimensions of technology regulation. Finding your bearings in the research space of an emerging discipline*, in M.E.A. GOODWIN, B.-J. KOOPS, R.E. LEENES (a cura di), *Dimensions of technology regulation*, Nijmegen, Wolf Legal Publishers, 2010, 309 ss. In senso più specifico, cfr. J. BLACK, *Critical Reflections on Regulation*, in *Australian Journal of Law and Philosophy*, 1, 27, 2002, 26, secondo cui «regulation is the sustained and focused attempt to alter the behaviour of others according to defined standards or purposes with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information-gathering and behaviour-modification». Per una ulteriore definizione di regolazione più restrittiva, cfr. K. YEUNG, *Algorithmic Regulation: A Critical Interrogation*, in *Regulation & Governance*, 12, 2018, 507, che enfatizza l'obiettivo verso cui i regolatori vogliono indirizzare il comportamento dei consociati, e per questo si sofferma anche su soggetti coinvolti nella regolazione (anche non pubblici), la diversità nella platea dei soggetti regolati (da se stessi, all'intera società), il soggetto responsabile della "direzione" da impartire con la regolazione.

2. *La* risk-regulation *delle TRF: la rilevanza complessiva del principio di precauzione*

Lo sviluppo delle nuove tecnologie, nel produrre conseguenze difficilmente prevedibili a lungo termine, ha contribuito in modo determinante a qualificare quella che – come noto – nella "nuova modernità" viene chiamata "società del rischio"[14]. A fronte della potenziale incidenza esercitata dalle TRF sui diritti fondamentali, è stata giustamente sostenuta da taluni la necessità che la regolamentazione giuridica in ambiti di questo tipo debba ispirarsi al *principio di precauzione*, dal momento che non solo siamo di fronte al pericolo, attualmente non valutabile con certezza, che determinate tecnologie risultino dannose per l'essere umano e le società, ma soprattutto che sistemi efficaci di regolamentazione non siano stati ancora elaborati contro queste evenienze[15]. Nella disamina delle forme complementari di regolazione alle TRF, dunque, è opportuno avviare l'analisi dalla valenza regolativa assunta dal principio di precauzione, in quanto volta non solo a strutturare quella che può essere definita come "regolazione del rischio", ma, più in generale, ad offrire un criterio guida nei confronti delle altre forme di regolazione che si andranno a richiamare qui di seguito.

Il principio di precauzione – come noto – nasce per offrire risposta al problema della valutazione e gestione dei rischi per la salute e per l'ambiente quando la scienza non è in grado di fornire delle certezze riguardo ai pericoli, agli oneri e agli effetti collaterali connessi ad una determinata attività[16].

[14] Si fa qui riferimento alla nota elaborazione sociologica di U. BECK, *La società del rischio. Verso una seconda modernità*, Carocci, Roma, 2013. Che nella "tecnica" sia inevitabilmente insito anche il "rischio" è oggetto delle riflessioni in N. LUHMANN, *Sociologia del rischio*, Mondadori, Milano, 1996, spec. 98 ss.

[15] Così A. SIMONCINI, *Sovranità e potere nell'era digitale*, cit., 36; ID., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, cit., 86 s. Ma si veda già S. RODOTÀ, *Il diritto di avere diritti*, cit., 403.

[16] A. ZEI, *Principio di precauzione*, in *Dig. disc. pubbl.*, Agg. III, II, 2008, 670. Sull'origine de principio di precauzione, dalla elaborazione del *Vorsorgeprinzip* nell'ordinamento tedesco a partire dagli anni '70 del secolo scorso, all'affermazione in ambito internazionale nella tutela dell'ambiente, sino alla diffusione in ambito comunitario con l'art. 130R del Trattato di Maastricht e le diverse direttive in tema di am-

Nonostante la sua diffusione nella regolazione di numerosi ambiti materiali[17], le elaborazioni dottrinali[18] e le più celebri definizioni enunciate nei documenti internazionali[19], il principio di precauzione conserva ancora una notevole indeterminatezza quanto ai relativi contenuti[20]. Uno dei principali documenti istituzionali che offrono una cornice organica a questo principio è la comunicazione della Commissione europea sul principio di precauzione, risalente al 2000, secondo cui tale

biente e sicurezza alimentare, v. G. MANFREDI, *Note sull'attuazione del principio di precauzione in diritto pubblico*, in *Diritto pubblico*, 3, 2004, 1077 ss. Più di recente, v. R. TITOMANLIO, *Il principio di precauzione fra ordinamento europeo e ordinamento italiano*, Giappichelli, Torino, 2018, 1 ss.

[17] Tale principio informa oggi la regolazione di numerosi ambiti materiali, come ambiente, salute, finanza, tutela dei consumatori, sicurezza pubblica; ciascuno particolarmente segnato dallo sviluppo delle nuove tecnologie; per una panoramica sulla applicazione di questo principio nei vari ambiti di regolazione, v. P. DE VINCENTIIS, F. CULASSO, S.A. CERRATO (a cura di), *The Future of Risk Management. I. Perspectives on Law, Healthcare, and the Environment*, Springer, Cham, 2019; ID., *The Future of Risk Management. II. Perspectives on Financial and Corporate Strategies*, Springer, Cham, 2019.

[18] Nella tutela dell'ambiente, si considerino i sei concetti riportati in S. GRASSI, *Prime osservazioni sul "principio di precauzione" come norma di diritto positivo*, in *Dir. gest. amb.*, 1, 2001, 45 s., ovvero anticipazione preventiva; salvaguardia degli ecosistemi o spazi ambientali liberi; proporzionalità della risposta o efficacia rispetto ai costi dei margini di errore; dovere di cautela, o inversione dell'onere della prova; promozione dei diritti naturali intrinseci; obbligo di pagare per il debito ecologico causato nel passato.

[19] Si pensi alla celebre Dichiarazione di Rio de Janeiro delle NU, secondo cui «Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation»; oppure alla definizione elaborata in esito alla Conferenza organizzata dalla *Science and Environment Health Network* (SEHN) nel 1998, secondo cui «[w]hen an activity raises threats of harm to human health or the environment, precautionary measures should be taken even if some cause and effect relationships are not fully established scientifically».

[20] Una complessità e indeterminatezza che stanno alla base delle numerose critiche mosse a tale principio. V. ad esempio C.R. SUNSTEIN, *Il diritto della paura*, il Mulino, Bologna, 2010, per le critiche circa l'intrinseca "incoerenza del principio di precauzione", in quanto "principio paralizzante". Secondo l'A. occorrebbe non parlare di rischi in genere, bensì di rischi particolari e di "piccoli" principi di precauzione che ampliano i margini di sicurezza con riferimento ad essi (spec. 42 ss.).

principio può essere invocato quando un fenomeno, un prodotto o un processo può avere effetti potenzialmente pericolosi, individuati tramite una valutazione scientifica e obiettiva, se questa valutazione non consente di determinare il rischio con sufficiente certezza[21]. Il principio precauzionale viene così intimamente connesso al concetto di definizione del "*rischio*", con il quale condividono la stessa matrice "prudenziale", poiché tesi ad anticipare la soglia di rilevanza di fenomeni lesivi, traducendosi nell'esigenza di rappresentare anticipatamente, e quindi di scongiurare preventivamente, eventi potenzialmente dannosi[22]. Tale principio assume così ad oggetto il metodo di valutazione, calcolo, gestione e comunicazione dei rischi che la scienza non è in grado di rilevare pienamente[23].

Tenendo dunque fermi i fattori di "incertezza scientifica" e di "rischio", ai fini dell'analisi sulle FRT preme chiarire due aspetti di fondo che possono condizionare la regolazione in questo ambito.

Innanzitutto, i contenuti e le procedure di normazione che si rifanno al principio di precauzione sono aperti a tre grandi ordini di valutazione, ovvero: la dimensione politica, nella scelta del livello di rischio accettabile e della relativa gestione; quella tecnico-scientifica, legata allo sviluppo tecnologico e alla valutazione (incerta) dei potenziali pericoli che ne nascono; quella economica, in particolare dal punto di visita metodologico, nella analisi in termini di costi/benefici derivanti

[21] Cfr. COMMISSIONE DELLE CE, *Comunicazione della Commissione sul principio di precauzione*, COM(2000) 1 final, 2 febbraio 2000. In particolare, tale principio costituisce una "strategia di gestione dei rischi" nella misura in cui vi sono ragionevoli motivi di temere il concretizzarsi di potenziali pericoli, ma i dati disponibili non consentono una valutazione particolareggiata del rischio (*ivi*, 2). In questo modo, «il fatto di invocare o no il principio di precauzione è una decisione esercitata in condizioni in cui le informazioni scientifiche sono insufficienti, non conclusive o incerte e vi sono indicazioni che i possibili effetti sull'ambiente e sulla salute degli esseri umani, degli animali e delle piante possono essere potenzialmente pericolosi e incompatibili con il livello di protezione prescelto» (*ivi*, 7 s.). Ricorda la centralità di questo documento, anche di recente, M. GRAZIADEI, *La regolazione del rischio e il principio di precauzione: Stati Uniti ed Europa a confronto*, in *Sistemi intelligenti*, 2, 2017, 500 s.

[22] M.C. TALLACCHINI, *Ambiente e diritto della scienza incerta*, in S. GRASSI, M. CECCHETTI, A. ANDRONIO, *Ambiente e diritto*, I, Olschi, Firenze, 1999, 81.

[23] S. GRASSI, *Prime osservazioni sul "principio di precauzione" come norma di diritto positivo*, cit., 57.

dall'impiego delle tecnologie, da condurre tenendo conto anche dello stato di incertezza epistemologica[24].

Il principio di precauzione, inoltre, può essere caricato di significati differenti a seconda dell'angolo visuale, della sensibilità, delle attese o dei timori dell'interprete[25]: chi nutre una sfiducia più accentuata nei confronti delle innovazioni tecnologiche sarà indotto a ritenere che tale principio possa giustificare addirittura la messa al bando di certe tecnologie, mentre chi nutre il timore dell'avvento di una qualche forma di "neooscurantismo antiscientifico" sarà inevitabilmente portato a restringerne la portata applicativa.

La complessità delle valutazioni presupposte e la permeabilità di questo principio a presupposizioni ideologiche dovrebbero indurre, prudenzialmente, a non cedere alla tentazione di immaginare sempre il "*worst-case scenario*", ovvero adottare un pregiudizio sistematico nei confronti di tecnologie come quelle di riconoscimento facciale, le quali possono essere viste esclusivamente come fonte di rischio e, perciò, da vietare. Il principio di precauzione può essere valorizzato soprattutto per la sua spiccata valenza procedurale e metodologica nel guidare le decisioni[26], in grado di far emergere gli interessi in gioco e condurre ad una loro composizione più equilibrata e bilanciata, alla luce dei rischi pendenti[27].

[24] Spunti ripresi da L. BUFFONI, A. CARDONE, *Il procedimento normativo precauzionale come caso paradigmatico del ravvicinamento "formale-procedurale" delle "fonti" del diritto*, in *Osservatorio sulle fonti*, 3, 2012, 2.

[25] G. MANFREDI, *Note sull'attuazione del principio di precauzione in diritto pubblico*, cit., 1090.

[26] Per la distinzione tra le diverse accezioni del principio di precauzione come regola decisionale, come principio epistemologico o etico, o come principio procedurale e metodologico, v. M. AHTEENSUU, P. SANDIN, *The Precautionary Principle*, in S. ROESER, R. HILLERBRAND, P. SANDIN, M. PETERSON (a cura di), *Handbook of Risk Theory*, Springer, 2012, 963 ss., anche per i richiami della letteratura specialistica.

[27] È lo stesso risultato cui giungono coloro che muovono una obiezione fondamentale alla teoria del "*precautionary constitutionalism*", propendendo invece per un diverso "o*ptimizing constitutionalism*", che esorta a non assolutizzare il concetto di rischio, bensì a soppesare i rischi politici caso per caso e in relazione alle diverse circostanze, per poi operare un bilanciamento in termini ottimali: l'obiettivo del regolatore, in questo caso, non dovrebbe essere "*maximal precautions*", ma "*optimal precautions*"; cfr. A. VERMEULE, *The Constitution of Risk*, Cambridge, New York, 2014, 77.

In questo contesto, ai fini della regolazione delle nuove tecnologie, il principio di precauzione è stato valorizzato soprattutto dalle istituzioni europee piuttosto che dalle autorità nazionali[28]. Se ne ha riprova nei più recenti atti di indirizzo riferiti all'IA cui si è fatto più volte riferimento. Già il Parlamento europeo, nella sua risoluzione del 2017 sulla robotica, ha indicato la valutazione dei rischi come condizione per il finanziamento dei progetti di sviluppo tecnologico e come guida attraverso cui i ricercatori nel settore possono massimizzare i vantaggi e ridurre i potenziali danni[29]. Nel 2019, più in generale, il Parlamento ha richiamato alla necessità che «la ricerca sull'IA e altre attività correlate dovrebbero essere condotte nel rispetto del principio di precauzione e dei diritti fondamentali»[30]. Ma è nel più recente Libro Bianco sulla IA del 2020 che la Commissione ha deciso di promuovere un vero e proprio «*risk-based approach*» nella regolazione dell'IA, per garantire che l'intervento normativo sia proporzionato ai rischi posti da queste tecnologie nei confronti "della protezione della sicurezza, dei diritti dei consumatori e dei diritti fondamentali"[31]. In particolare, la Commissione, nel promuovere la costruzione di una cornice regolatoria uniforme a livello europeo, ha posto l'accento sugli impieghi dell'IA considerati ad "*high risk*"[32], in considerazione del duplice criterio riguar-

[28] Come rilevato anche da P. ZUDDAS, *Pregiudizi digitali e principio di precauzione*, in *Consulta online*, 2, 2020, 413 s., con riguardo al Libro Bianco dal titolo "L'Intelligenza Artificiale al servizio del cittadino", curato nel marzo 2018 dall'Agenzia per l'Italia Digitale, e nelle "Proposte per una Strategia Italiana per l'Intelligenza Artificiale", elaborate dal Gruppo di Esperti del MISE sull'Intelligenza Artificiale nel luglio 2019.

[29] Cfr. PARLAMENTO EUROPEO, *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, cit., ove si sottolinea che «gli organismi pubblici e privati di finanziamento della ricerca sulla robotica dovrebbero esigere che ogni proposta di finanziamento di attività di ricerca in materia sia corredata di una valutazione dei rischi», e si aggiunge anche che «il funzionamento di un sistema robotico dovrebbe sempre basarsi su un rigoroso processo di valutazione dei rischi, che dovrebbe essere improntato ai principi di proporzionalità e di precauzione» (allegato).

[30] PARLAMENTO EUROPEO, *Una politica industriale europea globale in materia di robotica e intelligenza artificiale*, cit., p. 19.

[31] EUROPEAN COMMISSION, White Paper "*On Artificial Intelligence - A European approach to excellence and trust*", cit., 17 s.

[32] Nonostante che il Garante europeo abbia criticato tale categorizzazione perché

dante il settore in cui essi ricadono e l'uso che concretamente viene fatto. Le TRF, rientrando nelle applicazioni di IA "per scopi di identificazione biometrica a distanza", sono espressamente considerate ad "alto rischio"[33]. Di conseguenza, la normativa dovrebbe stabilire "requisiti giuridici obbligatori" per una serie di profili che – come anche emerso fin qui – possono essere fonti di tali rischi, riguardanti segnatamente: i dati con cui vengono allenati gli algoritmi; la conservazione dei dati e il loro tracciamento in relazione al relativo utilizzo; la informazioni circa gli algoritmi impiegati e l'architettura dei sistemi di IA; le informazioni da rendere agli interessati relative all'impiego del sistema, per assicurare una maggiore trasparenza; l'accuratezza e la robustezza del sistema, per garantirne l'affidabilità e la sicurezza; il controllo dell'essere umano, nei confronti del funzionamento complessivo del sistema e in occasione della singola decisione adottata[34].

Il principio di precauzione viene in gioco per guidare il legislatore nella definizione di tali "requisiti giuridici obbligatori". A questo scopo, si potrebbe sostenere che tale principio si carichi di significati "forti" o "deboli", in ragione – come detto sopra – anche dei diversi ordini di valutazione presupposti (politici, tecnici, economici), del soggetto che ne fa applicazione e, in ultimo, della coscienza sociale in un dato momento storico[35].

Nei suoi significati "forti", il principio in questione può operare

troppo rigida e poco attenta alle specificità di questi mezzi tecnologici, come invece richiederebbe un approccio propriamente precauzionale; cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust*, cit., p. 27.

[33] *Ibidem*.

[34] *Ivi*, 18 ss., con riguardo a «*training data*, *data and record-keeping*, *information to be provided*, *robustness and accuracy*, *human oversight*, *specific requirements for certain particular AI applications*». Requisiti specifici vengono richiesti proprio per la "identificazione biometrica a distanza", come "l'impiego di riconoscimento facciale negli spazi pubblici", portatore di "specifici rischi per i diritti fondamentali".

[35] Sulle interpretazioni "deboli" e "forti" del principio di precauzione, v. M. AHTEENSUU, P. SANDIN, *The Precautionary Principle*, cit., 970, che richiamano le due dichiarazioni elaborate a livello internazionale, riportate sopra in nota 19, come due classici esempi, rispettivamente, in questo senso. Cfr. anche J. MORRIS, *Defining the Precautionary Principle*, in ID. (a cura di), *Rethinking Risk and the Precautionary Principle*, Butterworth-Heinemann, Oxford, 2000, 1 ss.

come "regola per decidere"[36], postulando un obbligo di cautela e di astensione dalle attività di cui siano ignoti i potenziali effetti negativi. Si valorizza così quella accezione del principio di precauzione come "anticipazione preventiva", che impone di intraprendere le azioni precauzionali che consentano di evitare, o comunque minimizzare, i possibili danni «rispetto alla prova scientifica dell'evidenza del bisogno di intervenire», sulla base del fatto che un ritardo potrebbe costare troppo alla società, specie nel lungo periodo[37]. In questo senso, il principio di precauzione colloca la soglia della necessità di circondare di cautele l'impiego di TRF, giustificandone al limite la relativa preclusione, in presenza di rischi per i diversi profili richiamati sopra: ad esempio la presenza di *bias* non chiaramente identificabili all'interno del *dataset* impiegato per allenare gli algoritmi di riconoscimento facciale; la possibilità o meno di ottenere informazioni sufficientemente esaustive relative al funzionamento di tali sistemi; poter sottoporre efficacemente a test preliminari di verifica l'accuratezza dello stesso; applicare soluzioni crittografiche in grado di garantire la sicurezza delle immagini raccolte o utilizzate nelle gallerie. In assenza di queste condizioni, si potrebbe al limite giungere a vietare le TRF e, se allo stato non fosse possibile disciplinare tali condizioni, sarebbe giustificata l'imposizione di una moratoria o un divieto temporaneo, sulla scorta di quanto deciso da taluni enti territoriali negli Stati Uniti o di cui si discute in UE[38].

Nei suoi significati "deboli", invece, il principio di precauzione opererebbe come "regola per procedere"[39], con la quale non si pone l'accento tanto sull'anticipazione della soglia entro cui predisporre misure precauzionali, ma si impone un obbligo di "presa in considerazione" dell'incertezza scientifica nell'ambito di una analisi costi/benefici o rischi/benefici, nella quale peserebbero anche i costi dei margini di errore non prevedibili[40]. In questi termini, le misure restrittive all'impiego delle TRF da cui potrebbero scaturire rischi impreve-

[36] Così P. ZUDDAS, *Pregiudizi digitali e principio di precauzione*, cit., 420.

[37] S. GRASSI, *Prime osservazioni sul "principio di precauzione" come norma di diritto positivo*, cit., 45.

[38] Cfr. *retro* Introduzione.

[39] Così P. ZUDDAS, *Pregiudizi digitali e principio di precauzione*, cit., 420.

[40] S. GRASSI, *Prime osservazioni sul "principio di precauzione" come norma di diritto positivo*, cit., 45.

dibili verrebbero a loro volta limitate in termini di proporzionalità, nella ricerca di un giusto equilibrio tra efficacia delle preclusioni e costi conseguenti da sopportare. Così, ad entrare nella valutazione sulle condizioni di utilizzabilità di queste tecnologie vi sarebbero anche, ad esempio, le conseguenze in termini di riduzione o meno dell'efficienza e della rapidità della decisione adoperata con l'ausilio di TRF (si pensi a quanto avviene nel settore della sicurezza pubblica o nelle politiche di immigrazione), non da ultimo la sostenibilità economica di tale rinuncia[41]. Tuttavia, si tratterebbe – è bene ricordarlo – di una operazione di bilanciamento che si configurerebbe come "ineguale", nella quale la tutela dei diritti fondamentali non potrebbe che assumere un "peso" decisivo rispetto ad altre istanze, come quelle economiche[42].

Nel senso indicato, il principio di precauzione e la regolazione del rischio acquisiscono pregnanza sotto una molteplicità di dimensioni rilevanti per la nostra analisi. Si pensi innanzitutto alla loro valenza strumentale, nella misura in cui si declinano in una serie di tecniche e istituti che improntano le tutele dei diritti ad una logica non puramente rimediale e risarcitoria, bensì anticipata, preventiva e proattiva. È l'impostazione adottata, come visto, dalla più recente disciplina sulla protezione dei dati personali[43], ma che viene auspicata, ad esempio, anche per la riforma del regime di responsabilità civile per le applicazioni dei sistemi di IA[44].

[41] La già citata comunicazione della Commissione europea sul principio di precauzione fornisce utili riferimenti metodologici in relazione alla predisposizione delle misure precauzionali, secondo i diversi criteri di: a) proporzionalità; b) non discriminazione; c) coerenza con le misure adottate in situazioni analoghe; d) valutazione del rapporto vantaggi/oneri derivanti dall'azione e inazione; e) attenzione all'evoluzione scientifica: a pesare, nel caso della valutazione relativa alle TRF, sarebbero soprattutto i criteri alle lett. a) e d). Cfr. COMMISSIONE DELLE CE, *Comunicazione della Commissione sul principio di precauzione*, cit., 17 ss.

[42] Così prendendo in prestito il criterio – invero affatto pacifico – impiegato dalla Corte costituzionale per guidare il bilanciamento tra diritti sociali ed esigenze di bilancio; in dottrina, su tutti, v. tra i primi M. LUCIANI, *Sui diritti sociali*, in AA.VV., *Studi in onore di Manlio Mazziotti di Celso*, Cedam, Padova, 1995, 127 ss., e, da ultimo, S. FILIPPI, *La giurisprudenza costituzionale tra congiuntura economica ed evoluzione del sistema delle fonti: verso l'affermazione dell'"argomento della crisi"?*, in *Osservatorio sulle fonti*, 3, 2020, 1590 ss.

[43] V. *retro* Cap. III, par. 2.

[44] Sul punto, cfr. A. BERTOLINI, *Artificial Intelligence and Civil Liability*. *Study re-*

Secondo questa accezione, concordemente alle sollecitazioni della Commissione europea[45] e del Consiglio d'Europa[46], la *risk-regulation* può assumere la forma delle diverse tecniche di *analisi del rischio e di impatto sui diritti fondamentali* da esperire in relazione al puntuale impiego delle TRF in singoli contesti. Tra le elaborazioni meglio sviluppate e consolidate a livello normativo, per quanto qui interessa maggiormente, vi è la "valutazione d'impatto sulla protezione dei dati"[47], recentemente introdotta dalla legislazione in questione e volta ad identificare, valutare e gestire i "rischi elevati" per i diritti e le libertà prima che vanga effettuato il trattamento dei dati, anticipandone i possibili effetti[48]. Queste forme di analisi sono state anche declinate in alcune

quested by the JURI committee, PE 621.926, luglio 2020, 13 ss. e 99 ss., ove si suggerisce di attribuire tale responsabilità verso chi subisce un danno al soggetto nella migliore posizione per identificare il rischio, verificarlo e minimizzarlo attraverso le sue scelte, e gestirlo. Tale soggetto potrebbe cambiare a seconda delle diverse applicazioni tecnologiche: ad esempio, in alcuni casi potrebbe essere appropriato imputare la responsabilità all'operatore che impiega la tecnologia (come ne caso dei droni), all'azienda che si occupa di integrare i sistemi tecnologici (ad es. nel caso della robotica industriale avanzata), il fornitore dei servizi (ad es. nel caso dei servizi di consulenza), al produttore (ad es. nel caso dei veicoli a guida autonoma). Più ampiamente, v. anche EUROPEAN COMMISSION, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, COM(2020) 64 final, 19 febbraio 2020. In dottrina, v. U. RUFFOLO, *La responsabilità da* artificial intelligence*, algoritmo e* smart product*: per i fondamenti di un diritto dell'intelligenza artificiale* self-learning, in ID. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., 93 ss. Ulteriori anche spunti *retro*, Cap. III, nota 349.

[45] Cfr. CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data,* cit., 3.

[46] EUROPEAN COMMISSION, White Paper "*On Artificial Intelligence - A European approach to excellence and trust*", cit., 23.

[47] Cfr. art. 35 del GDPR; art. 27 della LED.

[48] Più ampiamente, cfr. N. VAN DIJK, R. GELLERT, K. ROMMETVEIT, *A Risk to a Right: Beyond Data Protection Risk Assessments*, in *Computer Law & Security Review*, 32, 2, 2016, 286 ss.; R. BINNS, *Data protection impact assessments: a meta-regulatory approach*, in *International Data Privacy Law*, 7, 1, 2017, 22 ss.; A. YORDANOV, *Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation*, in *European Data Protection Law Review*, 3, 4, 2017, 486 ss.; K. DEMETZOU, *Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation*, in *The com-*

tecniche concernenti specificatamente i procedimenti di decisione algoritmica[49], come la c.d. *Algorithmic Impact Assesment*[50] o, più in generale, la "*Fundamental Rights Impact Assessment*"[51].

Ai fini del presente discorso, le ricadute del principio di precauzione e della regolazione del rischio che interessano ulteriormente vanno in una duplice direzione: innanzitutto, come criterio per *guidare i contenuti* della regolazione di specifiche applicazioni delle TRF, specificando le condizioni di utilizzo a partire dalla duplice logica dei significati "deboli" e "forti" sopra richiamata; ma soprattutto, come criterio per *guidare la scelta tra le diverse forme di regolazione* più adeguate allo scopo. È un tipo di valutazione ben conosciuta a livello di istituzioni europee, come dimostrano gli strumenti a disposizione nell'ambito della strategia di "*Better Regulation*" messa in atto dalla Commissione, che contempla anche alcuni metodi per la scelta dei "*policy instruments*"[52]. Come riferito introduttivamente, nel panorama

puter law and security report, 35, 6, 2019, 1 ss.; A. MANTELERO, *La gestione del rischio*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, cit., 473 ss. Si veda anche GRUPPO DI LAVORO ARTICOLO 29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, 4 aprile 2017.

[49] Una necessità sottolineata anche in EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust*, cit., 44.

[50] Cfr. D. REISMAN, J. SCHULTZ, K. CRAWFORD, M. WHITTAKER, *Algorithmic impact assessments: a practical framework for public agency accountability*, AI Now Institute, 2018, quale strumento di valutazione a disposizione delle agenzie pubbliche pensato per essere utilizzato nelle ipotesi di acquisto e utilizzo di tecnologie basate su IA.

[51] Cfr. H.L. JANSSEN, *An approach for a fundamental rights impact assessment to automated decision-making*, in *International data privacy law*, 10, 1, 2020, 76 ss.; A. MANTELERO, *AI and big data: a blueprint for a human rights, social and ethical impact assessment*, in *Computer Law & Security Review*, 34, 4, 2018, 754 ss. Tra le elaborazioni e guide pratiche più sviluppate, v. N. GÖTZMANN, T. BANSAL, E. WRZONCKI, C. POULSEN-HANSEN, J. TEDALDI. R. HØVSGAARD, *Human Rights Impact Assessment. Guidance and Toolbox*, The Danish Institute for Human Rights, 2016.

[52] In particolare, tra i documenti che rientrano nel "*toolbox*" utilizzato dalla Commissione europea per confezionare nuove proposte di atti normativi o valutare la normazione esistente, v. *Tool #18. The choice of policy instruments*, giugno 2017 [bit.ly/2R7nLua]. Più ampiamente, cfr. H. XANTHAKI, *European Union Legislative*

variegato della regolazione delle TRF, assieme alle norme giuridiche in senso stretto concorrono differenti sistemi e strumenti che, come si vedrà, divergono per fattori come cogenza espressa dalle norme o coinvolgimento dei destinatari nell'adozione delle stesse. La decisione su quale strumento regolativo impiegare, secondo quanto qui si propone, dovrà essere assunta proprio alla luce del principio di precauzione. Tale valutazione, da una parte, dovrà appuntarsi sulla ricerca di quale tra essi possa essere più idoneo, in base alle caratteristiche espresse, a far sì che si riesca ad anticipare la soglia di tutela contro i rischi di possibili lesioni ai diritti fondamentali. Dall'altra, al contempo, tale valutazione sarà condizionata da un giudizio sulla proporzionalità tra le implicazioni e le conseguenze rispetto ai costi che ne derivano, in termini, ad esempio, di efficienza e rapidità delle decisioni, effettività delle politiche, oneri economici da sostenere.

3. *La* self-regulation *delle TRF: virtù e vizi dei principi etici*

Dall'analisi della prassi emerge una prima forma di regolazione complementare al diritto che ha trovato una certa diffusione nel settore delle TRF, ovvero la c.d. *self-regulation*, o auto-regolamentazione.

Con questo termine si fa riferimento ad un concetto complesso e dai contorni incerti, che si colloca nella zona grigia tra i due estremi della libertà di mercato, dominata dall'assoluta discrezionalità degli operatori economici, e la regolamentazione "*command and control*", espressione – si è detto – del "controllo totale"[53]. Al fondo, la *self-regulation* consiste in una normativa adottata dal soggetto destinatario della stessa, la quale può variare a seconda di elementi come l'adozione delle regole su base volontaria, il loro grado di cogenza, il loro contenuto tecnico, il coinvolgimento delle istituzioni pubbliche nella loro formazione, il ruolo stesso dei destinatari[54]: si fa quindi rife-

Quality After the Lisbon Treaty: The Challenges of Smart Regulation, in *Statute Law Review*, 1, 2013, 66 ss.; S. TOMBS, *Making better regulation, making regulation better?*, in *Policy Studies*, 4, 2016, 332 ss.

[53] C. COGLIANESE, E. MENDELSON, *Meta-Regulation and Self-Regulation*, cit., 146.

[54] Cfr. J. BLACK, *Decentring Regulation: Understanding the Role of Regulation and*

rimento alle più varie tipologie di regole, linee guida o standard, adottati dalle singole imprese, da più imprese in accordo, dalle loro forme associative o da *partnership* pubblico-private. L'universo della *self-regulation*, comunque, origina da un approccio *bottom-up*, espressione di una diversa concezione nei rapporti tra soggetto regolatore e soggetti regolati[55],

Nel settore del riconoscimento facciale, questo tipo di regolazione ha avuto particolare diffusione in quegli ordinamenti entro cui, da una parte, le industrie dell'*high tech* sono più attive e, dall'altra, manca una regolazione di tipo legislativo che possa interessare anche solo indirettamente le TRF, come una disciplina a protezione dei dati personali.

Self-regulation in a 'Post-regulatory' World, *Current Legal Problems*, 54, 1, 2001, 121, che sottolinea il carattere fortemente ambiguo del termine: «self-regulation is used to mean variously soft law, collective arrangements that may be non-legal, and/or entail no government involvement, bilateral arrangements between firms and the government, unilateral adoption of standards, the involvement of industry in rule-formation, neo-corporatist arrangements in which the collective shares in the state's authority to make decisions about standards of conduct, monitoring, and enforcement, but in which the relationship with government may vary, and/or in which those other than the persons being regulated may play a role (auditors, stakeholders). Self-regulation can additionally or alternatively mean intra-firm regulation; it can mean private contracting. What anyone definition of 'self-regulation' does not encompass is picked up by other labels: co-regulation, quasi-regulation, quasi-law, soft law, voluntarism, the exact application of those labels varying with the model of 'self-regulation' to which it is opposed».

[55] Quella indicate è una delle due prospettive con cui guardare alla *self-regulation*, ovvero a partire dal ruolo regolativo dello Stato. Secondo I. BARTLE, P. VASS, *Self-Regulation within the Regulatory State: Towards a New Regulatory Paradigm?*, in *Public Administration*, 85, 4, 2007, 885 ss., è possibile guardare a tale fenomeno regolatorio anche a partire dalla complessità sociale, ovvero come conseguenza della frammentazione e della dispersione del potere, delle dinamiche e delle interdipendenze che si innescano tra attori all'interno di sistemi complessi. In questo caso, come sottolinea J. BLACK, *Decentring Regulation: Understanding the Role of Regulation and Self-regulation in a 'Post-regulatory' World*, cit., 103 ss., si pone l'accento sul carattere "decentrato" della regolazione, o sul momento "autopoietico", inteso come capacità di un sistema di costruire spontaneamente proprie strutture attraverso cui dare forma ad un ordinamento autonomo e alterare tali strutture secondo propri criteri (*self-reflexive*); sul punto cfr. anche G. TEUBNER, *Evolution of autopietic Law*, in G. TEUBNER (a cura di), *Autopoietic Law: a new approach to law and society*, Walter de Gruyten, Berlino-New York, 1988, 217 ss.

Caso paradigmatico in questo senso è offerto dagli Stati Uniti, ove alcuni Stati si sono attivati per adottare una propria disciplina, ma manca a livello federale una normativa analoga al GDPR[56]. Conseguentemente, si assiste all'iniziativa autonoma di organizzazioni non governative[57] e, soprattutto, degli stessi *Big Tech* principalmente impegnati nella ricerca e sviluppo di queste tecnologie, come Amazon[58], Google[59], Microsoft[60], numerosi dei quali si sono dotati di "*ethical board*"[61]. Si tratta in prevalenza, appunto, di principi di natura etica, che spesso richiamano i valori, se non i contenuti veri e propri, alla base della legislazione sulla protezione dei dati personali, ad esempio, vigente in UE.

I fautori della *self-regulation* sostengono che, tramite questi strumenti sia possibile ovviare alle rigidità della *hard law*, soddisfando una maggiore velocità, flessibilità, sensibilità alle dinamiche di mercato, e minori costi[62]. L'auto-regolazione – si dice – riesce meglio ad esprimere il punto di vista delle imprese e degli operatori economici, ossia di

[56] Maggiori riferimenti dottrinali e giurisprudenziali in S. NAKAR, D. GREENBAUM, *Now you see me. Now you still do: facial recognition technology and the growing lack of privacy*, cit., 102 ss. In questo ordinamento, invece, sono piuttosto consolidati i "*Fair Information Practicies Principle*", i quali, seppure non impongano vincoli legali, valgono comunque ad offrire un quadro uniforme e direttive per bilanciare la tutela della *privacy* con altri interessi.

[57] Per limitarsi agli esempi più recenti, si pensi ai "*Privacy Principles for Facial Recognition Technology in Commercial Applications*", pubblicati nel settembre 2018 dal *Future of Privacy Forum*, organizzazione noprofit di cui fanno parte imprese e fondazioni private. Si pensi anche ai "*Facial Recognition Policy Principles*", adottati nel dicembre 2019 dalla *U.S. Chamber of Commerce*, organizzazione anch'essa non governativa che riunisce oltre tre milioni di imprese.

[58] M. PUNKE, *Some Thoughts on Facial Recognition Legislation*, in *AWS Machine Learning Blog*, 7 febbraio 2019 [amzn.to/39Q3qjN].

[59] GOOGLE AI, *Our approach to facial recognition* [bit.ly/3uo7Whc]; GOOGLE, *AI Principles 2020. Progress update* [bit.ly/2PMlBjt].

[60] MICROSOFT CORPORATION, S*ix Principles for Developing and Deploying Facial Recognition Technology*, dicembre 2018 [bit.ly/3fNnp6o].

[61] Cfr. A. MAYNARD, *Ethics Boards Won't Save Big Tech*, in *OneZero*, 15 aprile 2019 [bit.ly/3ac1Bom]; E. MOSS, J. METCALF, *The Ethical Dilemma at the Heart of Big Tech Companies*, in *Harvard Business Review*, 14 novembre 2019.

[62] N. GUNNINGHAM, J. REES, *Industry Self-Regulation: An Institutional Perspective*, in *Law & Policy*, 19, 1997, 366.

coloro che possiedono un maggior bagaglio di informazioni tecniche; che sono al passo con gli sviluppi tecnologici; che hanno un quadro più chiaro degli interessi in gioco; che percepiscono la vera consistenza delle problematiche e conoscono meglio i destinatari stessi della regolazione.

Non occorre sminuire lo sforzo di iniziative volte ad approfondire l'impatto etico delle TRF e orientare queste tecnologie verso valori umani condivisi. Piuttosto, occorre mettere in guardia dai rischi di un approccio che ritenga la *self-regulation* di per sé sola adeguata e sufficiente a regolare le TRF.

Quanto alle norme etiche, si consideri solamente la loro natura non vincolante[63], o l'eccessiva generalità con cui sono formulati i principi etici[64], o la mancanza di un consenso unanime attorno alla loro definizione nei regimi pluralistici contemporanei[65].

Quanto all'utilizzo della *self-regulation*, più in generale, sono state criticamente sottolineate le ragioni per cui i *Big Tech* dominanti preferiscano gli standard etici piuttosto che le norme giuridiche vincolanti, a partire dalla mancanza di sanzioni in caso di violazione[66]. Si tratta di soggetti che, tramite questa soluzione, riescono comunque a perseguire i propri interessi – soprattutto economici – e ad imporre il proprio punto di vista, a potenziale discapito dell'interesse generale. In assenza di alcuna rappresentatività, inoltre, riescono anche ad impostare un processo regolativo privo della trasparenza tipica dei processi decisionali degli organi politici[67]. Lasciare il governo di queste tecnologie agli

[63] COUNCIL OF EUROPE, *Discrimination, artificial intelligence, and algorithmic decision-making*, cit., 27.

[64] M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges*, cit., 92.

[65] A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, cit., 11. Come messo in luce dalla filosofia giuridica con riguardo, più in generale, alla regolazione dell'IA, un approccio regolativo troppo schiacciato sull'etica rimane incerto a partire dalle stesse disparità di vedute tra le diverse teorie morali, come l'utilitarismo, il deontologismo o l'etica delle virtù; cfr. U. PAGALLO, *Intelligenza Artificiale e diritto. Linee guida per un oculato intervento normativo*, in *Sistemi intelligenti*, 3, 2017, 618 ss.

[66] R. CALO, *Artificial Intelligence Policy: A Primer and Roadmap*, cit., 408.

[67] D. HIRSCH, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, in *Seattle University Law Review*, 34, 2011, 458.

attori privati, dunque, espone ad una inaccettabile mancanza di responsabilità sul piano giuridico e sociale, oltre che ad un difetto di programmazione a lungo termine sullo sviluppo tecnologico[68]. Basti pensare che la volontà dei *Big Tech* di interrompere lo sviluppo delle TRF ha natura puramente volontaria e si può comprendere anche con la volontà di "cavalcare l'onda" dei timori espressi dalla pubblica opinione[69]. Una volta scaduto il termine di riflessione, nulla impedisce – come già sta accadendo – che la corsa all'innovazione ricominci[70].

In definitiva, questi rilievi spingono ad affermare come non si possa fare ricorso alla *self-regulation* come *alternativa* al diritto[71]. Diverse considerazioni, invece, possono sorgere quando si imposta il discorso sulla regolazione delle TRF in termini di *complementarietà* nel rapporto tra diritto e etica. I due domini, infatti, possono concorrere e contribuire positivamente ad influenzare il comportamento umano e lo sviluppo delle nuove tecnologie[72]. Pur dovendo rimanere debitamente distinti, etica e diritto possono interagire reciprocamente con risultati proficui, come in quelle ipotesi che prospettano una regolamentazione

[68] C. CATH, S. WACHTER, B. MITTELSTADT, M. TADDEO, L. FLORIDI, *Artificial Intelligence and the 'Good Society': the US, EU, and UK approach*, in *Sci Eng Ethics*, 24, 2018, 507 s.

[69] R. BROWNE, *Tech giants want rules on facial recognition, but critics warn that won't be enough*, in *CNBC*, 30 agosto 2019 [cnb.cx/2RhCumw].

[70] R. WINGFIELD, *Why are major tech companies halting sales of facial recognition technology?*, in *Global Partner Digital*, 26 giugno 2020 [bit.ly/3t0iSBo].

[71] Non appare condivisibile quella posizione che vorrebbe riservare al diritto un ruolo minimale, sul presupposto che l'etica dovrebbe fondare il discorso, più in generale, sui sistemi di IA, mentre il diritto non dovrebbe spingersi molto al di là di quanto già ricomprende, ovvero la disciplina sulla responsabilità di costruttori, proprietari e utilizzatori delle macchine – in una parola, l'uso umano della tecnologia; cfr. J.J. BRYSON, *The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation*, cit., 25 s. Neppure pare sostenibile l'idea che il diritto rappresenti solamente un punto di partenza per identificare le problematiche, mentre spetti solamente all'etica il compito di risolverle, come invece sostenuto in C. CANCA, *Human Rights and AI Ethics – Why Ethics Cannot be Replaced by the UDHR*, in *United Nations University: AI & Global Governance Articles & Insights*, luglio 2019.

[72] B. WAGNER, *Ethics as an Escape from Regulation: From Ethics-Washing to Ethics-Shopping?*, in E. BAYAMLIOĞLU, I. BARALIUC, L. JANSSENS, M. HILDEBRANDT (a cura di), *Being Profiling. Cogitas ergo sum. 10 Years of Profiling the European Citizen*, Amsterdam University Press, Amsterdam, 2018, 86.

giuridica fondata, e non sostituita, dalla c.d. *hard ethics*[73], che aiuti a comprendere quando gli impieghi di TRF a determinate finalità andrebbe vietato[74]. Di contro, la c.d. *soft ethics* non concorre ad indebolire regole e principi giuridici, ma soccorre a colmare le lacune presenti o irrobustire il quadro delle garanzie vigenti, orientando anche l'attività interpretativa del diritto[75].

Anche le istituzioni dell'Unione europea si mostrano generalmente consapevoli di questi rischi. Senza trascurare la valenza normativa degli strumenti di *self-regulation*[76], Parlamento e Commissione europea ribadiscono l'esigenza di un rapporto di complementarietà tra etica e diritto[77]. Gli stessi comitati etici e di esperti mettono in guardia dai possibili fenomeni di "*ethics shopping*"[78], sebbene il rilievo

[73] Cfr. L. FLORIDI, *Soft Ethics and the Governance of the Digital*, in *Philosophy & Technology*, 31, 1, 2018, 4 ss., ovvero quei principi morali che potrebbero spingere a contravvenire le norme giuridiche.

[74] Sull'insufficienza in questo senso della *self-regulation*, cfr. E. LEARNED-MILLER, V. ORDÓÑEZ, J. MORGENSTERN, J. BUOLAMWINI, *Facial Recognition Technologies in the Wild: A Call for a Federal Office*, cit., 4.

[75] Cfr. L. FLORIDI, *Soft Ethics and the Governance of the Digital*, cit., 4 ss., il quale prosegue sostenendo che la *soft ethics* dovrebbe invece riempire gli spazi aperti dalla regolamentazione giuridica, nell'ambito non di ciò che "deve" essere fatto, ma di ciò che "può" essere fatto. V. anche U. PAGALLO, *Etica e diritto dell'Intelligenza Artificiale nella governance digitale: il* Middle-out Approach, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., 32 ss.

[76] Sulla quale, per la relativa diffusione a livello di UE, v. SENDEN, *Soft Law, Self-regulation and Co-regulation in European Law: Where Do They Meet?*, in *Electronic Journal of Comparative Law*, 9, 1, 2005, 1 ss.

[77] Come nella PARLAMENTO EUROPEO, *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, cit., ove si legge che «la proposta di codice etico-deontologico nel settore della robotica getterà le basi per l'identificazione, il controllo e il rispetto di principi etici fondamentali dalla fase di progettazione e di sviluppo», ma anche che «il codice non dovrebbe sostituirsi alla necessità di affrontare tutte le principali questioni giuridiche in materia, bensì avere una funzione complementare». Si consideri anche EUROPEAN COMMISSION, Communication "*Artificial Intelligence for Europe*", cit., ove si legge che «while self-regulation can provide a first set of benchmarks against which emerging applications and outcomes can be assessed, public authorities must ensure that the regulatory frameworks for developing and using of AI technologies are in line with these values and fundamental rights».

[78] Cfr. EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES, *Artificial Intelligence, Robotics and 'Autonomous' Systems*, 9 marzo 2018, 14, ove si

delle regole giuridiche non sempre venga percepito in tutta la sua importanza[79].

4. *La* co-regulation *delle TRF: standard tecnici, codici di condotta e oltre*

Il panorama delle TRF contempla forme di regolazione ulteriori, in continuità con la richiamata *self-regulation*. Quest'ultima, infatti, è una categoria eterogenea che solamente in pochi casi può dirsi puramente spontanea, e che contempla al suo interno anche forme di produzione normativa nelle quali possono essere coinvolte le autorità pubbliche.

A tal proposito è stata proposta una distinzione in quattro tipologie di *self-regulation* a seconda delle relazioni che possono innescarsi con le autorità pubbliche: "delegata", in cui quest'ultima definisce una cornice normativa che viene riempita dalle forme di auto-regolazione; "approvata", in cui le norme auto-prodotte vengono approvate dall'autorità pubblica; "obbligata", in cui la *self-regulation* viene sviluppata in risposta alla minaccia dell'autorità pubblica di imporre sanzioni normative; "volontaria", in cui non c'è alcun coinvolgimento dell'autorità pubblica, diretto o indiretto[80].

Le prime tre ipotesi possono essere propriamente inquadrate in quella che è definibile come *co-regulation*, ove autorità pubbliche e destinatari della regolazione condividono la responsabilità di adottare e attuare la normazione. Tali forme di co-regolazione sono state poi affinate, sul piano teorico, in una pluralità di varianti, a seconda della natura e dello scopo del coinvolgimento del decisore pubblico, come la

sostiene che «regulatory patchworks may give rise to 'ethics shopping', resulting in the relocation of AI development and use to regions with lower ethical standards».

[79] Come avviene in GRUPPO DI ESPERTI AD ALTO LIVELLO SULL'INTELLIGENZA ARTIFICIALE, *Orientamenti etici per un'IA affidabile*, cit., 2 ss., secondo cui per sviluppare una "IA affidabile" occorrono tre componenti, ovvero legalità, eticità e robustezza, trascurando però di affrontare la rilevanza della prima, in quanto si ritiene che le affermazioni concernenti le altre due «sono in qualche misura già presenti nelle leggi vigenti» (nota 1).

[80] Così J. BLACK, *Constitutionalising Self-Regulation*, in *Modern Law Review*, 59, 1, 1996, 27 s., che parla di "*mandated*", "*sanctioned*", "*coerced*" e "*voluntary*" *self-regulation*.

"*process-oriented regulation*"[81], oppure la "*meta-regulation*"[82]. Solitamente è quest'ultimo che pone gli obiettivi e mantiene i tradizionali strumenti di condizionamento, ovvero la leva finanziaria, l'intervento normativo e la gestione delle informazioni (*the carrot*, *the stick*, *the sermon*)[83].

Nel settore delle TRF la co-regolazione viene in rilievo principalmente in ragione dello stretto rapporto che viene ad instaurarsi tra la normativa giuridica e le norme tecniche, o *standards*.

Volendo inquadrare la nozione di standard, è possibile fare riferimento, in senso ampio, alle norme, gli obiettivi, le finalità o le regole attorno alle quali un regime regolatorio è organizzato, tramite procedimenti di adozione che coinvolgono attori pubblici e privati, a livello nazionale e sovranazionale, rendendone così condivisa la responsabilità[84]. In senso stretto, invece, si fa riferimento agli standard elaborati da organi di stan-

[81] Cfr. le considerazioni in S. GILAD, *It runs in the family: Meta-regulation and its siblings*, in *Regulation & Governance*, 4, 4, 2010, 486 ss. Entro di essa sono ricomprese, ad esempio, teorie come la "*enforced self-regulation*" (su cui v. I. AYRES, J. BRAITHWAITE, *Responsive Regulation. Transcending the Deregulation Debate*, Oxford University Press, Oxford, 1992, spec. 101 ss.), in cui è lo Stato che richiede all'industria di adottare la propria *self-regulation* e tali regole possono essere fatte rispettare (*enforced*) anche dal decisore pubblico; oppure la "*management-based regulation*" (su cui v. C. COGLIANESE, J. NASH, *Management-Based Strategies for Improving Private Sector Environmental Performance*, 2005, *Faculty Scholarship. Paper 105*, 5 ss. [bit.ly/3mqZKK8], in cui il soggetto pubblico prefigge degli obiettivi ma, al contempo, definisce e monitora il rispetto di criteri generali in base ai quali il soggetto privato deve adottare una regolazione e sviluppare la propria organizzazione interna per raggiungere tali obiettivi.

[82] Per le ipotesi in cui "ciascun livello regola la regolazione di altri livelli in combinazione di diversi gradi verticali e orizzontali di influenza"; così C. PARKER, C. SCOTT, N. LACEY, J. BRAITHWAITE, *Introduction*, in IID. (a cura di), *Regulating Law*, Oxford University Press, New York, 2004, 6. Cfr. anche S. GILAD, *It runs in the family: Meta-regulation and its siblings*, cit., 485 ss.

[83] Così J.A. DE BRUIJN, E.F. TEN HEUVELHOF, *Policy instruments for steering autopoietic actor*s, in R.J. IN 'T VELD, C.J.A.M. TERMEER, L. SCHAAP, M.J.W. VAN TWIST (a cura di), *Autopoiesis and Configuration Theory: New Approaches to Societal Steering*, Springer, Dordrecht, 1991, 161 ss.

[84] C. SCOTT, *Standard-Setting in Regulatory Regimes*, in M. CAVE, R. BALDWIN, M. LODGE (a cura di), *The Oxford Handbook on Regulation*, Oxford University Press, Oxford, 2010, 104 s.

dardizzazione tecnica[85], come a livello internazionale la *International Organization for Standardization* (ISO)[86]. Questi non agiscono come organi politici legittimati democraticamente, ma come attori privati o "ibridi" – nel senso che, seppur finanziati da soggetti pubblici, mantengono sempre una certa indipendenza da essi – la cui legittimazione al fondo deriva dalle conoscenze tecnico-scientifiche in loro possesso[87].

Oltre alle diverse tipologie di standard, distinte tra standard di prodotto o di processo[88], standard dettagliati o generali[89], appare caratterizzante anche il procedimento di formazione degli stessi, che risulta in grado di condizionare al contempo la loro qualità, in relazione alle informazioni acquisite, e la loro legittimazione, in ragione della trasparenza, l'apertura e la partecipazione al processo di adozione[90]. A differenza della *hard law*, inoltre, gli standard rimangono formalmente volontari e non pongono regole giuridicamente vincolanti[91].

[85] Cfr. A. IANNUZZI, *Il diritto capovolto*, cit, 31 ss.

[86] Sempre a livello globale è possibile ricordare la *International Electrotechnical Commission* (IEC); a livello europeo vi è lo *European Committee for Standardization* (CEN) e lo *European Committee for Electrotechnical Standardization* (CENELEC); in Italia si ricordi Ente nazionale italiano di unificazione (UNI). Su tali organismi e sulle principali coordinate normative che disciplinano la normazione (*standardisation*), tecnica e non solo, rinvenibili nel regolamento UE n. 1025/2012, basti rinviare a v. A. IANNUZZI, *Il diritto capovolto*, cit., 56 ss.

[87] F. CAFAGGI, *New foundation of transnational private regulation*, in *Journal of Law and Society*, 38, 1, 2011, 20 ss.

[88] Cfr. C. SCOTT, *Standard-Setting in Regulatory Regimes*, cit., 107 s. I primi si riferiscono a proprietà specifiche o al *design* di un prodotto, mentre i secondi si riferiscono a processi attraverso cui un prodotto viene realizzato.

[89] *Ivi*, 109 s. Gli standard dettagliati si concentrano su specifiche proprietà di un prodotto o un processo, mentre gli standard generali guardano al risultato o l'obiettivo da perseguire, senza indicare esaurientemente i mezzi necessari. La scelta tra gli uni o gli altri deve essere ponderata, poiché i primi offrono una maggior concretezza, ma rischiano di ingenerare un atteggiamento di rispetto formalistico e di elusione delle finalità complessivamente presidiate; i secondi sono invece più flessibili e consentono di adattare le misure più appropriate per raggiungere determinati obiettivi, ma rischiano di essere troppo generici e lasciare margini troppo ampi; cfr. J. BRAITHWAITE, V. BRAITHWAITE, *The Politics of Legalism: Rules versus Standards in Nursing-Home Regulation*, in *Social and Legal Studies*, 4, 1995, 311 ss.

[90] C. SCOTT, *Standard-Setting in Regulatory Regimes*, cit., 112 s.

[91] E. FOSCH VILLARONGA, A. JR GOLIA, *Robots, standards and the law: Rivalries*

Per comprendere il rilievo degli standard nel settore del riconoscimento facciale si ricordi, ad esempio, che l'accuratezza del sistema dipende molto dalla qualità delle immagini processate o dei *template* biometrici elaborati[92]. Gli algoritmi di riconoscimento facciale più diffusi, inoltre, tendono ad avere una soglia di tolleranza sulla qualità dei dati piuttosto variabile[93] e, dunque, anche a processare immagini poco rappresentative, con il rischio di generare con facilità casi di falsi-positivi o falsi-negativi[94]. Da qui l'importanza di poter misurare la qualità dei dati e delle immagini utilizzate per allenare gli algoritmi, per comporre le gallerie impiegate nel confronto, oppure di quelle acquisite dal vivo.

Allo stato non ci sono standard per le metriche sulla qualità delle immagini facciali, al pari di quanto accade per le impronte digitali[95]. Tuttavia, gli organismi di normalizzazione hanno adottato standard che si riferiscono alle migliori partiche per l'acquisizione di immagini di buona qualità, specialmente ai fini dell'inserimento nei documenti di identità[96], o alle metriche per giudicare l'accuratezza di un sistema di riconoscimento biometrico, anche facciale, per finalità di verificazione o identificazione[97]. I più importanti standard, inoltre, si riferiscono alla qualità delle biometrie facciali (come i *template* biometri-

between private standards and public policymaking for robot governance, in *Computer Law & Security Review*, 35, 2, 2019, 131.

[92] V. *retro* Cap. I, par. 2.

[93] Sebbene sul punto vi siano algoritmi in grado di valutare la qualità dell'immagine prima di processarla: cfr. NIST, *Face Recognition Vendor Test (FRVT) Part 5: Face Image Quality Assessment*, Draft NIST Interagency Report, 6 marzo 2020.

[94] P. GROTHER, M. NGAN, K. HANAOKA, *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*, cit., 17.

[95] Cfr. "ISO/IEC 29794-4:2017 Information Technology – Biometric Sample Quality – Part 4: Finger image data".

[96] Cfr. "ISO/IEC 19794-5:2011 Information technology – Biometric data interchange formats – Part 5: Face image data", con riguardo al formato dell'immagine, ma anche i vincoli da rispettare nell'acquisizione (luce, posa, espressione, capigliatura), proprietà fotografiche (posizionamento della fotocamera, focus), attributi dell'immagine digitale (risoluzione, dimensione, saturazione del colore).

[97] Cfr. "ISO/IEC 19795-1:2006 Information technology – Biometric performance testing and reporting – Part 1: Principles and framework".

ci)[98], grazie ai quali, sia gli Stati che le imprese[99], riescono a raggiungere una uniformità tale da consentire lo scambio dei dati biometrici tra differenti TRF provenienti da diversi produttori, la condivisione delle banche dati, l'implementazione della interoperabilità tra sistemi.

Gli standard tecnici finiscono così, in forza di una sorta di "effetto network"[100], per essere sempre più diffusi, e quindi di fatto vincolanti nei confronti degli Stati e delle imprese – basti considerare i costi di mercato proibitivi che occorrerebbe sopportare a seguito di un loro eventuale abbandono[101]. Sebbene adottati da soggetti autorevoli che godono di una certa indipendenza, tuttavia, gli standard aprono ad una serie di problematiche sul piano giuridico. Si pensi alla assenza di responsabilità di tali organismi o alla mancanza di controlli da parte di organi politici[102], soprattutto per standard, come quelli impiegati nel riconoscimento facciale, da cui dipendono decisioni che influiscono sui diritti fondamentali delle persone. Gli standard, inoltre, non prendono in considerazione i bisogni e le implicazioni di natura non tecni-

[98] Cfr. "ISO/IEC 39794-1:2019 Information technology – Extensible biometric data interchange formats". NIST ha invece elaborato uno standard nazionale per i dati biometrici utilizzabili a scopo di polizia, "ANSI/NIST ITL 1-2017". Maggiori informazioni in J. GALBALLY, P. FERRARA, R. HARAKSIM, A. PSYLLOS, L. BESLAY, *Study on Face Identification Technology for its Implementation in the Schengen Information System*, cit., 86 ss.

[99] In generale, osservano E. FOSCH VILLARONGA, A. JR GOLIA, *Robots, standards and the law: Rivalries between private standards and public policymaking for robot governance*, cit., 131 s., come le imprese, da parte loro, ne guadagnano sotto diversi punti di vista: in credibilità e legittimazione agli occhi dei consumatori e degli altri operatori di mercato; perché la conformità agli standard è spesso condizione per accedere a mercati specifici o protetti e per partecipare ad appalti pubblici; perché tale conformità favorisce il coordinamento, riducendo le incertezze e i costi di transazione nei vari mercati, e garantisce un maggior grado di interoperabilità tecnologica e produttiva. Ma anche gli Stati, nel rifarsi in varie forme agli standard, ottengono molteplici utilità: nel regolare fenomeni transnazionali; nel disciplinare ambiti in cui non si raggiunge il consenso politico per stipulare trattati internazionali vincolanti; nel colmare le lacune di conoscenze tecniche; nello sviluppare processi normativi più efficaci, tramite il recepimento di regole già elaborate e messe alla prova dagli operatori stessi.

[100] A proposito del "*network effect*" v. le considerazioni in G. CONTISSA, *Information technology for the law*, Giappichelli, Torino, 2017, 7 ss.

[101] F. CAFAGGI, *New foundation of transnational private regulation*, cit., 22.

[102] C. SCOTT, *Standard-Setting in Regulatory Regimes*, cit., 115 s.

ca e godono di una legittimazione limitata al circolo degli operatori economici coinvolte[103]. Non da ultimo, occorre ricordare come la conoscenza degli standard sia a pagamento.

Fino a che gli standard vengono adottati spontaneamente dalle imprese – pur con le costrizioni che, di fatto, le inducono a tale scelta – ci troviamo ancora nell'ambito della *self-regulation*. Nel momento in cui, tuttavia, gli Stati o le istituzioni sovranazionali volessero adottare una disciplina giuridica sulle TRF, non si potrà soprassedere dagli standard che, attualmente, risultano più diffusi e consolidati nella pratica e nei mercati, come quelli visti a proposito degli aspetti qualitativi delle immagini processate. Allo scopo, la normativa potrà concepire diversi meccanismi cui fare rinvio, ad esempio fissando una cornice di principi che sarà poi riempita dalle norme tecniche; formulando una disciplina cedevole nei confronti dell'adozione di standard; incorporando gli standard al suo interno[104]; quand'anche stabilisse l'adozione di nuovi standard, questi necessariamente – per le ragioni viste – dovranno rifarsi a quelli più diffusi, come già avviene ampiamente, ad esempio, nell'ambito dei servizi della società dell'informazione[105].

Si consideri quanto sta accadendo con i sopra citati regolamenti "interoperabilità"[106]. Tra i principali presupposti e condizioni per realizzare l'enorme infrastruttura digitale che dovrebbe integrare i sistemi di informazione gestiti a livello europeo, vi è la necessità di far convergere i dati biometrici e i sistemi impiegati nei singoli Stati verso standard comuni. Per questo risulterà cruciale la creazione del "formato

[103] E. FOSCH VILLARONGA, A. JR GOLIA, *Robots, standards and the law: Rivalries between private standards and public policymaking for robot governance*, cit., 139.

[104] È la distinzione tra coordinamento, delega o incorporazione, su cui *ivi*, 132 s. Una diversa casistica è proposta da A. PREDIERI, *Le norme tecniche nello Stato pluralista e prefederativo*, in *Il diritto dell'economia*, 1996, 290 s., che individua tre metodi: il primo, caratterizzato dalla partecipazione degli organismi privati nel procedimento di adozione della norma tecnica. Il secondo, che consiste nell'imputazione al soggetto statale e non di disposizioni formulate congiuntamente. Il terzo, che consiste nel riconoscimento indiretto di effetti giuridicamente vincolanti tramite la tecnica del "rinvio mobile", da giudicare più appropriata perché aperta agli sviluppi della tecnica.

[105] Sulla direttiva (UE) 2015/1535, più approfonditamente, v. A. IANNUZZI, *Il diritto capovolto*, cit., 99 ss.

[106] Cfr. *retro* Cap. IV, par. 6.

universale dei messaggi" (UMF), quale standard sul quale improntare la costruzione stessa dei nuovi sistemi informativi e permettere lo scambio di informazioni e dati biometrici tra di essi. L'agenzia eu-LISA, responsabile per la progettazione, lo sviluppo e la gestione dei sistemi, nonché per l'adozione delle misure di sicurezza, è consapevole delle enormi difficoltà pratiche da superare su questo fronte e, proprio per questo, è impegnata nello sviluppo di standard che facciano leva sulle norme tecniche attualmente più diffuse[107].

La *co-regulation*, dunque, assieme alla *self-regulation*, è stata già da tempo individuata dalle istituzioni dell'UE come una forma ulteriore alla regolazione tradizionale[108]. Tra i settori nei quali ha già conosciuto una significativa diffusione, per quanto qui interessa maggiormente[109], vi è proprio la tutela dei dati personali. Al suo interno non solo si co-

[107] Ad esempio, tra le iniziative volte a rafforzare la *cybersecurity* delle infrastrutture e dei network, eu-LISA sta promuovendo l'adozione di un quadro comune di controlli di sicurezza, a partire dagli standard "NIST 800-53" e "ISO 27002". Cfr. EU-LISA, *eu-LISA Consolidated Annual Activity Report 2019*, 2020-124 REV. 2, 30 giugno 2020. Maggiori informazioni disponibili su: [bit.ly/32dS9p6].

[108] L'accordo interistituzionale *Legiferare meglio* (2003/2131(ACI)) stabilisce definizioni, criteri e procedure comuni per la coregolamentazione e l'autoregolamentazione. Tali tecniche ulteriori di regolazione sono poi richiamate e implementate in atti normativi successivi, come la direttiva 2010/13/UE sui servizi di media audiovisivi, che al considerando 44 esorta «gli Stati membri, nel rispetto delle loro diverse tradizioni giuridiche, [a] riconoscere il ruolo che può svolgere un'efficace autoregolamentazione a complemento dei meccanismi legislativi e giudiziari e/o amministrativi in vigore [...]. Tuttavia, se l'autoregolamentazione può essere uno strumento complementare per attuare determinate disposizioni della presente direttiva, non dovrebbe sostituirsi ai compiti del legislatore nazionale». Invece «la coregolamentazione, nella sua forma minima, fornisce un collegamento giuridico tra l'autoregolamentazione e il legislatore nazionale, in conformità delle tradizioni giuridiche degli Stati membri. La coregolamentazione dovrebbe consentire l'intervento statale qualora i suoi obiettivi non siano conseguiti».

[109] Si consideri, ad esempio, che i "codici di condotta" sono al centro della disciplina del regolamento (UE) 2018/1807, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'UE, dovendo considerare le migliori prassi per agevolare il cambio di fornitore di servizi e la portabilità dei dati; gli obblighi d'informazione minimi per gli utenti professionali prima della conclusione di un contratto di trattamento di dati; gli approcci in materia di sistemi di certificazione; tabelle di marcia in materia di comunicazione (art. 6).

mincia a registrare una certa produzione di standard tecnici[110], ma soprattutto, nella disciplina attualmente in vigore[111], si valorizzano molto ulteriori strumenti di *co-regulation*, quali i "*codici di condotta*". Questi ultimi sono atti elaborati dalle associazioni rappresentative dei titolari del trattamento e approvati dalle autorità garanti, se riferiti ad un unico Stato, o estesi al territorio dell'UE dalla Commissione, se aventi portata sovranazionale[112]. Tramite questi codici è possibile concretiz-

[110] Cfr. I. KAMARA, *Co-regulation in EU personal data protection: The case of technical standards and the privacy by design standardisation 'mandate'*, in *European Journal of Law and Technology*, 8, 1, 2017.

[111] Sull'applicazione delle previsioni all'art. 27 della precedente direttiva 95/46/CE, v. D. HIRSCH, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, cit., 439 ss. Sulla prassi italiana dei "codici di deontologia e di buona condotta", a partire dall'art. 31, c. 1, lett. h, della legge n. 675/1996, invero non cospicua, v. A. SIMONCINI, *I* codici deontologici *di protezione dei dati personali nel sistema delle fonti. L'emersione di un nuovo «paradigma» normativo?*, in U. DE SIERVO (a cura di), *Osservatorio sulle fonti 1999*, Giappichelli, Torino, 2000, 277 ss., che rileva come i codici presentino una diversa struttura ed efficacia giuridica a seconda dell'intervento di "*regulation*" cui il Garante delle *privacy* è chiamato, o della disciplina giuridica sul trattamento di speciali categorie di dati personali. V. anche A.R. POPOLI, *Codici di condotta e certificazioni*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, cit., 529, che osserva come la direttiva non prescrivesse una approvazione formale del codice da parte delle autorità di controllo. Più ampiamente, cfr. S. SILEONI, *Autori delle proprie regole. I codici di condotta per il trattamento dei dati personali e il sistema delle fonti*, Cedam, Padova, 2011, 130 ss.

[112] Ai sensi dell'art. 40 del GDPR, «gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese» (par. 1). L'autorità di controllo – in Italia, il Garante della privacy – ha il compito, fra l'altro, di esprimere un parere sulla conformità del codice di condotta al GDPR e di approvare tali codici (par. 5). Una procedura più complessa è prevista nel caso il codice di condotta si riferisca alle attività di trattamento in vari Stati membri, che coinvolge il Comitato europeo per la protezione dei dati, con la possibilità per la Commissione di estenderne l'efficacia a tutto il territorio UE (parr. 7 ss.). I codici adottati fino all'entrata in vigore del GDPR sono stati sottoposti a controllo di conformità con la nuova disciplina da parte del Garante e accorpati, con la denominazione di "codici di deontologia", in allegato al d.lgs. n. 196/2003 (cfr. art. 20, d.lgs. n. 101/2018). Più ampiamente, sulle diverse tipologie di codici, anche per un confronto con la precedente direttiva, v. A.R. POPOLI, *Codici di condotta e certificazioni*, cit., 546 ss.

zare e integrare i principi e le clausole previste nella normativa generale[113], ma anche – in relazione al principio di *accountability* – consentire al titolare del trattamento di dimostrare la conformità a tale disciplina[114]. I codici di condotta devono arrecare un "sufficiente valore aggiunto"[115] rispetto alla disciplina generale, in quanto da ritagliare sulle specificità dei trattamenti nei diversi ambiti. In futuro, entro questi atti potrebbe trovare spazio anche una regolamentazione delle nuove tecnologie algoritmiche e biometriche, ad esempio, per incentivare una maggior trasparenza nei confronti degli utenti[116].

Spostandosi al di fuori del continente europeo, *mutatis mutandis*, un cenno meritano le "*Privacy Best Practice Recommendations For Commercial Facial Recognition Use*"[117], definite e pubblicate negli Stati Uniti nel giugno 2016 dall'agenzia federale *US National Telecommunications and Information Administration* (NTIA), in esito ad un proces-

[113] L'art. 40, par. 3 del GDPR indica i possibili contenuti dei codici, con una elencazione non esaustiva che comprende, fra l'altro: il trattamento corretto e trasparente dei dati; i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici; la raccolta dei dati personali; la loro pseudonimizzazione; l'informazione fornita al pubblico e agli interessati; l'esercizio dei diritti degli interessati; l'informazione e il consenso del minore; l'attuazione delle previsioni sulla responsabilità del titolare del trattamento e dei principi di *privacy by design* e *by default*.

[114] M.C. CAUSARANO, *GDPR e forme di autoregolamentazione privata: continuità e discontinuità nella disciplina dei codici di condotta*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali*, cit., 249, cui si rinvia per ulteriori considerazioni, anche in ordine ad ulteriori novità del GDPR come la previsione di organismi di controllo privati accreditati per monitorare il rispetto dei codici (art. 41).

[115] EUROPEAN DATA PROTECTION BOARD, *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, 12 febbraio 2019, 36. I codici possono esser formulati in senso stretto o ampio (12), allo scopo di stabilire un set di regole che contribuisca all'applicazione del GDPR in maniera pratica, trasparente e potenzialmente conveniente (11), che offrano soluzioni pratiche a problemi relativi al settore specifico (15).

[116] Nel settore delle nuove tecnologie che sfruttano algoritmi si cominciano ad ipotizzare nuovi meccanismi di co-regolazione; ad esempio, v. F. DI PORTO, M. ZUPPETTA, *Co-regulating algorithmic disclosure for digital platforms*, in *Policy and Society*, 2020, proprio con riguardo alle piattaforme digitali e agli oneri di trasparenza e informazione.

[117] Disponibile su: [bit.ly/3fRMq0q].

so partecipativo che ha interessato numerosi *stakeholders* e organizzazioni non governative[118], dando origine ad un intenso dibattito e a diverse prese di posizione sui pericoli e le necessarie garanzie da accordare ai cittadini[119]. Pur in un contesto regolatorio completamente diverso, prescindendo anche dall'esito di questo esperimento, si ha comunque la riprova dell'attenzione crescente nel settore verso meccanismi di co-regolazione che coinvolgano autorità pubbliche e destinatari della regolazione.

In definitiva, la *co-regulation* si pone a metà strada tra la *hard law* e la *self-regulation*, delle quali riesce a coniugare, rispettivamente, la flessibilità e il rigore[120], potendo, da una parte, garantire un intervento da parte delle autorità pubbliche e, dall'altra, non "ingessare" lo sviluppo tecnologico e far leva sulle conoscenze a disposizione degli attori privati. Di esse però ripete anche alcuni limiti, come una minore trasparenza dei processi decisionali e una minore responsabilità per le decisioni assunte, poiché, se paragonata alla regolamentazione più tradizionale, dalla negoziazione che ne nasce le imprese hanno una maggiore opportunità di imporre il proprio punto di vista e ottenere maggiori vantaggi, a discapito dell'interesse pubblico[121]. Ciò nonostante, la co-regolazione, meglio dell'auto-regolazione, può rappresentare un mezzo più idoneo a soddisfare la necessità che il diritto si riappropri degli spazi che gli spettano, nel tentativo di orientare anche la tecnica verso i valori propriamente costituzionali[122].

[118] Cfr. E. WRIGHT, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, in *Fordham Intellectual Property, Media and Entertainment Law Journal*, 29, 2, 2019, 650 s.

[119] Come è accaduto per numerose ONG che si sono ritirate dalla discussione giudicando non soddisfacente il documento prodotto, dal momento che non stabiliva espressamente la possibilità per gli interessati di sottrarsi alla raccolta delle proprie immagini facciali; cfr. J. LYNCH, *EFF and Eight Other Privacy Organizations Back Out of NTIA Face Recognition Multi-Stakeholder Process*, in *Electronic Frontier Foundation*, 16 giugno 2015 [bit.ly/3sUU6T4].

[120] D. HIRSCH, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, cit., 441.

[121] *Ivi*, 442.

[122] In N. IRTI, E. SEVERINO, *Dialogo su diritto e tecnica*, Laterza, Roma-Bari, 2001, 19, Irti rileva che la tecnica «non è in grado di rispondere alle domande del diritto: al

5. *La valenza regolativa del* design *delle TRF*

Il diritto rappresenta solamente uno degli "attrezzi" a disposizione nelle "*regulatory tool-box*" degli organi di governo. A seconda delle circostanze, questi soggetti pubblici non è detto debbano necessariamente sfruttare i propri poteri autoritativi e ricorrere alla formalità e ufficialità del diritto[123]. A questo proposito, come ha messo bene in evidenza Lawrence Lessig, in generale e con particolare riguardo alle tecnologie, vi sono quattro modalità che concorrono come una "rete" a regolare (*net regulation*) tanto lo spazio reale quanto il *cyberspazio*: la legge in senso tradizionale, le norme sociali, il mercato, e soprattutto l'architettura o il codice[124]. Con questa presa di consapevolezza, le autorità pubbliche sono invitate a ripensare il paradigma della normazione, proprio nel senso di sfruttare maggiormente la capacità del co-

triplice interrogativo del legislatore, del cittadino e del giudice. Che cosa prescrivere? Come comportarsi? In base a quale criterio decidere, cioè separare la ragione e il torto?». Osserva G. AZZARITI. *Diritto e conflitti. Lezioni di diritto costituzionale*, Laterza, Roma-Bari, 2010, 210, come sia una precipua responsabilità del giurista aver coscienza della dimensione storica del fenomeno giuridico e che «il mezzo giuridico non è buono a ogni scopo, ma solo a quelli che l'ordinamento concreto definisce tali»; il punto di partenza è offerto dalle norme costituzionali, come suggerisce l'A. e, da una prospettiva culturale e ideologica diversa, propone anche L. MENGONI, *Diritto e tecnica*, in *Rivista trim. di dir. e proc. civ.*, 2001, 7, secondo cui «l'innovazione basilare della costituzione sta nel passaggio dal punto di vista esterno al punto di vista interno, ossia nella stabilizzazione del punto di vista morale all'interno del diritto positivo come istanza di controllo di legittimità sostanziale delle leggi».

[123] Cfr. C.C. HOOD, H.Z. MARGETTS, *The Tools of Government in the Digital Age*, Palgrave Macmillan, Basingstoke, 2007, 2 ss.

[124] Cfr. L. LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, 113, 1999, 501 ss. Più specificatamente, la legge in senso tradizionale, intesa come comando assistito da sanzione, che nel *cyberspazio* disciplina copyright, diffamazione, buon costume, ecc.; le norme sociali, che pure minacciano sanzioni *ex post* ma che vengono prodotte e messe in atto dalla comunità intera, e che nel *cyberspazio* trovano applicazione, ad esempio, nelle comuni chat, dalle quali si può essere esclusi a seconda di certi comportamenti; il mercato, con la propria legge dei prezzi, che nel *cyberspazio* muove il grande mercato delle *ads*; l'architettura, o il codice, che rappresenta il modo con cui una determinata realtà si presenta e conseguentemente vincola i comportamenti "codificando" o meno certi valori.

dice per regolare le nuove tecnologie[125]. Anche nel caso delle TRF, come si vedrà, non solo non è possibile trascurare questo fattore, ma occorre soprattutto stabilire in che modo esso sia destinato ad interagire con la regolamentazione giuridica.

Il *codice* può essere inteso alla stregua di architettura o *design* di un artefatto, la cui scelta implica decisioni in grado di rendere certe condotte più difficili, più costose, o addirittura impossibili, con una cogenza affine a quella delle regole di diritto[126]. Il codice, in generale, è capace di esercitare una differente forza costrittiva in relazione a diverse tecniche regolative[127], le quali producono effetti analoghi a quelli delle norme giuridiche nella misura in cui assolvono ad una funzione promozionale, oppure riducono l'impatto degli eventi dannosi, oppure

[125] Il dibattito sul rapporto tra "*code and law*" emerge prepotentemente a livello accademico e scientifico con la diffusione di internet, spingendo autori come il già citato Lawrence Lessig, parlando di *cyberlaw* (cfr. L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999) o Joel Reidenberg, parlando di *lex informatica* (cfr. J.R. REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, in *Texas Law Review*, 76, 3, 1998, 553 ss.), a porre in luce l'inadeguatezza della legislazione tradizionale a regolare il web e ad invitare le autorità pubbliche a ripensare il paradigma della regolazione. Più ampiamente, v. anche E. MAESTRI, *Lex Informatica*, cit., 87 ss.

[126] Con ciò, questa normatività non assume solamente una rilevanza di natura etico-valoriale; cfr. V. DIGNUM ET AL., *Ethics by Design: necessity or curse?*, in *AIES 2018. Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, 2018, 60 ss.; B. LATOUR, C. VENN, *Morality and Technology: The End of the Means*, in *Theory, Culture & Society*, 19, 5-6, 2002, 247 ss.

[127] Cfr. R. LEENES, F. LUCIVERO, *Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design*, in *Law, Innovation and Technology*, 6, 2, 2014, 203 ss., che distinguono "*persuasive technologies*", "*nudging*", "*affordances*" e "*techno-regulation*". Tra le più note vi è forse il "*nudging*" o "spinta gentile", dovuta all'architettura con cui sono organizzate le scelte, attraverso la quale è possibile indirizzare le persone verso decisioni più "corrette", ad esempio, dal punto di vista morale, della salute o dell'ambiente; cfr. C.R. SUNSTEIN, R.H. THALER, *Nudge. Improving decisions about health, wealth, and happiness*, Penguin, London, 2009. Tuttavia, ai fini di un paragone con il diritto, vengono in rilievo soprattutto i fenomeni di "tecnoregolazione", nei quali le norme vengono intenzionalmente incorporate in una soluzione tecnologica e costringono o impediscono in senso stretto ad un soggetto di tenere un certo comportamento; cfr. R. LEENES, *Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology*, in *Legisprudence*, 5, 2011, 150 ss.

ancora esprimono una vera e propria funzione repressiva, che impedisce o costringe a tenere un certo comportamento[128].

Le norme giuridiche, in particolare, vengono sempre più immesse nel codice dei dispositivi tecnologici, nel tentativo di affrontare i problemi posti dall'innovazione per mezzo della tecnologia stessa[129]. Il diritto assume così rilievo non soltanto nel caso della regolazione *della* tecnologia (*regulation of technology*), ma anche con la regolazione *attraverso* la tecnologia (*regulation through technology*)[130].

Come chiarito dalla scienza informatica, il buon *design* degli algoritmi permette di assicurare che i sistemi intelligenti operino all'interno dei parametri prefissati e forniscano i risultati attesi[131]. Nel caso del riconoscimento facciale, vi sono diverse variabili che vengono in gioco nel *design* dell'algoritmo e, di conseguenza, nell'incidenza su principi giuridici e diritti fondamentali[132]: la scelta in sé del tipo di algoritmo, ovvero tra i più risalenti algoritmi incapaci di autoapprendere o algoritmi di *machine learning*; la costruzione del *dataset* con cui allenare l'algoritmo di *machine learning*; la scelta del peso da accordare alle variabili all'interno del processo decisionale; le impostazioni riguardanti le soglie di sensibilità da cui dipendono le percentuali di falsi-positivi o falsi-negativi (c.d. *benchmark*); il tipo di test svolti durante lo sviluppo degli algoritmi per verificarne le prestazioni nella risoluzione di problemi specifici e non altri[133].

[128] Cfr. U. PAGALLO, *Il diritto nell'età dell'informazione*, Giappichelli, Torino, 2014, 136, ove si riporta come esempio della prima funzione i dossi stradali, della seconda gli air-bag, della terza i sistemi di frenata automatica delle macchine di ultima generazione.

[129] *Ivi*, 4.

[130] Cfr. R. BROWNSWORD, K. YEUNG (a cura di), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Hart Publishing, Oxford, 2008, i quali distinguono "*Technology as a Regulatory Target*" da "*Technology as a Regulatory Tool*".

[131] J.J. BRYSON, A. THEODOROU, *How Society Can Maintain Human-Centric Artificial Intelligence*, in M. TOIVONEN, E. SAARI (a cura di), *Human-Centered Digitalization and Services*, Springer, 2019, 310. Giudizio ripreso anche in F. DE VANNA, *Diritto e nuove tecnologie: il nodo (controverso) della regolazione giuridica*, in *Lo Stato*, 11, 2018, 395.

[132] U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, cit., 32; D. LESLIE, *Understanding bias in facial recognition technologies: an explainer*, cit., 17.

[133] Per una definizione più ampia, v. E. LEARNED-MILLER, V. ORDÓÑEZ, J. MOR-

Il regolatore politico non si dimostra inconsapevole della valenza "normativa" che il codice può esercitare in relazione a ciascuno di questi fattori e delle finalità che così possono essere perseguite. Basti ricordare che anche la legislazione sulla protezione dei dati personali contiene specifiche previsioni sul punto, che si declinano nel principio del "*data protection by design*"[134]. Tale principio sta ad indicare un approccio che orienta l'intero ciclo di attività di un sistema tecnologico – ricerca, progettazione, sviluppo, implementazione e utilizzo pratico – attraverso l'integrazione della tutela dei dati nel *design* dello stesso[135].

GENSTERN, J. BUOLAMWINI, *Facial Recognition Technologies in the Wild: A Call for a Federal Office*, cit., 41.

[134] Cfr. art 25, par. 1 del GDPR; art. 20, par. 1 della LED, secondo cui occorre «mette[re] in atto misure tecniche e organizzative adeguate [...] volte ad attuare in modo efficace i principi di protezione dei dati [...] e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti [normativi] e tutelare i diritti degli interessati», «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso». V. anche art. 10, par. 3, della Convenzione 108+.

[135] Cfr. L. MITROU, *Data Protection, Artificial Intelligence and Cognitive Services. Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?*, cit., 75. Per la strutturazione di una metodologia divisa in fasi per la realizzazione di un sistema *privacy-by-design-based*, cfr. D. WIESE SCHARTUM, *Making privacy by design operative*, in *International Journal of Law and Information Technology*, 24, 2, 2016, 151 ss. V. anche I. RUBINSTEIN, N. GOOD, *Privacy by Design: a Counterfactual Analysis of Google and Facebook Privacy Incidents*, in *Berkeley Technology Law Journal*, 28, 2, 2013, 1333 ss., per una disamina di tali criteri utilizzati dal punto di vista di "*privacy engineering*", ovvero delle soluzioni di ingegneria informatica finalizzate a garantire la *privacy by design*, e dello "*usable privacy design*", ovvero il *design* che guarda alla "*user experience*" per implementare la *privacy by design*. V. anche S. CALZOLAIO, *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *Federalismi.it*, 24, 2017, spec. 15 ss., per alcune critiche all'impostazione del GDPR, che carica eccessivamente il titolare del trattamento di responsabilità che in realtà dovrebbero essere in capo a coloro che hanno progettato il sistema. Ad ispirare la formalizzazione di tale principio è stato anche il contributo di Ann Cavoukian, che ha specificato il principio di "*Privacy By Design*" in altri sette principi costitutivi: 1. *Proactive not Reactive*; *Preventative not Remedial*; 2. *Privacy as the Default Setting*; 3. *Privacy Embedded into Design*; 4. *Full Functionality – Positive-Sum, not Zero-Sum*; 5. *End-to-End Security – Full*

Calato sulle TRF, il principio di protezione dei dati "*by design*" consiste nello sfruttare il *design* di un sistema per inverare i principi e i diritti sopra ricostruiti a tutela dei dati personali e nei loro riflessi su altri diritti fondamentali. Anche qui, l'ottica è quella di anticipare la protezione ad un momento anteriore al verificarsi di una potenziale lesione.

Così accade a partire dal principio di minimizzazione dei dati, nella scelta sulla quantità e la qualità dei dati impiegati dagli algoritmi di riconoscimento facciale per costruire i *template* biometrici o le gallerie di immagini necessarie per il confronto[136].

Nell'implementare il regime di conservazione dei dati e di sicurezza degli stessi[137], poi, fin dalla fase di progettazione è possibile strutturare un sistema di riconoscimento facciale in modo che disponga la cancellazione automatica dei dati grezzi subito dopo la costruzione del modello biometrico, o che effettui tale cancellazione entro un determinato periodo di tempo; è possibile conservare i dati biometrici in forma pseudonimizzata o criptata; è altresì possibile decidere se la conservazione debba avvenire attraverso *database* gestiti in forma centralizzata o decentrandone la disponibilità attraverso dispositivi portatili.

Nella prestazione del consenso esplicito – lo si ricorda[138] – il *design* di un ambiente fisico può favorirne la bontà sfruttando, ad esempio, dispositivi di rilevamento facciale attivabili volontariamente dall'interessato, o la disponibilità di corsie di accesso ad uno spazio sottratte a questi tipi di controllo. Analogamente, l'architettura di uno spazio reale o di un ambiente virtuale è in grado di agevolare o meno la consapevolezza circa la sottoposizione a riconoscimento facciale e l'esercizio dei diritti accordati all'interessato[139].

Lifecycle Protection; 6. *Visibility and Transparency – Keep it Open*; 7. *Respect for User Privacy – Keep it User-Centric*; cfr. A. CAVOUKIAN, *Privacy By Design: The 7 Foundational Principles*, 2011.

Diverso, ma strettamente correlato, è il principio di "*privacy by default*", secondo cui occorre «mette[re] in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento» (cfr. art 25, par. 2 del GDPR; art. 20, par. 2 della LED).

[136] V. *retro* cap. III, par. 5.2.

[137] V. *retro* cap. III, par. 5.3.

[138] V. *retro* cap. III, par. 4.1.

[139] V. *retro* cap. III, par. 6.1.

Si pensi poi alla scelta del se e come strutturare un sistema di riconoscimento facciale che produca autonomamente una decisione che si ripercuote sull'interessato oppure, viceversa, offra un risultato che necessiti della convalida di un essere umano[140].

Inoltre, non basta sancire a livello di norme scritte un principio come quello di comprensibilità se poi i sistemi tecnologici vengono concepiti e progettati con una struttura simbolica del tutto incomprensibile per l'uomo, fosse anche un tecnico informatico[141]. Già al momento della scrittura del codice, quindi, occorre avere a mente che sarà il linguaggio utilizzato a garantire l'effettività di simile principio giuridico; parimenti, bisogna considerare quali test e tecniche di audit si rendano necessarie per avere un riscontro e dar conto degli effetti di una decisione sull'interessato.

La rilevanza del "codice", inoltre, emerge in tutte le sue conseguenze allorché si tratta di evitare quei pregiudizi (*bias*) in cui è possibile incorrere in ogni fase di costruzione del sistema. Rinviando a quanto già detto sopra[142], basti solo osservare qui come alcuni studi abbiano descritto quello che nella letteratura specialistica viene chiamato "*The Other Race Effect*", per il quale gli esseri umani, e di conseguenza anche gli algoritmi, riescono meglio ad identificare individui appartenenti alla propria etnia a motivo di un maggior contatto e frequentazione. Diversi test su TRF, ad esempio, hanno dimostrato come gli algoritmi elaborati da programmatori asiatici siano più performanti nell'identificare persone di origine asiatica[143]. Da qui l'ipotesi di integrare i team di sviluppatori con esperti provenienti da diverse aree geografiche, o comunque per garantire un pluralismo che, ci si aspetta, possa mitigare gli effetti discriminatori del riconoscimento.

Infine, vale la pena richiamare ancora una volta la valenza politica e gli effetti sulla tutela dei diritti fondamentali che porta con sé la scelta complessiva di strutturare i sistemi di informazione europei raffor-

[140] V. *retro* cap. III, par. 6.3.

[141] V. *retro* cap. III, par. 6.5

[142] V. *retro* cap. III, par. 7.

[143] P.J. PHILLIPS, F. JIANG, A. NARVEKAR, J. AYYAD, A.J. O'TOOLE. *An Other-Race Effect for Face Recognition Algorithms*, in *ACM Transactions on Applied Perception*, 14, febbraio 2011.

zando l'interoperabilità degli stessi. In relazione a profili più specifici, si pensi anche alla scelta – ad esempio – sulle modalità concrete con cui si prevede vengano interrogati tali sistemi da un operatore, nell'alternativa tra la possibilità di rivolgersi direttamente a questi ultimi o l'obbligo di effettuare prima ricerche su altre banche dati secondo la descritta logica "a cascata"[144].

Quanto appena visto sulle TRF conferma come tra "*code and law*" si instauri un rapporto di mutua interazione[145], nel senso che la legge può vincolare il codice, imponendo determinati canoni o valori lungo tutto il procedimento di decisione algoritmica, come avviene secondo la logica del principio di "*technological due process*"[146]; ma, parallelamente, il codice può vincolare la legge, influendo sulla sua attuazione ed effettività, come accade in forza del principio di "*legal by design*"[147].

[144] V. *retro* Cap. IV, par. 6.

[145] L. LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, cit., 521 ss.

[146] Tale principio si riferisce a meccanismi in grado di garantire che gli algoritmi decisionali rispondano a certi standard e siano sottoposti a determinate procedure di revisione per assicurare la loro correttezza e accuratezza, finanche imposta dalla legge; cfr. D.K. CITRON, *Tecnological Due Process*, in *Washington University Law Rev*, 85, 2008, 1249 ss.; ma anche D.K. CITRON, F. PASQUALE, *The Scored Society: Due Process for Automated Predictions*, cit., 20 ss. Così, ad esempio, nelle ipotesi di decisioni che assegnano un punteggio (*score*) ad una persona, occorre garantire differenti diritti a seconda delle differenti fasi del processo decisionale: nella raccolta dei dati utilizzati per classificare le persone, occorrerebbe garantire loro il diritto di accedere, correggere e contestare i dati, o di conoscere la fonte dei dati; nella fase di calcolo dei punteggi, occorrerebbe che il processo di calcolo fosse controllabile; nella fase di diffusione dei dati classificanti, occorrerebbe che gli interessati fossero avvertiti di tale diffusione; nella fase di utilizzo dei punteggi per assumere altre decisioni, occorrerebbe che queste ultime fossero soggette ad un regime di licenza o di audit per essere verificabili e contestabili, soprattutto quando ricadono in ambiti sensibili come lavoro, salute, assicurazioni.

[147] Principio da intendersi come riferito al ricorso a soluzioni tecnologiche da parte dei giuristi allo scopo, ad esempio, di organizzare i procedimenti di elaborazione delle informazioni o adottare atti giuridici, in modo da favorire e rafforzare l'attuazione della legge scritta; cfr. P. LIPPE, D.M. KATZ, D. JACKSON, *Legal by Design: A New Paradigm for Handling Complexity in Banking Regulation and Elsewhere in Law*, in *Oregon Law Review*, 93, 4, 2015, 833 ss., a proposito di un sistema informatico ideato dalla IBM che può essere sfruttato per risolvere problemi legali complessi come l'attività di "*resolution and recovery planning*" (RRP) da parte delle istituzioni bancarie.

Per esplicitare tutta la valenza regolativa del codice e la capacità di influire su un ventaglio indeterminato di diritti fondamentali, allora, si potrebbe fare riferimento alla più ampia nozione di "*Legal Protection by Design*"[148], la quale esige che le norme giuridiche, espresse nel linguaggio naturale e forti di una legittimazione democratica e sociale, siano trasfuse nei requisiti e negli elementi tecnologici che strutturano l'ambiente, ad un tempo fisico e digitale, entro cui siamo più ampiamente immersi[149]. Questa condizione è fondamentale per garantire giustificazione e consentire di nutrire ragionevolmente fiducia nei processi decisionali basati su algoritmi[150].

Sfruttare in questi termini il *design* di un sistema algoritmico porta con sé vantaggi anche sulla scorta di una impostazione alla regolazione basata sul rischio e tesa ad anticipare la tutela in un'ottica non puramente rimediale. La forza regolativa del codice, infatti, è in grado, potenzialmente, di favorire la tutela dei diritti proprio laddove i principi di trasparenza degli algoritmi e e di "comprensibilità" non si dimostrano sufficienti allo scopo[151]. Gli strumenti a disposizione nella fase di costruzione di un sistema computazionale possono essere molto più incisivi e responsabilizzanti di obblighi, come quelli che derivano da tali principi, da imporre su di un sistema già esistente[152]. Il *design* re-

[148] Cfr. M. HILDEBRANDT, *Saved by Design? The Case of Legal Protection by Design*, in *Nanoethics*, 11, 2017, 307 ss.; EAD., *Legal Protection by Design: Objections and Refutations*, in *Legisprudence*, 5, 2, 2011, 223 ss. Il concetto nasce a partire dalla elaborazione di altri concetti come "*Ambient Intelligence*" e "*Ambient Law*", sviluppati in EAD., *A Vision of Ambient Law*, in R. BROWNSWORD, K. YEUNG (a cura di), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, cit., 175 ss., per descrivere questo "*digitally enhanced environment*" e la legge, o meglio l'architettura tecnologica, che lo regola. Analogie sono presenti con il concetto di "*human rights by-design approach*", su cui cfr. CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on Artificial Intelligence and Data Protection*, T-PD(2017)01, 25 gennaio 2019, p. 3.

[149] Il riferimento va al già citato concetto di "infosfera" usato da L. FLORIDI, *La quarta rivoluzione*, cit., 55 ss.

[150] Cfr. T. SCANTAMBURLO, A. CHARLESWORTH, N. CRISTIANINI, *Machine Decisions and Human Consequences*, cit., 51.

[151] Come ad esempio L. EDWARDS, M. VEALE, *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You are Looking for*, cit., 18 ss.

[152] J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YU, *Accountable Algorithms*, cit., 637.

sponsabile, infatti, può essere molto più efficace di altri rimedi a disposizione una volta che una discriminazione o la lesione di un diritto fondamentale è stata perpetrata. Gli interventi *ex post* in alcuni casi consentono di rivelare l'esistenza di un problema, ad esempio, relativo alla qualità dei dati, ma possono non essere in grado di individuare specificamente il problema e condurre ad una rettifica dei dati[153].

Tuttavia, questa prospettiva non può affatto indurre a considerare il codice come fungibile rispetto alla legge.

Si pensi, per rimanere sul principio di protezione dei dati "*by design*", all'ampiezza delle previsioni normative che così si dovrebbero presidiare, in quanto prive di un significato specifico e univoco, e alla impossibilità che tramite l'architettura di un sistema di riconoscimento facciale si riesca a coglierne tutte le sfumature e implicazioni giuridiche[154].

Ma, da un punto di vista più generale, si pensi anche alla differenza tra i procedimenti di produzione normativa e di definizione del codice. Mentre negli ordinamenti liberal-democratici contemporanei l'attività di produzione normativa segue determinati regimi, viceversa le scelte legate al codice non offrono affatto le medesime garanzie, a partire dalla legittimazione del soggetto che decide quali valori incorporare nel codice o di come assumere tali decisioni[155]. Da qui gli inevitabili interrogativi sull'impatto in termini democratici e di valori costituzionali di tale forma di regolazione[156].

Altro nodo è legato alla libertà individuale. Di fronte al codice, che opera quasi come una sorta di "inconscio tecnologico"[157], le persone

[153] A.D. SELBST, *Disparate Impact in Big Data Policing*, in *Georgia Law Review*, 52, 1, 2017, 163.

[154] Cfr. B.-J. KOOPS, R. LEENES, *Privacy Regulation Cannot be Hardcoded. A Critical Comment on the "Privacy By Design" Provision in Data-Protection Law*, in *International Review of Law, Computers & Technology*, 28, 2, 2014, 159 ss.

[155] Cfr. R. CALO, *Code, Nudge, or Notice?*, in *Iowa Law Review*, 99, 2014, 781.

[156] B.-J. KOOPS, *Criteria for Normative Technology: The Acceptability of 'Code as law' in Light of Democratic and Constitutional Values*, in R. BROWNSWORD, K. YEUNG (a cura di), *Regulating Technologies*, cit., 157 ss., cui si rinvia anche per la elaborazione di una serie di criteri per valutare l'accettabilità e la sostenibilità della capacità regolativa della tecnologia.

[157] Espressione richiamata da C. ACCOTO, *Il mondo dato*, cit., 11.

possono trovarsi nelle condizioni di non poter esercitare alcuna resistenza o disobbedienza[158]. Da questo punto di vista la legge è molto più flessibile, perché è aperta ad una pluralità di interpretazioni e significati a seconda, ad esempio, di colui che la interpreta o del contesto in cui viene interpretata; al limite è possibile anche trasgredirla, decidendo di andare incontro alle conseguenze sanzionatorie. Davanti al codice, invece, le persone possono non avere alternative tra l'adeguarsi o meno ad un certo comportamento[159].

Non è possibile ritenere, dunque, che la regolamentazione giuridica tradizionale debba essere soppiantata al punto da sancire la "fine della legge"[160]. È tuttavia necessario, da una parte, prendere atto che principi e regole tradizionalmente a presidio dei diritti fondamentali, come consenso informato, libertà di informazione, correttezza o certezza legale, non possono essere più garantite solamente dalle norme giuridiche. Occorre però, dall'altra, che queste ultime riguadagnino il proprio ruolo nella costruzione dell'ordine sociale, definendo i valori da integrare nel "codice" e guidando le scelte dei tecnici informatici[161].

Non è ammissibile che i principi e i valori instillati nel *design* di una macchina siano definiti solamente da tecnici o operatori economici, e neppure che vengano formulati senza piena consapevolezza; occorre invece strutturare processi che garantiscano un sufficiente livello di trasparenza e democraticità per legittimare la norma integrata nel

[158] Cfr. R. CALO, *Code, Nudge, or Notice?*, cit., 782.

[159] Specie se il contesto informazionale viene potentemente condizionato dalle nuove tecnologie di *big data analytics*; in questo senso K. YEUNG, *'Hypernudge': Big Data as a mode of regulation by design*, in *Information, Communication & Society*, 20, 1, 2017, 118 ss. V. anche B.-J. KOOPS, *The (In)flexibility of Techno-Regulation and the Case of Purpose-Binding*, in *Legisprudence*, 5, 2012, 171.

[160] Sottolinea questo rischio M. HILDEBRANDT, *Smart technologies and the End(s) of Law. Novel Entanglements of Law and Technology*, Edward Elgar, Cheltenham, 2015, spec. 181 ss., sul presupposto che nell'*onlife world*, ove la norma legale viene incorporata nel *design*, nel codice o in un determinato ambiente, il paradigma legale sia posto in crisi a causa di una serie di fattori, come l'assenza di un mezzo scritto in cui la legge viene esternalizzata; la riduzione degli spazi interpretativi; il venir meno del riferimento offerto dai confini statuali; la fine del monopolio dei giuristi sul diritto; la pretermissione del principio di separazione dei poteri.

[161] EAD, *Saved by Design? The Case of Legal Protection by Design*, cit., 309.

sistema stesso[162], al pari di quanto avviene per le norme giuridiche tradizionali[163]; il rischio, altrimenti, è di abbandonarsi alla *self-regulation* dei *Big Tech*[164]. Ma emerge anche come la figura più adeguata a muoversi entro questi spazi regolativi non sia quella del giurista o del tecnologo puro, bensì di coloro che sono in grado di maneggiare le conoscenze giuridiche con la consapevolezza della complessità tecnologica[165].

6. *La maggior flessibilità normativa richiesta dalle TRF*

6.1. *Regolare le TRF tramite sperimentazioni normative*

Prima che in Europa il tema delle TRF cominciasse ad acquisire una certa eco, queste tecnologie sono state oggetto di un interessante esperimento condotto da alcune autorità pubbliche tedesche, tra il

[162] Con riguardo al principio di *privacy by design*, v. D. WIESE SCHARTUM, *Making privacy by design operative*, cit., 161 ss., che sottolinea la necessità di «*bridging law and technology*».

[163] Sull'istituto della riserva di legge e il principio di legalità, v. *infra* par. 7.

[164] M. HILDEBRANDT, *Legal Protection by Design: Objections and Refutations*, cit., 242.

[165] Di tutela "*by education*" parlano A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, cit., 103, a proposito della necessità di intervenire quando scienziati e tecnologi sono ancora in formazione per spiegare il valore di principi quale la "*privacy by design*" oppure il principio della "comprensibilità" degli algoritmi predittivi. V. anche le considerazioni in J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YU, *Accountable Algorithms*, cit., 695 ss., ove si sottolinea l'impellenza di una collaborazione tra *computer scientists*, *lawmakers* e *policymakers*, in virtù della quale i primi dovrebbero concepire modelli algoritmici che incorporino determinati valori (*by design*) e adatti ad essere sottoposti a verifiche *ex post*; i secondi e i terzi devono offrire categorie (giuridiche) chiare e in grado di guidare i primi, anche attraverso l'indicazione di standard, con la consapevolezza delle opportunità tecnologiche che vengono offerte, ma anche della loro complessità e specificità. Sul versante degli esperti di questioni tecnologiche, gli ingegneri sono chiamati a sviluppare, accanto ai requisiti funzionali legati alla funzionalità dell'artefatto, un *design* che risponda anche a requisiti non funzionali, richiesti da sistema socio-tecnico, entro cui rientrano anche le regole giuridiche.

2017 e il 2018, presso la stazione ferroviaria Südkreuz di Berlino[166]. L'obiettivo di questa iniziativa era accertare le *performance* tecniche di tre differenti sistemi di riconoscimento facciale impiegati dal vivo a fini identificativi, sul presupposto che sarebbe stato impossibile per un operatore umano analizzare il materiale video raccolto dalle telecamere a circuito chiuso per individuare singoli individui ripresi. La sperimentazione coinvolgeva solamente soggetti volontari, che venivano invitati ad attraversare una certa zona della stazione ferroviaria. Una parte di essi era stata precedentemente fotografata, allo scopo di impiegare le relative immagini per popolare la galleria utilizzata ai fini del riconoscimento e verificare la capacità dei software di identificarli tra la folla. Al termine della sperimentazione, le forze di polizia hanno pubblicato un report sui risultati, dal quale si evince come il riconoscimento fosse realmente efficace solamente impiegando contemporaneamente tutti e tre i sistemi[167]. Al di là delle preoccupazioni e delle polemiche scaturite da questa iniziativa[168], il test si è limitato a valutare il rendimento tecnico di questi strumenti, chiarendo come spettasse agli organi politici dettare una disciplina sul riconoscimento facciale, ovvero stabilire i presupposti e i casi in cui impiegare questa tecnologia o, ad esempio, i criteri con cui popolare le gallerie.

Questa vicenda è significativa di come le autorità pubbliche, chiamate a regolare nuove tecnologie come quelle di riconoscimento facciale, necessitino allo scopo di verificare in concreto quale sia il funzionamento di queste ultime in scenari "reali" e quale sia l'impatto prodotto sui cittadini. A questo proposito, la già richiamata strategia di "*Better Regulation*"[169] messa in atto dalla Commissione europea e la prassi a livello globale dimostrano come sia possibile attingere ad uno strumentario regolativo variegato dal quale il legislatore potrebbe trarre spunto, venendo così incontro alle esigenze di flessibilità che queste nuove tecnologie richiedono all'universo giuridico.

[166] FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., 12.

[167] POLIZEIPRÄSIDIUM POTSDAM, *Biometrische Gesichtserkennung*, 18 settembre 2018 [bit.ly/3dK2LRP].

[168] Cfr. J. DELCKER, *Big Brother in Berlin*, in *Politico*, 13 settembre 2018.

[169] Cfr. *Tool #21. Research & Innovation*, giugno 2017 [bit.ly/31Sm1av].

Tra gli strumenti più ricorrenti e diffusi in questo senso vi sono i regimi regolatori speciali e temporanei basati sulla collaborazione tra regolatore e soggetti regolati. È il caso delle c.d. "*regulatory sandboxes*", ovvero ambienti delimitati e protetti entro cui imprese o soggetti pubblici possono sperimentare per un determinato periodo di tempo servizi o prodotti innovativi da porre sul mercato, senza però essere obbligati a soddisfare puntualmente ogni previsione normativa vigente, ma sottoponendosi volontariamente ad un più stretto monitoraggio da parte del regolatore. In questo modo è possibile verificare in un ambiente reale il rendimento di un servizio o l'impatto di un prodotto, mentre il regolatore può meglio stabilire quali sono gli interessi da tutelare, le barriere e i costi della regolazione da abbattere, le misure tecniche e organizzative da imporre[170].

Le sperimentazioni più significative si registrano nell'ambito della tecno-finanza (*FinTech*). A livello europeo, si possono ricordare quelle portate avanti dall'autorità inglese dei mercati finanziari (*Financial Conduct Authority* – FCA)[171], mentre più recentemente in Italia sono state previste dal d.l. n. 34/2019, sotto la guida e con la collaborazione delle autorità di vigilanza preposte nel settore[172].

[170] Paventate già in EUROPEAN COMMISSION, Communication "*Artificial Intelligence for Europe*", cit., come strumento da mettere in campo dopo il 2020.

[171] M.D. FENWICK, W.A. KAAL, E.P.M. VERMEULEN, *Regulation Tomorrow: What Happens When Technology is Faster Than the Law?*, in *American University Business Law Review*, 6, 3, 2017, 591 ss. Le *sandboxes* sono state concepite dalla FCA per consentire alle imprese di testare prodotti finanziari in un ambiente controllato, con minori costi regolatori e una assistenza diretta da parte del regolatore, fermi restando specifici livelli di protezione dei consumatori. Le *sandboxes* sono condotte su piccola scala, consentendo alle imprese di sperimentare i loro prodotti innovativi per un periodo limitato con un numero ristretto di clienti. Durante i test le imprese possono essere dotate di appositi strumenti (*sandbox tools*) messi a disposizione dal regolatore. Cfr. anche F. SARPI, *La regolazione di domani. Come adeguare il processo normativo alle sfide dell'innovazione*, cit., 450 s. Per maggiori informazioni sulle *regulatory sandboxes* testate da altre autorità, come la "*Australian Securities and Investment Commission*" (ASIC), la "*Singapore's Monetary Authority*" (MAS) e la "*Abu Dhabi's Financial Services Regulatory Authority*" (FSRA), v. P. DWYER, *Regulatory Sandboxes: 'Safe Spaces' for Start–Ups*, in *FinTech Business*, 27 giugno 2016 [bit.ly/3dMAREO].

[172] In base all'art. 36, c. 2-*bis*, del d.l. 30 aprile 2019, n. 34 (c.d. Decreto Crescita), introdotto dalla legge di conversione 28 giugno 2019, n. 58, si prevede che «al fine di

Per quanto riguarda più da vicino le TRF[173], merita ricordare l'iniziativa lanciata nel 2019 dall'*Information Commissioner's Office* (ICO) del Regno Unito, come supporto offerto a progetti specifici presentati da soggetti che vogliano verificare in anticipo e mitigare i rischi del relativo impatto sulla protezione dei dati personali[174]. Tra questi progetti si ricorda quello portato avanti dalla Heathrow Airport Ltd., inteso ad implementare un servizio di verificazione tramite riconoscimento facciale che, a partire dal *template* contenuto nei passaporti biometrici, permetta poi ai viaggiatori di superare i controlli interni più rapidamente e con maggiore sicurezza[175].

promuovere e sostenere l'imprenditoria, di stimolare la competizione nel mercato e di assicurare la protezione adeguata dei consumatori, degli investitori e del mercato dei capitali, nonché di favorire il raccordo tra le istituzioni, le autorità e gli operatori del settore», il Ministro dell'economia e delle finanze, sentiti la Banca d'Italia, la Commissione nazionale per le società e la borsa (CONSOB) e l'Istituto per la vigilanza sulle assicurazioni (IVASS), avrebbe dovuto adottare uno o più regolamenti «per definire le condizioni e le modalità di svolgimento di una sperimentazione relativa alle attività di tecno-finanza (Fin.Tech) volte al perseguimento, mediante nuove tecnologie quali l'intelligenza artificiale e i registri distribuiti, dell'innovazione di servizi e di prodotti nei settori finanziario, creditizio, assicurativo e dei mercati regolamentati». Tale sperimentazione, in base al c. 2-*ter*, è caratterizzata da: a) una durata massima di diciotto mesi; b) requisiti patrimoniali ridotti; c) adempimenti semplificati e proporzionati alle attività che si intende svolgere; d) tempi ridotti delle procedure autorizzative; e) definizione di perimetri di operatività. Secondo il c. 2-*sexies*, ciascuna delle autorità indipendenti citate, «nell'ambito delle materie di propria competenza, anche in raccordo con le altre autorità, ha facoltà di adottare iniziative per la sperimentazione delle attività» sopra citate. Cfr. N. MACCABIANI, *An empirical approach to the Rule of Law: the case of Regulatory Sandboxes*, in *Osservatorio sulle fonti*, 2, 2020, 742 ss.

[173] Sull'esperienza brasiliana, cfr. T.G. MORAES, E.C. ALMEIDA, J.R.L. DE PEREIRA, *Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-)public spaces*, in *AI Ethics*, 2020, 11.

[174] Maggiori informazioni disponibili su: [bit.ly/3fVmGjx].

[175] Il progetto ha avuto corso dal luglio 2019 al marzo 2020. Tra i profili problematici vi era la necessità di trovare un sufficiente fondamento giuridico al trattamento dei dati biometrici. Accertata l'insufficienza della base giuridica costituita dalla necessità di adempiere ad un obbligo legale ai sensi dell'art. 6, par. 1, lett. c, del GDPR, ovvero l'obbligo di effettuare i controlli di frontiera, l'ICO ha sollecitato la necessità che gli interessati esprimessero un consenso esplicito al trattamento in base all'art. 9 del GDPR. Durante il programma, la proposta dell'organizzatore di raccogliere tale consenso tramite comunicazione dei controlli in atto e conseguente comportamento af-

Fuori dall'Europa, invece, tra gli istituti che richiamano più da vicino le *sandboxes* vi sono le c.d. zone "*Tokku*", diffuse in Giappone da oltre un quindicennio, ovvero aree ampiamente deregolate in cui sperimentare interazioni tra robot ed esseri umani per verificare non solo le opportunità, i problemi e i rischi derivanti dalla reciproca interazione, ma anche per disporre di informazioni su quali soluzioni tecnologiche implementare e quali questioni giuridiche possono insorgere[176].

Negli Stati Uniti, invece, merita menzionare i c.d. *Safe harbor*, quale regime di co-regolazione in cui il soggetto privato coinvolto è sollecitato ad impegnarsi in un programma di "*safe harbor*", ovvero ad adottare delle "linee guida" che vengono approvate dalla *Federal Trade Commission* al soddisfacimento di determinate condizioni[177]; in caso di approvazione, scatta una presunzione di rispetto della disciplina legislativa da parte del soggetto in questione, il quale si trova così in una sorta di "porto sicuro" – secondo la traduzione letterale del termine –

fermativo non è stata giudicata sufficiente in questo senso e conforme alla normativa vigente; cfr. ICO, *Regulatory Sandbox Final Report: Heathrow Airport Ltd.*, giugno 2020, 6.

[176] Riporta U. PAGALLO, *Intelligenza Artificiale e diritto. Linee guida per un oculato intervento normativo*, cit., 630 ss., come le questioni giuridiche testate nei *Tokku* hanno riguardato le leggi del codice stradale (a Fukuoka, nel 2003); la disciplina sulle trasmissioni radio (a Kansai, nel 2005); la tutela della privacy (a Kyoto, nel 2008); le misure di sicurezza e il sistema impositivo (a Tsukuba, nel 2011); fino alla normativa per la circolazione nelle autostrade (a Sagami, nel 2013). Cfr. anche E. STRADELLA, *La regolazione della Robotica e dell'Intelligenza artificiale: il dibattito, le proposte, le prospettive. Alcuni spunti di riflessione*, cit., 88 ss.; Y.-H. WENG, Y. SUGAHARA, K. HASHIMOTO, A. TAKANISHI, *Intersection of "Tokku" Special Zone, Robots, and the Law: A Case Study on Legal Impacts to Humanoid Robots*, in *International Journal of Social Robotics*, 7, 5, 2015, 841 ss.

[177] Introdotto dal Congresso con il *Children's Online Privacy Protection Act* del 1998, il programma "*safe harbor*" viene approvato a patto che esso rispetti almeno i cinque requisiti posti dalla legge, ovvero: che il gestore di un sito internet che possa avere frequentatori minorenni fornisca informazioni sul trattamento dei dati; il consenso dei genitori prima del trattamento dei dati; il diritto dei genitori di controllare tali dati; il rispetto del canone di proporzionalità; l'adozione di misure di sicurezza. Si richiede inoltre che sia disposto un meccanismo effettivo e indipendente di valutazione del rispetto delle linee guida, e l'indicazione di "incentivi effettivi" per assicurare il rispetto di tali linee guida.

sollevato dai controlli dell'autorità pubblica[178]. In assenza – lo si ricorda – di una legislazione generale a protezione dei dati personali, questi meccanismi sono diretti ad incentivare l'adozione di misure a garanzia dei dati e delle persone al di là di quelle stabilite dalla normativa in questione[179].

Queste forme di sperimentazione normativa entro zone deregolate presentano, più in generale, diversi vantaggi: sono utili per raccogliere dati e informazioni prodromiche all'assunzione di decisioni razionali relative a nuove tecnologie emergenti; accrescono la comprensione dei sistemi tecnologici e di come essi interagiscono nei più diversi contesti; permettono di identificare i rischi derivanti dalla mancanza di controllo e di regolazione; consentono di valutare con maggior cognizione i vincoli e i costi giuridici imposti a operatori economici e sviluppatori scientifici. Tra i limiti, invece, non bisogna trascurare la necessità di strutturare sistemi di controllo efficienti, oppure di predisporre incentivi effettivi alla condivisione delle informazioni, necessari per sviluppare una regolazione adeguata[180].

6.2. *TRF e* soft-regulation

Queste ipotesi regolative, che rappresentano solamente alcuni esempi, possono essere inserite in una cornice teorica che la dottrina, già da decenni, ha descritto offrendo alcune coordinate significative. Tra queste vi è il passaggio dal "*government*" alla "*governance*"[181], da

[178] Cfr. I.S. RUBINSTEIN, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, in *I/S: A Journal of Law and Policy for the Information Society*, 6, 3, 2011, 394 ss., anche per alcuni dati sulla diffusione di questi programmi.

[179] E. WRIGHT, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, cit., 683 s.

[180] Cfr. U. PAGALLO, *LegalAIze: Tackling the Normative Challenges of Artificial Intelligence and Robotics Through the Secondary Rules of Law*, in M. CORRALES, M. FENWICK, N. FORGÓ (a cura di.), *New Technology, Big Data and the Law*, Springer, Singapore, 2017, 293 s.

[181] R.A.W. RHODES, *The New Governance: Governing without Government'*, in *Political Studies*, 44, 1996, 652 ss., che individua sei definizioni di *governance*, da intendersi come *minimal state*, *corporate governance*, "*good governance*", *socio-cybernetic system*, *self-organizing networks*, *new public management*, per proporre infine una de-

intendersi come quel «nuovo stile di governo, distinto dal modello del controllo gerarchico e caratterizzato da un maggior grado di cooperazione e dall'interazione tra lo stato e attori non statuali all'interno di reti decisionali miste pubblico/private»[182].

A questo passaggio si potrebbe accostare un ulteriore cambio di paradigma, ovvero l'affiancamento alla "*hard law*" della c.d. "*soft law*"[183]. Quest'ultimo è un concetto ampio, che assume diversa consistenza a seconda dei diversi ordinamenti in cui si colloca[184], ma che al fondo indica una forma alternativa di regolazione costituita da atti solo genericamente di natura normativa, perché privi del carattere tipico della vincolatività e della autoritatività delle norme giuridiche, formulati in esito ad un procedimento non necessariamente formalizzato, ma latamente consensuale[185].

Stanti questi caratteri, taluni dubitano della giuridicità della *soft law*[186], accusandola di favorire una eccessiva contrazione del potere politico tradizionale[187]. Forte della sua ampia diffusione, tuttavia, essa

finizione come "*self-organizing interorganizational networks*" che integrano il mercato e le gerarchie istituzionali nell'allocazione delle risorse, esercizio dei controlli e coordinamento per le politiche pubbliche.

[182] R. MAYNTZ, *La teoria della governance: sfide e prospettive*, in *Rivista italiana di Scienza politica*, 1, 1993, 3 ss., cui si rinvia anche per una seconda accezione di *governance*, più generica, da intendersi come «modalità distinte di coordinamento delle azioni individuali, intese come forme primarie di costruzione dell'ordine sociale», ma anche per le diverse possibili interpretazioni e ulteriori indicazioni bibliografiche al riguardo.

[183] A. ALGOSTINO, *La soft law comunitaria e il diritto statale: conflitto fra ordinamenti o fine del conflitto democratico?*, in *Costituzionalismo.it*, 3, 2016, 258, nota 13.

[184] Così partendo dal diritto internazionale, entro cui è stato elaborato, o dal diritto dell'UE e dal diritto nazionale; cfr. E. BUCALO, *Autorità indipendenti e* soft law. *Forme, contenuti, limiti e tutele*, Giappichelli, Torino, 2018, 3 ss.; E. MOSTACCI, *La* soft law *nel sistema delle fonti: uno studio comparato*, Cedam, Padova, 2008, 49 ss., cui si rinvia per i richiami bibliografici.

[185] Cfr. le considerazioni riassuntive di E. BUCALO, *Autorità indipendenti e* soft law, cit., 25 ss., e E. MOSTACCI, *La* soft law *nel sistema delle fonti: uno studio comparato*, cit., 1 ss.

[186] R. BIN, *Soft law, no law*, in A. SOMMA (a cura di), *Soft law e hard law nelle società postmoderne*, Giappichelli, Torino, 2009, 31 ss.

[187] A. ALGOSTINO, *La soft law comunitaria e il diritto statale: conflitto fra ordinamenti o fine del conflitto democratico?*, cit., 263.

esprime l'esigenza di superare una concezione delle fonti basata solamente sulle forme[188], nell'interno di regolare ambiti ove manchino le condizioni per adottare una normativa giuridica in senso stretto[189].

Tecnologie come quelle di riconoscimento facciale richiedono un approccio che consenta di sfruttare tutti gli elementi di flessibilità offerti dal carattere "soft" della regolazione, in quanto adattabile nel corso del tempo; suscettibile di essere sottoposta a verificazione nel suo impatto in concreto; in grado di garantire un ruolo partecipativo ai destinatari della stessa; presidiata nella sua osservanza non dalla cogenza in senso tradizionale, ma dalla capacità persuasiva e dalla convenienza[190].

In assenza di una legislazione sovranazionale o nazionale a disciplina delle TRF, è proprio agli atti di *soft law* che bisogna guardare per comprendere in che direzione si sta muovendo la regolazione di queste tecnologie. Ciò accade soprattutto a livello ultrastatale, come nel caso delle norme tecniche più diffuse – di cui si è già dato conto[191] – che potrebbero anche essere ricondotte a tale categoria. Ma si pensi anche alle comunicazioni, risoluzioni e piani di azione delle istituzioni

[188] A. POGGI, *Soft law nell'ordinamento comunitario*, in AA.VV., *Associazione Italiana dei Costituzionalisti. Annuario 2005. Atti del XX Convegno Annuale, Catania 14-15 ottobre 2005*, Cedam, Padova, 2007, 369 ss.

[189] Esprimendo una valenza, che secondo la categorizzazione comune, può essere classificata come integrativa, addirittura alternativa, o comparativa alla *hard law*; cfr. E. MOSTACCI, *La* soft law *nel sistema delle fonti: uno studio comparato*, cit., 41 ss. e 117 ss. In ciò, la *soft law* potrebbe rappresentare un luogo di incrocio tra modalità giuridiche dello Stato di diritto e modalità di *governance* della globalizzazione, la quale pare capace di eludere la sovranità dello Stato e le sue più tipiche manifestazioni di volontà normativa senza tuttavia metterle in discussione; cfr. E. MAESTRI, *Lex Informatica*, cit., 102.

[190] Per una ricostruzione delle origini degli strumenti regolatori "*soft*", cfr. A. DI ROBILANT, *Genealogies of Soft Law*, in *The American Journal of Comparative Law*, 54, 3, 2006, 499 ss. Riporta M. RAMAJOLI, Self regulation*,* soft regulation *e* hard regulation *nei mercati finanziari*, in *Rivista della Regolazione dei mercati*, 2, 2016, 60 s., come il termine "regolamentazione flessibile" sia stato utilizzato nel nostro ordinamento dalla legge di delega del codice dei contratti pubblici all'art. 1, c. 1, lett. t, della legge n. 11/2016, e poi all'art. 213, c. 2, del d.lgs. n. 50/2016, per indicare il carattere proprio di una serie di atti di competenza dell'Anac, la cui natura rimane peraltro incerta.

[191] V. *retro* par. 4.

dell'Unione europea, con le quali – come si è già ricordato – il Parlamento europeo ha avuto modo di manifestare "profonda preoccupazione" per i programmi di "sorveglianza emotiva" e i sistemi di "credito sociale"[192], o la Commissione ha inteso mettere in guardia dall'impiego di sistemi di identificazione biometrici che sfruttano IA, per la tutela dei diritti fondamentali o gli effetti discriminatori che possono derivare[193]. Analogamente, anche il *Consultative committee* della Convenzione 108+ dimostra una crescente attenzione verso questo tipo di tecnologie[194].

La quota più consistente di atti di *soft law* in tema di TRF va tuttavia attribuita alle pronunce delle istituzioni di garanzia dei dati personali, come le "linee guida" adottate dall'allora Gruppo di lavoro "Articolo 29"[195], oggi Comitato europeo per la protezione dei dati[196], quale sviluppo concreto della disciplina generale. Decisivo, inoltre, è il concorso delle singole autorità nazionali di controllo, più sensibili alle politiche concretamente adottate e alle prassi sviluppatesi nel contesto dei singoli ordinamenti[197].

La scarsità del dato normativo in senso stretto non esprime solamente la difficoltà, quando non la reticenza, a disciplinare le TRF sul piano giuridico, ma rivela come occorra seguire una prospettiva regolatoria differente che solo da ultimo può – e in molti casi, deve – sfociare in un atto giuridico di livello legislativo. È stato osservato, infatti,

[192] Cfr. PARLAMENTO EUROPEO, *Una politica industriale europea globale in materia di robotica e intelligenza artificiale*, cit., p. 13.

[193] Cfr. EUROPEAN COMMISSION, White Paper "*On Artificial Intelligence - A European approach to excellence and trust*", cit., 21 e 11.

[194] CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on Facial Recognition*, cit.

[195] Tra le più significative, cfr. GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile*, cit.; ma anche ID., *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, cit.

[196] Cfr. COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit.

[197] Tra i molti atti già citati, si ricordi GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento generale prescrittivo in tema di biometria*, cit.; CNIL, *Facial recognition: for a debate living up to the challenges*, cit.; INFORMATION COMMISSIONER'S OFFICE, *ICO investigation into how the police use facial recognition technology in public places*, cit.

come il carattere non vincolante della *soft law* e l'apertura alla partecipazione degli *stakeholders* nella relativa fase di adozione e implementazione costituiscano, allo stesso tempo, i pregi ma anche i principali limiti di questa forma di regolazione. Per questo la *soft law* «non sembra sufficiente ad assicurare l'armonizzazione ed il conseguimento di beni ed obiettivi comuni», rimanendo intatta la necessità «della produzione di una quota, seppure limitata, di *hard law*, la quale potrebbe comunque mantenere i tratti di un diritto "guida" sovranazionale, che mira all'armonizzazione, gestisce problemi transnazionali in una dimensione più ampia rispetto a quella nazionale, ma lascia un margine di apprezzamento agli Stati», i quali detengono ancora competenze rilevanti soprattutto con riguardo all'impatto di queste tecnologie su interessi costituzionali e diritti fondamentali[198].

7. *Spunti sul ruolo delle norme giuridiche nella regolazione delle TRF*

Il moltiplicarsi di canali e di tecniche regolative induce a giudicare come limitata la prospettiva di una regolazione che si imponga in termini uniformi a tutti i processi decisionali e a tutte le possibili applicazioni delle TRF[199]: sarebbe un "*one-size-fits-all approach*"[200] che pure il Parlamento europeo tende a osteggiare[201]. Occorrerebbe invece immaginare una combinazione degli strumenti sopra richiamati, allo scopo di confezionare schemi regolatori "*tailor-made*", in quanto "cuciti su misura" rispetto ai casi specifici e, ad un tempo, sufficientemente

[198] Cfr. E. STRADELLA, *La regolazione della Robotica e dell'Intelligenza artificiale: il dibattito, le proposte, le prospettive. Alcuni spunti di riflessione*, cit., 84.

[199] Più in generale, cfr. COUNCIL OF EUROPE, *Discrimination, artificial intelligence, and algorithmic decision-making*, cit., 37.

[200] Cfr. R. BROWNSWORD, *Law, Technology and Society*, cit., 43, che distingue tra i due estremi di "*top-down regulatory environments*" e "*bottom-up self-regulatory environments*", con tutte le possibili varianti intermedie.

[201] PARLAMENTO EUROPEO, *Una politica industriale europea globale in materia di robotica e intelligenza artificiale*, cit., punto 116, ove si specifica che il Parlamento «ritiene che una legge o una regolamentazione completa dell'intelligenza artificiale deve essere affrontata con cautela, in quanto la regolamentazione settoriale può offrire politiche sufficientemente generali ma anche perfezionate a un livello utile per il settore industriale».

stringenti per offrire tutela in relazione agli utilizzi ed ai diritti fondamentali coinvolti di volta in volta[202].

Si è consapevoli che, in questo modo, il quadro regolativo è destinato a complicarsi e che, di conseguenza, occorrerebbe calibrare il ruolo delle norme giuridiche in questa prospettiva. Ad esse dovrebbe comunque spettare il compito di orientare tale complessità e, così, aspirare a dirigere lo sviluppo tecnologico, anziché limitarsi ad inseguirlo[203]. A questo riguardo, può essere utile formulare alcune considerazioni ulteriori in relazione all'analisi fin qui svolta.

Nella regolazione di tecnologie come quelle di riconoscimento facciale, prima di tutto, le norme giuridiche sono necessariamente chiamate a veicolare una visione politica complessiva delle scelte regolative, che non rimetta completamente l'iniziativa a singoli operatori, siano esse imprese private o anche amministrazioni settoriali, entro contesti limitati e senza alcuna prospettiva di fondo[204]. Come recentemente chiarito dal Garante della *privacy*, il rischio è che «singole iniziative, sommate tra loro, definendo un nuovo modello di sorveglianza introducano, di fatto, un cambiamento non reversibile nel rapporto tra individuo ed autorità»[205]. Occorre invece che il decisore politico si assuma pienamente la responsabilità – e conseguentemente si sottoponga al controllo democratico – su scelte relative, ad esempio, al punto in cui collocare la soglia di rischio accettabile per l'impiego delle TRF in relazione alla possibile limitazione delle libertà in un dato momento storico, se contenere fortemente il ricorso a tali tecnologie o addirittura proibirlo[206].

[202] Come anche suggerito in EUROPEAN PARLIAMENT, *Artificial Intelligence and Civil Liability. Study requested by the JURI committee*, cit., 98.

[203] «The need to shift from chasing to leading», sottolineato da L. FLORIDI, *Soft Ethics and the Governance of the Digital*, in *Philos. Technol.*, 31, 2018, 2. Spunti sulla necessità che il diritto "guidi" e "orienti" la tecnologia anche in A. PAJNO ET AL. *AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal*, 3, 2019, 215.

[204] Come suggerito anche in CNIL, *Facial recognition: for a debate living up to the challenges*, cit., 2.

[205] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, cit., p. 1.

[206] CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on Facial Recognition*, cit., 5.

Tra le diverse forme che possono assumere le norme giuridiche allo scopo, come anche si evince dalla disciplina attualmente in vigore a protezione dei dati personali, la più adatta sembrerebbe essere quella dei *principi* piuttosto che delle regole puntuali. Ciò in ragione di una molteplicità di fattori.

La forma dei principi contribuisce, in primo luogo, a superare alcune obiezioni che possono essere mosse alla pretesa delle norme giuridiche di regolare le tecnologie più innovative. Da una parte, infatti, il diritto interferisce con la tecnologia rischiando di ingessarne inutilmente la ricerca e lo sviluppo, a causa dell'emergere continuo di problematiche che il diritto non ha – o non ha ancora – considerato[207]. Dall'altra, mentre la tecnologia evolve esponenzialmente, il diritto segue dinamiche e processi di produzione molto più lenti[208], in una sorta di "desincronizzazione"[209] tra il tempo umano, quello della politica e quello della tecnologia.

In risposta, i principi giuridici, grazie alla loro formulazione sufficientemente ampia e indeterminata, spesso limitata alla proclamazione di valori, e grazie al loro contenuto normativo, non espresso tramite un enunciato tipicamente condizionante o limitato ad una unica fattispecie[210], possono essere riferiti non ad un solo dato tecnico o ad un solo problema, ma a tendenze di lungo periodo[211].

[207] Al riguardo, il Parlamento europeo ha raccomandato «che per l'Unione dovrebbe essere adottato un approccio graduale, pragmatico e cauto [...] per quanto riguarda qualsiasi iniziativa futura sulla robotica e sull'intelligenza artificiale al fine di garantire che l'innovazione non sia soffocata»; cfr. PARLAMENTO EUROPEO, *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, cit. È condiviso, infatti, il giudizio sulla opportunità di evitare di disciplinare una nuova tecnologia ad uno stadio ancora poco avanzato di sviluppo. Tuttavia, come osserva R. CALO, *Artificial Intelligence Policy: A Primer and Roadmap*, cit., 409, risulta parimenti necessario monitorare sistematicamente gli effetti sulla società e sull'economia, per acquisire una base conoscitiva, mappare gli interessi rilevanti e riuscire a formulare una disciplina più consapevole.

[208] COUNCIL OF EUROPE, *Discrimination, artificial intelligence, and algorithmic decision-making*, cit., 33 s.

[209] L. ALEXANDRE, *La guerra delle intelligenze*, cit., 51 ss.

[210] Sulla distinzione tra principi e norme e sulle caratteristiche specifiche assunte dai primi, per gli aspetti citati e per un quadro riassuntivo, cfr. R. GUASTINI, *Teoria e dogmatica delle fonti*, Giuffrè, Milano, 1998, 275 ss.

[211] S. RODOTÀ, *Tecnologie e diritti*, cit., 42.

Al riguardo, sul piano metanormativo, viene in rilievo il principio di "neutralità tecnologica della legge", ovvero l'idea – accolta anche dalla normativa UE[212] – che spetti alla regolazione giuridica definire gli obiettivi e i valori da tutelare, a prescindere dal singolo particolare tecnologico impiegato per perseguirli[213]. Che la legge non si riferisca ad una tecnologia specifica – ad esempio, le TRF che sfruttano algoritmi "di vecchia generazione", piuttosto che quelli di *machine learning* – è una necessità che può giustificarsi non solo per non limitare ingiustamente lo sviluppo di specifiche tecnologie, ma anche per non correre il rischio di rendere la norma giuridica rapidamente obsoleta innanzi allo sviluppo tecnologico, o che possa risultare inefficace nella tutela di diritti fondamentali minacciati da forme tecnologiche che tendono a sfuggire a rigide classificazioni[214].

I principi giuridici, in secondo luogo, paiono la forma la più adatta per assolvere al compito di orientare gli altri strumenti di regolazione nella misura in cui assumono il carattere di norme "fondamentali", destinate cioè a dare fondamento e giustificazione ad altre norme attraverso le quali trovano specificazione e sviluppo[215].

[212] Questa accezione del principio di neutralità tecnologica costituisce un pilastro della disciplina europea sulle telecomunicazioni, di cui alla direttiva quadro 2002/21/CE, del 7 marzo 2002, (v. cons. 18, ove si esortano gli Stati membri a non imporre l'uso di un particolare tipo di tecnologia né operare discriminazioni tra particolari tecnologie), e, per quanto qui rileva più direttamente, trova espressa menzione al cons. 15 del GDPR e al cons. 18 della LED, ove si suggerisce che «la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate».

[213] Come stabilito anche dalla Commissione, «neutralità rispetto alle tecnologie significa che la legislazione deve definire gli obiettivi da perseguire e non deve imporre né favorire l'uso di un particolare tipo di tecnologia per conseguirli»; cfr. COMMISSIONE EUROPEA, comunicazione del 10 novembre 1999, *Verso un nuovo quadro per l'infrastruttura delle comunicazioni elettroniche*, COM(1999) 539 definitivo, 13. Cfr. anche U. PAGALLO, *Intelligenza Artificiale e diritto. Linee guida per un oculato intervento normativo*, cit., 626 s., che distingue tra "neutralità tecnologica della legge", per il quale il legislatore non deve favorire una delle tecnologie per dare attuazione agli obiettivi prefissati, e "indifferenza tecnologica della legge", per il quale le finalità perseguite dal legislatore non devono dipendere dalla tecnologia utilizzata.

[214] Cfr. M. HILDEBRANDT, *Smart technologies and the End(s) of Law. Novel Entanglements of Law and Technology*, cit., 214 ss., che si riferisce ai tre obiettivi come "innovation objective", "sustainability objective" e "compensation objective".

[215] Cfr. sempre R. GUASTINI, *Teoria e dogmatica delle fonti*, cit., 282 s.

In questo modo è possibile costruire la cornice entro cui si possono giocare, assieme alle regole propriamente giuridiche, anche le diverse combinazioni per delineare le citate disciplina "su misura" delle TRF, facendo leva – come visto – su differenti variabili quali il grado di cogenza e vincolatività espressa dalle diverse forme di regolazione, oppure la garanzia di un coinvolgimento dei destinatari nella relativa adozione. Tale scelta potrà essere graduata a seconda dei contesti particolari[216], anche alla luce del principio di precauzione. Per garantire la tutela di interessi rilevanti, quindi, diviene possibile fare affidamento sulla auto-regolazione, nella misura in cui si ritenga sufficiente rimettersi all'iniziativa spontanea dei destinatari della normazione tramite l'adozione di principi etici, oppure sfruttare il "codice" e il "*design*" di un sistema, eventualmente imponendo determinati requisiti tramite il richiamo a standard tecnici, per costringere ad un certo comportamento e impedire a monte la violazione di specifici interessi; contestualmente, è possibile fare ricorso a forme di auto-regolazione o co-regolazione per fondare sulla collaborazione con i destinatari l'adozione e l'implementazione di una regolazione più efficace, sino alla specificazione di divieti e sanzioni eteroimposte tramite regole giuridiche; allo scopo, ancora, si possono adoperare le diverse formule sperimentali e gli strumenti di "*soft-regulation*" per acquisire gli elementi necessari e addivenire in maniera graduale alla formulazione di una regolazione delle TRF che non ne soffochi il progresso, ma che presidi allo stesso tempo l'imprescindibile esigenza di tutela dei diritti.

In questo modo, in via esemplificativa, la regolazione delle TRF utilizzate per finalità verificative all'ingresso di una abitazione privata si troverebbe a dover accordare protezione a consumatori e utenti sotto i richiamati profili della tutela di riservatezza, *privacy*, dati personali, ed anche eguaglianza. In questo caso, dovrà necessariamente venire in gioco il regime legislativo sulla sicurezza dei prodotti e sulla responsa-

[216] Si tratta di prospettive ben consciute alla riflessione politologica sulla regolazione, come emerge, ad esempio, dalle "*pyramids of supports and of sanctions*" elaborate in J. BRAITHWAITE, *Fasken Lecture: The Essence of Responsive Regulation*, in *University of British Columbia Law Review*, 44, 2011, 475 ss., ove si integrano diverse strategie di regolazione tramite incentivi e sanzioni su molteplici livelli, a partire da strumenti di persuasione fino alla forma della sanzione cogente.

bilità dei produttori[217], ma anche – oggetto qui di maggiore attenzione – sulla tutela dei dati personali. In termini complementari, gli standard occuperanno rilievo cruciale nel garantire la sicurezza e la qualità dei sistemi di riconoscimento facciale, mentre forme di auto-regolazione da parte delle imprese saranno ben ammissibili allo scopo di promuovere l'affidabilità ed incentivare l'impiego di queste tecnologie, garantendo eventualmente una maggiore trasparenza nelle relative caratteristiche e funzionamento.

Questa combinazione di tecniche normative non sarà identica quando le TRF sono impiegate, sempre in via esemplificativa, per finalità di categorizzazione a scopi di marketing negli esercizi commerciali. A venire in gioco, in questo caso, oltre ai diritti citati sopra, vi sarà anche il profilo dell'identità personale e virtuale. In prospettiva, si potrebbe qui immaginare non solo una maggior precisazione tramite atti di *soft law* da parte delle autorità garanti per la protezione dei dati, ma anche accordare spazio più ampio a meccanismi di co-regolazione, sulla falsariga di quanto accaduto negli Stati Uniti con il "*code of conduct*" approvato dall'agenzia NTIA con il concorso di molteplici *stakeholders*, attraverso cui concordare con i produttori di queste tecnologie o coloro che offrono questi servizi un regime di tutela finalizzato a tali specifiche situazioni, sfruttando le conoscenze in loro possesso per comprendere i cambiamenti tecnologici in atto.

Infine, un regime ancora differente dovrà essere stabilito in Paesi, come l'Italia, in cui le TRF cominciano ad essere sfruttate routinariamente con finalità identificative da parte delle forze dell'ordine. Qui a venire in gioco sono anche altri diritti di libertà classici, in relazione anzitutto alla libertà personale, ma anche, indirettamente, di riunione o manifestazione del pensiero. In questo caso alla legge sarà richiesto di stabilire, in ossequio alle riserve contenute in Costituzione, regole più precise sulle condizioni di impiego di questi strumenti di sorve-

[217] Cfr. direttiva 2001/95/CE del 3 dicembre 2001, relativa alla sicurezza generale dei prodotti, e la direttiva 85/374/CEE del 25 luglio 1985, in materia di responsabilità per danno da prodotti difettosi, che ricevono attuazione generale nel d.lgs. 6 settembre 2005, n. 206, recante Codice del consumo; con tutte le difficoltà di riferire la disciplina in vigore su questi profili alle nuove tecnologie algoritmiche: v. A. BERTOLINI, *Artificial Intelligence and Civil Liability. Study requested by the JURI committee*, cit.

glianza, ma non è escluso che possano immaginarsi meccanismi di coregolazione con i quali le forze di polizia siano chiamate a definire, in analogia a quanto avviene nel Regno Unito[218], ulteriori garanzie a protezione dei dati personali.

La rilevanza così assunta da principi e norme giuridiche dovrebbe contribuire anche a salvaguardare le ragioni di fondo di alcuni istituti e principi cardine del sistema delle fonti e posti a presidio dei diritti fondamentali in Costituzione, quali la riserva di legge e il principio di legalità.

Pur rifuggendo da generalizzazioni improprie[219], si pensi comunque alle funzioni che complessivamente, fin dai primi anni della storia repubblicana, vengono ricollegate all'istituto della riserva di legge, ovvero la sua *ratio* garantista e democratica[220]. In questo modo tale istitu-

[218] V. *retro* Cap. III, par. 7, a proposito del *Surveillance Camera Code of Practice*.

[219] Sul carattere non omogeneo delle diverse riserve, cfr. R. BALDUZZI, F. SORRENTINO, *Riserva di legge*, in *Enc. dir.*, XL, 1989, 1218, ma in generale tutta la dottrina alla prossima nota. Allo stesso modo, osserva G.U. RESCIGNO, *Sul principio di legalità*, in *Diritto pubblico*, 1995, 290: «il principio di legalità significa una cosa se riferito al sistema normativo, e significa altra cosa quando viene riferito ai giudici, e altra cosa ancora quando viene riferito alla pubblica amministrazione»: nel primo caso, può assumere una valenza anche formale, mentre per gli altri deve sempre assumere una valenza sostanziale, non potendosi limitare a conferire un nudo potere, ma deve disciplinare tale potere in tutti i suoi aspetti sostanziali.

[220] Della sterminata letteratura sul punto, basti qui richiamare la recente ricostruzione offerta in G. PICCIRILLI, *La "riserva di legge"*, cit., spec. 24 ss., cui si rinvia anche per le riflessioni dottrinarie più risalenti sulla riserva di legge, che oscillano nel rimarcare la *ratio* garantista dell'istituto, in quanto posto a garanzia dei diritti individuali e, in particolare, a protezione del singolo contro le possibili arbitrarietà dell'esecutivo, specie in rapporto alle violazioni della pubblica amministrazione, anche per il tramite del sindacato giurisdizionale della Corte costituzionale; e la *ratio* democratica, che enfatizza il collegamento tra produzione normativa e Parlamento, nella sua legittimazione di unico organo investito dal popolo sovrano, aperto alla partecipazione delle minoranze e, nel suo *modus operandi*, alla pubblicità delle sedute. Sul punto, basti rinviare anche a F. SORRENTINO, *Lezioni sulla riserva di legge*, I, Cooperativa libraria universitaria, Genova, 1980; R. BALDUZZI, F. SORRENTINO, *Riserva di legge*, cit., 1207 ss.; L. CARLASSARE, *Legge (riserva di)*, in *Enc. giur.*, XVIII, 1990; R. GUASTINI, *Legge (riserva di)*, in *Dig. disc. pubbl.*, IX, 1997, 163 ss.; S. FOIS, *"Delegificazione", "riserva di legge" e principio di legalità*, in AA.VV. *Studi in onore di Manlio Mazziotti di Celso*, I, Cedam, Padova, 1995, 727 ss.

to, comunque da rimeditare e adeguare ai cambiamenti di sistema che investono il nostro ordinamento[221], impone – come noto – che nel caso di riserve assolute, come quella a presidio della libertà personale, la legge disciplini l'intera materia[222]. Qualora si ritenesse, dunque, che le TRF vadano ad incidere su tale libertà, nella sua accezione di "libertà morale", è alle fonti di rango primario che occorrerebbe rivolgersi per stabilire le relative condizioni di impiego da parte delle forze dell'ordine. Qualora, invece, si propendesse per una accezione di tale libertà più ristretta, la sottoposizione a TRF senza il consenso dell'interessato potrebbe comunque qualificarsi come imposizione di un "obbligo personale", e pertanto l'attenzione si sposterebbe sulla riserva di legge relativa all'art. 23 Cost., che pure nel tempo ha visto ridurre lo spazio di intervento richiesto alla fonte legislativa[223]. Quest'ultimo tipo di riserve, comunque, risultano soddisfatte dall'intervento di una fonte di rango primario che eventualmente stabilisca una cornice di principi, fosse anche in concorso con le fonti dell'UE[224].

Oppure, si consideri l'analoga *ratio* garantista e democratica riconosciuta – in stretta continuità[225], pur senza sovrapposizione[226] – al

[221] Cfr. sempre G. PICCIRILLI, *La "riserva di legge"*, cit., a proposito della necessità di operare una "de-mitizzazione" dell'istituto, anche grazie all'ausilio della giurisprudenza costituzionale, per non riproporre acriticamente le argomentazioni della prima riflessione costituzionalistica, o quantomeno attualizzarle alla luce dei mutamenti di contesto del sistema costituzionale; tale operazione porta l'A., fra l'altro, a valorizzare la riconducibilità al sindacato di legittimità costituzionale degli atti che ricadono negli ambiti coperti da riserva di legge.

[222] Sul punto, cfr. *retro* Cap. II, par. 5.

[223] Per indicazioni in merito agli indirizzi giurisprudenziali sul punto, soprattutto circa le prestazioni patrimoniali, v. più approfonditamente D. MORANA, *Libertà costituzionali e prestazioni personali imposte*, cit., 134 ss.

[224] Più conferente sul punto è C.cost., sent. n. 383/1998, la quale, pronunciandosi sulla riserva di legge in materia di autonomia universitaria, ha ammesso, fra l'altro, il concorso di fonti dell'UE per delimitare la discrezionalità della pubblica amministrazione; sul punto, v. G.M. SALERNO, *Riserva di legge e principio di legalità nel processo di integrazione europea*, in F. MODUGNO (a cura di), *Trasformazioni della funzione legislativa. II. Crisi della legge e sistema delle fonti*, Giuffrè, Milano, 2000, 307 ss.

[225] Cfr. G. ZAGREBELSKY, *Manuale di diritto costituzionale. I, Il sistema delle fonti del diritto*, Utet, Torino, 1988, 53 s., che limita l'accezione sostanziale del principio di

principio di legalità[227]. Tale principio, nell'attuale assetto ordinamentale, ha visto smorzare la pretesa di porre l'atto legislativo come fondamento stringente ed esaustivo di ogni altra manifestazione normati-

legalità agli ambiti coperti da riserva di legge. Di differenza puramente quantitativa parla L. CARLASSARE, *Legalità (principio di)*, cit., 8, «dalla garanzia massima costituita dalla riserva assoluta in cui tutto deve essere nella legge, attraverso la figura intermedia della riserva relativa (limitata anch'essa alle materie indicate in Costituzione), si passa alle situazioni residue in cui vige il generale principio di legalità». Secondo V. CRISAFULLI, *Lezioni di diritto costituzionale,* II, 1, *L'ordinamento costituzionale italiano (le fonti normative)*, Cedam, Padova, 1993, 64 ss., in termini generali vi sarebbe una distinzione, perchè il principio di legalità offrirebbe fondamento positivo e limite negativo al potere delle pubbliche amministrazioni nella previa norma, mentre la riserva di legge «esige invece molto di più», ovvero che la legge regoli essa stessa in modo sufficientemente preciso la materia che ne è oggetto, limitando così la discrezionalità amministrativa; salvo poi ravvisare una convergenza sostanziale nel caso di riserva di legge relativa e legalità sostanziale, sebbene la prima imponga maggior determinatezza della disciplina.

[226] Sulla distinzione tra riserva di legge e principio di legalità sostanziale, la prima relativa al rapporto tra fonti e l'altro finalizzato a stabilire limiti e condizioni all'azione dell'amministrazione, cfr. R. BALDUZZI, F. SORRENTINO, *Riserva di legge*, cit., 1218. Sottolinea le differenze anche G.U. RESCIGNO, *Sul principio di legalità*, cit., 247 ss., a partire dalla natura di istituto dell'uno e di principio dell'altro.

[227] Sul punto, basti rinviare alla ricostruzione in A. CARDONE, *La «normalizzazione» dell'emergenza. Contributo allo studio del potere* extra ordinem *del Governo*, Giappichelli, Torino, 2011, 367 ss., e 372 ss., ove ci si riferisce alla componente garantistica del principio di legalità come "conformità alla legge", ovvero l'idea che il provvedimento amministrativo debba sempre essere adottato in forza di una disciplina legislativa sostanziale che definisce i limiti del potere esercitato, perché il rispetto dei medesimi possa essere sindacato da un giudice a tutela delle posizioni giuridiche soggettive del privato che lamenti una lesione a causa dell'illegittimità dell'azione amministrativa; mentre la componente democratica enfatizza la connotazione del principio di legalità come "presupposizione legislativa", secondo cui ogni atto del pubblico potere deve essere adottato in forza di una previa disciplina legislativa che istituisce il potere esercitato, a garanzia che ogni limitazione alla sfera giuridica degli interessati sia considerabile democratica, in quanto espressione della volontà dei governanti ad un tempo rappresentanti dei governati. Si veda, più in generale, S. FOIS, *Legalità (principio di)*, in *Enc. dir.*, XXIII, 1975, 659 ss.; R. GUASTINI, *Legalità (principio di)*, in *Dig. disc. pubbl.*, IX, 1991, 84 ss.; L. CARLASSARE, *Legalità (principio di)*, cit.; G.U. RESCIGNO, *Sul principio di legalità*, cit., 247 ss.; F. SORRENTINO, *Lezioni sul principio di legalità*, Giappichelli, Torino, 2007.

va[228]. Secondo quanto specificato dalla giurisprudenza costituzionale, la valenza garantista e democratica del principio di legalità sostanziale, come anche della riserva di legge, possono riceve una diversa configurazione in presenza di alcuni tratti specifici della normazione, come il carattere spiccatamente tecnico[229], o – come emerge soprattutto dai più recenti indirizzi sui poteri normativi delle autorità amministrative indipendenti – la presenza di moduli di coinvolgimento dei destinatari della stessa che, in una qualche misura, contemperino il *deficit* in punto di predeterminazione legislativa di queste forme innovative di attività regolativa[230].

[228] Sul mutamento del principio di legalità, in uno con il declino dei modelli democratici basati esclusivamente sulla rappresentanza di matrice liberale, prevalentemente a causa dell'imporsi del principio pluralista, cfr. A. CARDONE, *La «normalizzazione» dell'emergenza*, cit., 372 ss., con una analisi condotta sul piano del sistema delle fonti, nella prospettiva della compatibilità costituzionale dei poteri *extra ordinem* del Governo e della loro derivazione dal bilanciamento tra interessi costituzionali.

[229] Il principio di legalità sostanziale si dimostra "permeabile" rispetto alle ragioni della tecnica, come dimostra quella giurisprudenza costituzionale elaborata con specifico riguardo al coordinamento tecnico, secondo cui, quando vengono in rilievo regole tecniche «dalle quali non derivano limitazioni alle scelte rientranti nell'autonomia politico-amministrativa dell'ente, il principio di legalità può dirsi soddisfatto dall'esistenza di norme legislative abilitative di organi del potere esecutivo, dotati di specifiche attitudini» (cfr. C.cost., sent. n. 31/2001, n. 356/1994, n. 483/1991), secondo un indirizzo che sembrerebbe confermato anche dopo le riforme costituzionali del Titolo V; cfr. A. IANNUZZI, *Il diritto capovolto*, cit., 129 ss., e dottrina ivi richiamata.

[230] Si tratta di quella giurisprudenza costituzionale, soprattutto recente, con la quale, pur nelle specificità di ciascuna autorità amministrative indipendente e nelle diversità di leggi istitutive, relative funzioni e ambiti materiali in cui esse operano, è stata valorizzata l'ampia discrezionalità di cui godono, stante la difficoltà di «predeterminare con legge in modo rigoroso i presupposti delle funzioni amministrative attribuite alle autorità» (con riguardo alla riserva di legge relativa all'art. 23 Cost., v. sent. n. 69/2017, 7.2. cons. dir., concernente i poteri dell'Autorità per la regolazione dei trasporti). Altro elemento da sottolineare, dunque, è la natura tecnica della regolazione affidata alle autorità garanti, che può determinare una attenuazione del rigore del principio di legalità, sebbene i relativi poteri possano subire condizionamenti anche da parte del diritto dell'UE (sent. n. 99/2018, sui poteri regolativi della Banca d'Italia nella definizione della limitazione al rimborso in caso di recesso del socio a seguito di trasformazione delle banche popolari in s.p.a., vincolati dalle previsioni del regolamento (UE) n. 575/2013). La tecnicità delle relative funzioni, inoltre, ha condotto a ritenere una compensazione sufficiente la partecipazione degli operatori del setto-

Si tratta di indirizzi che rimarcano come, in presenza di questi caratteri della normazione, la legge sia chiamata a raggiungere un equilibrio nel manifestare un grado di elasticità sufficiente a garantire l'apertura verso diversi apporti regolatori e, allo stesso tempo, legittimare tali apporti definendone le condizioni e orientandoli verso determinati obiettivi. Secondo quanto emerge dalla giurisprudenza a livello europeo, inoltre, il quadro regolatorio che così risulta deve necessariamente soddisfare requisiti stringenti in punto di "qualità" e di "sostanza" delle norme, piuttosto che di mera forma[231].

Il moltiplicarsi di questi canali di regolazione, in definitiva, costituisce il portato di quel più ampio e ben conosciuto fenomeno riconducibile alla perdita di centralità dello Stato quale unico centro di produzione del diritto, e del diritto come fenomeno esclusivamente positivo[232]. In questo scenario, lo Stato assume un ruolo che è stato definito come "post-regolatorio", con il quale viene perso il tradizionale monopolio sul controllo e sul condizionamento di fenomeni sociali ed economici che deriva da una posizione di superiorità gerarchica, pur

re destinatari della regolazione, anche in funzione legittimante dell'intervento operato da un organismo estraneo al circuito democratico (v. la già richiamata sent. n. 69/2017, ma, più in generale, v. sent. n. 83/2015, n. 435/2001, n. 182/1994). Sul punto, riferimenti in G. PICCIRILLI, *La "riserva di legge"*, cit., 68 ss. Più in generale, sulla possibilità di fondare la legittimazione di questi organi sulla "democrazia procedimentale" e sulle "garanzie procedurali", v. le considerazioni e le critiche in G. GRASSO, *Le autorità amministrative indipendenti della Repubblica. Tra legittimità costituzionale e legittimazione democratica*, Giuffrè, Milano, 2006, 80 ss. Sui limiti della normativa che regola la partecipazione alle decisioni di queste autorità, riferiti alla eterodeterminazione della "legalità procedurale" e al "contraddittorio procedimentale", ma anche di distanza dalla partecipazione politica, v. L. BUFFONI, *Processo e pluralismo nell'ordinamento costituzionale italiano. Apologia e limiti dell'universalismo procedurale*, Jovene, Napoli, 2012, 331 ss. Più in generale, sulla prassi di questi aspetti, v. P. CARETTI (a cura di), *Osservatorio sulle fonti 2003-2004. I poteri normativi delle autorità indipendenti*, Giappichelli, Torino, 2004.

[231] Cfr. *retro* cap. III, par. 4.3.

[232] Sul punto, basti rinviare alle considerazioni ricostruttive in P. GROSSI, *L'Europa del diritto*, Laterza, Roma-Bari, 2007, spec. 219 ss., a proposito del Novecento giuridico come momento di riscoperta della complessità e dell'affievolirsi del rigido controllo della giuridicità da parte dello Stato; un controllo incrinato dal proliferare di fatti economici e sociali – ed anche, si potrebbe dire, tecnologici – che si impongono senza la sua mediazione.

continuando a intervenire tramite strumenti come la *soft law*, la capacità di indirizzare la *self-regulation* e le regole contrattuali adoperate da attori non pubblici, i processi di normalizzazione e di adozione di norme tecniche, finanche la "*regulation by architecture*"[233].

[233] Quelle che, tra le caratteristiche del "*Post-Regulatory State*", viene definita come "*variety in norms*" e "*in control mechanism*", a fianco di "*variety in controllers*" e in "*controllees*", da C. SCOTT, *Regulation in the Age of Governance. The Rise of the Post-Regulatory State*, in J. JACINT, D. LEVI-FAUR (a cura di), *The Politics of Regulation*, Edward Elgar, Cheltenham, 2004, 145 ss.

NOTE CONCLUSIVE

Al termine del percorso di analisi può dirsi pienamente confermata l'impressione secondo cui le TRF presentano caratteristiche uniche rispetto ad ogni altro sistema di sorveglianza.

Il riconoscimento facciale apre innanzitutto a forme inedite di sorveglianza di massa, come dimostra la perdita di anonimato entro gli spazi pubblici ove trovano impiego queste tecnologie, con il conseguente effetto dissuasivo (c.d. *chilling effect*) che ne deriva sull'esercizio delle proprie libertà. Ma, allo stesso tempo, le nuove tecniche algoritmiche e la loro capacità di analisi dei dati consentono a queste tecnologie di concentrare il controllo su singole persone[1], fino a sondare quei moti dell'animo che prendono forma nelle emozioni o nei tratti della personalità[2].

Come detto introduttivamente, la sfida che si profila nei prossimi anni è quella di guidare uno sviluppo delle tecnologie di IA che, su un piano etico, è stato definito dalle istituzioni europee come "*human-centred approach*". Di fronte a tecnologie così invasive come quelle di riconoscimento facciale, è pienamente giustificato interrogarsi a monte sull'alternativa tra proibirne l'utilizzo o accettare di formulare una regolazione più articolata. Allo stato attuale, infatti, sono evidenti la difficoltà dei legislatori a legittimare l'impiego di tali tecnologie *tout court* o anche solo a scopi limitati, al punto che persino le imprese private che si occupano della loro produzione stanno manifestando remore nei confronti del relativo sfruttamento per determinate finalità[3].

Su un piano propriamente giuridico, questa sfida si traduce in quello che potrebbe essere qualificato come il tentativo di formulare

[1] Sottolinea G. ZICCARDI, *Internet, controllo e libertà*, cit., 23 ss., come queste nuove tecnologie consentano di passare da forme di sorveglianza generale (uno-a-molti) a forme di sorveglianza particolare (uno-a-uno) in un istante.

[2] Cfr. *retro* Cap. I.

[3] Cfr. *retro* Introduzione.

una regolazione "costituzionalmente orientata"[4], entro cui la ricerca, lo sviluppo e l'utilizzo delle TRF risultino improntati al rispetto di principi giuridici e valori tipici del costituzionalismo liberal-democratico, come dignità, eguaglianza, libertà, autodeterminazione, che attualmente trovano consacrazione esplicita o implicita nelle Carte costituzionali e nelle Carte sovranazionali[5].

Il punto risulta estremamente delicato, se si pensa a come le TRF – si è visto[6] – riescano ad impattare su molteplici diritti fondamentali in maniera contestuale e trasversale. Ad esempio, l'uso di queste tecnologie dal vivo a scopi identificativi è suscettibile di invadere la sfera della *privacy* e della riservatezza personale; può risolversi in un trattamento illegittimo dei propri dati personali; può addirittura interessare la libertà personale, se intesa in senso lato; può condizionare l'esercizio della libertà di riunione e di manifestazione del pensiero; può produrre effetti discriminatori nei confronti di determinate categorie di soggetti per ragioni di origine etnica, sesso o età, e confermare condizioni personali di svantaggio.

Ma anche altri impieghi apparentemente più "innocui", come ad esempio a scopo di verificazione nei luoghi di lavoro o nella integrazione con applicazioni di *smartphone* di ultima generazione, possono intercettare numerosi dei profili sopra citati. Sino ad arrivare alle pra-

[4] Come suggerito da C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, cit., 102 ss., ulteriormente sviluppato in ID., *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, cit., 711 ss. V. anche A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, cit., 63 ss.; C. COLAPIETRO, A. MORETTI, *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali stampato*, *ivi*, 3, 2020, 368 ss.; T. GROPPI, *Alle frontiere dello stato costituzionale: innovazione tecnologica e intelligenza artificiale*, in *Consulta Online*, 3, 2020, 675 ss.

[5] Cfr. B. CARAVITA DI TORITTO, *Principi costituzionali e intelligenza artificiale*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., 461 ss. Come recentemente sottolineato dalla Corte costituzionale, «i principi e i diritti enunciati nella CDFUE intersecano in larga misura i principi e i diritti garantiti dalla Costituzione italiana (e dalle altre Costituzioni nazionali degli Stati membri), e che la prima costituisce pertanto «parte del diritto dell'Unione dotata di caratteri peculiari in ragione del suo contenuto di impronta tipicamente costituzionale» (sentt. n. 269/2017, n. 20/2019).

[6] Cfr. *retro* Cap. II.

tiche di categorizzazione per scopi commerciali e di marketing, che rischiano di favorire quelle ipotesi più riprovevoli di strumentalizzazione e riduzione della persona, oltre che dalla sua identità, ai dati e alle informazioni generate.

In questo quadro, i sistemi di informazione europei, tramite le politiche di integrazione in corso e la più accentuata circolazione dei dati che ne conseguirà, renderanno potenzialmente più strutturale l'assoggettamento a forme così penetranti di sorveglianza[7].

In direzione di questo approccio costituzionalmente orientato si muove la disciplina sulla protezione dei dati personali, che allo stato attuale offre il quadro normativo maggiormente sistematico cui assoggettare le TRF, in ragione sia della riconducibilità ad esso di ogni applicazione di riconoscimento facciale, sia della cornice offerta a qualsiasi altra disciplina settoriale, sia della sua valenza trasversale rispetto alle libertà sopra citate[8].

Da quest'ultimo punto di vista, si pensi alla valenza assunta dai principi di limitazione delle finalità e di minimizzazione dei dati, rispetto all'impiego delle immagini catturate dalle forze dell'ordine tramite "rastrellamenti", o acquisite dai datori di lavoro per esercitare un controllo a distanza sui propri dipendenti; oppure le condizioni previste per l'impiego di queste tecnologie di sorveglianza a "scopi pubblici rilevanti", che non legittimano la sottoposizione a riconoscimento facciale per il semplice fatto di circolare in luoghi pubblici o di aver pubblicato i propri dati sul web; o ancora al regime di sicurezza dei dati e ai limiti al loro riutilizzo, quale protezione contro i furto di identità digitale; o infine il divieto di discriminazioni, che sebbene allo stato non venga sancito in termini adeguati nei confronti di questi strumenti tecnologici, sta ricevendo una interpretazione estensiva per coprire anche le ipotesi di distorsioni algoritmiche (c.d. *bias*) produttive di diseguaglianze.

Presupposto per questo approccio costituzionalmente orientato, inoltre, è una dinamica cooperativa fra TRF, la società e le singole persone[9]. L'intento è di non far percepire queste tecnologie come espres-

[7] V. *retro* Cap. IV.

[8] Cfr. *retro* Cap. III.

[9] Così riprendendo uno spunto in P. BENANTI, *Le macchine sapienti*, Marinetti 1820, Bologna, 2018, 113.

sione di una manifestazione di "potere"[10] cui essere sottoposti[11]. Non si fa riferimento tanto alla questione se sia possibile o meno sottrarsi alle forme di sorveglianza digitale nelle quali siamo immersi[12], quanto piuttosto agli istituti giuridici a disposizione affinché la tecnologia rimanga uno strumento al servizio dell'essere umano – o meglio, di tutti gli esseri umani, nonché alle tecniche di tutela per proteggere contro i suoi impieghi indiscriminati e i relativi abusi. Da qui derivano tutti i diritti in cui si esprime un controllo e una autodeterminazione sui propri dati personali; la garanzia della trasparenza e della comprensibilità dei sistemi decisionali che sfruttano TRF; la salvaguardia offerta dell'intervento dell'essere umano nel meccanismo di riconoscimento; lo sfruttamento del design degli algoritmi per evitare *ad origine* che un sistema di riconoscimento facciale sia in grado di integrare, ad esempio, una discriminazione; l'anticipazione della soglia di tutela contro i rischi tramite una regolazione precauzionale. Sono solo alcuni dei profili che sono stati analizzati e che segnano il passaggio verso un approccio che non sia puramente rimediale, ma proattivo e preventivo.

La prima forma di garanzia contro queste tecnologie è la pregnanza assunta dal consenso di coloro che sono sottoposti a sorveglianza. Dove non arriva – e spesso non può arrivare – il consenso consapevole, allora deve necessariamente intervenire il vincolo di diritto a protezione di interessi meritevoli di tutela. Ne consegue l'indispensabilità di una regolazione giuridica che, in sintonia con il canone di proporzionalità, fissi almeno le condizioni entro cui le diverse applicazioni di

[10] Osserva B. ROMANO, *Algoritmi al potere. Calcolo giudizio pensiero*, Giappichelli, Torino, 2018, 21 ss., come non si tratti di una semplice "forza" esercitata dagli algoritmi, come le forze naturali cui gli esseri umani sono sottoposti, ma di una vera e propria forma di "potere", al servizio di soggetti che concepiscono e programmano questi strumenti algoritmici per obiettivi in grado di qualificare le relazioni sociali in una certa direzione. Di un nuovo tipo di "potenza" parla A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, cit., 67.

[11] Cfr. R. BODEI, *Dominio e sottomissione*, cit.

[12] Cfr. D. LYON, *La cultura della sorveglianza*, cit. È oggi diffusa l'espressione "*Algorithmic Society*", ripresa da J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data*, in *Faculty Scholarship Series*, 2017, 1219, per indicare "una società organizzata attorno a processi decisionali economici e sociali basati su algoritmi, robot, agenti di IA, che non assumono solo decisioni ma, in alcuni casi, le mettono in pratica" (trad. nostra).

TRF possono essere impiegate, fra cui le finalità del relativo ricorso, la composizione delle gallerie di immagini con cui operare il confronto, il livello minimo di accuratezza e affidabilità degli algoritmi di riconoscimento facciale, il periodo e le modalità di conservazione dei dati acquisiti, la possibilità di accesso e di trasferimento dei dati a soggetti esterni, le tecniche di verifica cui sottoporre il sistema, e così via[13]. Sul punto, occorre registrare una poco rassicurante carenza e confusione del quadro regolatorio italiano, data la vigenza di norme adottate sotto il vecchio regime della protezione dei dati, non pienamente allineate con la situazione attuale e all'altezza di queste tecnologie[14].

Il diritto è chiamato ad offrire una disciplina sufficientemente stringente per accordare tutela a diritti e interessi e a regolare gli aspetti in questione, ma anche sufficientemente ampia – sul punto, si è detto, "tecnologicamente neutrale" – per resistere ai mutamenti tecnologici[15]. Allo scopo, la prassi sulle TRF dimostra come le norme giuridiche siano chiamate ad offrire una cornice e ad orientare altri e più variegati strumenti regolativi per realizzare un regime "su misura" rispetto alle diverse specificità applicative di queste tecnologie[16]. Si tratta di forme regolative che variano a seconda di un differente grado di cogenza: minima nella auto-regolazione; orientativa nella *soft law*; che fa leva sulla adesione partecipata nella co-regolazione; che si impone con la forza delle pratiche e dei mercati negli standard tecnici; sino alla forza costrittiva del *design* dei sistemi di riconoscimento. Si tratta di forme regolative che variano anche a seconda del coinvolgimento dei destinatari stessi della regolazione: dall'affidamento completo ad essi nella auto-regolazione; alla dialettica pubblico-privato che si manifesta nella co-regolazione; alla necessaria collaborazione tra esperti tecnici e soggetti politicamente responsabili nella definizione del *design*; al coinvolgimento sperimentale di *stakeholders* e utenti nei diversi meccanismi di *governance*.

Come recentemente sintetizzato dal Garante europeo della prote-

[13] Cfr. *retro* Cap. III, par. 4. V. anche CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on Facial Recognition*, cit., 4.

[14] Cfr. *retro* Cap. III, par. 2.

[15] Cfr. *retro* Cap. V, par. 7.

[16] Cfr. *retro* Cap. V.

zione dei dati, il responsabile politico ha l'onere di indirizzare la regolazione verso un uso dei sistemi di sorveglianza biometrica, soprattutto da parte dei pubblici poteri, che sia "necessario per ragioni sostanziali di interesse pubblico, sulla base del diritto dell'UE o degli Stati, trasparente, responsabile, proporzionato allo scopo perseguito, soggetto a specifiche misure di salvaguardia, chiaramente limitato nel tempo e compatibile con l'essenza dei diritti fondamentali e il rispetto della dignità umana"[17].

In definitiva, quella indicata è parte della risposta che il diritto potrebbe offrire per evitare il realizzarsi degli scenari distopici contro cui la letteratura classica, la cinematografia e le serie televisive attuali mettono in guardia. La prospettiva costituzionale offre un riferimento imprescindibile per presidiare le libertà inviolabili e i processi di regolazione, affinché tecnologie innovative come quelle di riconoscimento facciale non contribuiscano a concretizzare mondi nuovi, e poco desiderabili.

[17] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust*, cit., p. 67 (trad. nostra), con riguardo ai sistemi biometrici di identificazione a distanza.

BIBLIOGRAFIA

Tutti gli indirizzi dei siti internet citati in precedenza e qui di seguito si intendono verificati al 1°aprile 2021.

AASHMI, SAHNI S., SAXENA S., *Survey: Techniques for Aging Problems in face recognition*, in *MIT International Journal of Computer Science and Information Technology*, 4, 2, agosto 2014, 82 ss.

ACCOTO C., *Il mondo dato. Cinque brevi lezioni di filosofia digitale*, Egea, Milano, 2017.

ACQUISTI A., GROSS R., STUTZMAN F., *Face recognition and privacy in the age of augmented reality*, in *Journal of Privacy and Confidentiality*, 6, 2, 2014, 1 ss.

ADEN H., *Interoperability Between EU Policing and Migration Databases: Risks for Privacy*, in *European Public Law*, 26, 1, 2020, 93 ss.

ADINOLFI A., *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in DORIGO S. (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini, Pisa, 2020, 13 ss.

ADLER P. ET AL., *Auditing Black-box Models for Indirect Influence*, in arXiv:1602.07043v2 [stat.ML], novembre 2016.

AHTEENSUU M., SANDIN P., *The Precautionary Principle*, in ROESER S., HILLERBRAND R., SANDIN P., PETERSON M. (a cura di), *Handbook of Risk Theory*, Springer, 2012, 961 ss.

AI HIGH LEVEL EXPERT GROUP, *A Definition of AI: Main Capabilities and Disciplines*, 9 aprile 2019.

AI HIGH LEVEL EXPERT GROUP, *Ethics Guidelines For Trustworthy AI*, 8 aprile 2019.

AI NOW INSTITUTE, *AI Now Report 2019*, dicembre 2019.

AI NOW INSTITUTE, *AI Now Report 2018*, dicembre 2018.

ALEGRE S., JEANDESBOZ J., VAVOULA N., *European Travel Information and Authorisation System (ETIAS): Border Management, Fundamental Rights and Data Protection*, *Study for the LIBE Committee*, PE 583.148, 2017.

ALEXANDRE L., *La guerra delle intelligenze. Intelligenza artificiale* contro *intelligenza umana*, EDT, Torino, 2018.

ALGOSTINO A., *La soft law comunitaria e il diritto statale: conflitto fra ordinamenti o fine del conflitto democratico?*, in *Costituzionalismo.it*, 3, 2016, 255 ss.

ALPA G., *La disciplina dei dati personali. Note esegetiche sulla Legge 31 dicembre 1996 n. 675 e successive modifiche*, SEAM, Formello, 1998.

ALPARSLAN Y. ET AL., *Adversarial Attacks on Convolutional Neural Networks in Facial Recognition Domain*, in *ar-Xiv:2001.11137v3 [cs.LG]*, 8 febbraio 2021.

ALLEGRETTI U., *Legge sull'ordine pubblico e libertà costituzionali*, in *Rivista trimestrale di diritto pubblico*, 1976, 472 ss.

AMATO G., *Art. 13*, in BRANCA G. (a cura di), *Commentario della Costituzione*, Zanichelli - Foro italiano, Bologna-Roma, 1977, 1 ss.

AMATO S., *Ai confini del corpo*, in AMATO S., CRISTOFARI F., RACITI S., *Biometria: i codici a barre del corpo*, Giappichelli, Torino, 2013, 1 ss.

AMATO MANGIAMELI A.C., *Algoritmi e big data. Dalla carta sulla robotica*, in *Rivista di filosofia del diritto*, 1, 2019, 107 ss.

AMOROSO D., TAMBURRINI G., *I sistemi robotici ad autonomia crescente tra etica e diritto: quale ruolo per il controllo umano?*, in *BioLaw Journal*, 1, 2019, 33 ss.

ANANNY M., CRAWFORD K., *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability*, in *New media & society*, 1, 2016.

ANDREJEVIC M., SELWYN N., *Facial Recognition Technology in Schools: Critical Questions and Concerns*, in *Learning, Media and Technology*, 2, 45, 2020, 115 ss.

ANJOS A., MARCEL S., *Counter-measures to photo attacks in face recognition: a public database and a baseline*, *International Joint Conference on Biometrics*, 2011, 1 ss.

ANTONINI L., *Art. 23 Cost.*, in CELOTTO A., BIFULCO R., OLIVETTI M. (a cura di), *Commentario alla Costituzione*, Utet, Torino, 2006, 484 ss.

ARCONZO G., *I diritti delle presone con disabilità. Profili costituzionali*, FrancoAngeli, Milano, 2020.

ARTICLE 29 WORKING PARTY, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, WP 211, 27 febbraio 2014.

ARTICLE 29 WORKING PARTY, *Opinion 02/2012 on facial recognition in online and mobile services*, WP 192, 22 marzo 2012.

ASIMOV I., *Circolo vizioso*, in *Astounding Science Fiction*, 1942, 100 ss.

ASTONE A., *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, GFL, Milano, 2019.

AZZARITI G., *Internet e Costituzione*, in *Costituzionalismo.it*, 2, 2011, 1 ss.

AZZARITI G., *Diritto e conflitti. Lezioni di diritto costituzionale*, Laterza, Roma-Bari, 2010.

BALDACCINI A., *Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases*, in *European Journal of Migration and Law*, 10, 2008, 31 ss.

BALDUZZI R., F. SORRENTINO, *Riserva di legge*, in *Enc. dir.*, XL, 1989, 1207 ss.

BALKIN J.M., *The Three Laws of Robotics in the Age of Big Data*, in *Faculty Scholarship Series*, 2017, 1217 ss.

BALZACQ T., *The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies*, in *Journal of Common Market Studies*, 46, 1, 2008, 75 ss.

BARBERA A., *I principi costituzionali della libertà personale*, Giuffrè, Milano, 1967.

BARBERA A., *Art. 2*, in BRANCA G. (a cura di), *Commentario della Costituzione*, Zanichelli - Foro italiano, Bologna-Roma, 1975, 50 ss.

BARBERA A., COCOZZA F., CORSO G., *Le situazioni soggettive. Le libertà dei singoli e delle formazioni sociali. Il principio di uguaglianza*, in AMATO G., BARBERA A. (a cura di), *Manuale di diritto pubblico*, I, il Mulino, Bologna, 1997, 223 ss.

BARFIELD W., *Towards a Law of Artificial Intelligence*, in BARFIELD W., PAGALLO U. (a cura di), *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar, Cheltenham, 2018, 2 ss.

BARILE P., *Diritti dell'uomo e libertà fondamentali*, il Mulino, Bologna, 1984.

BAROCAS S., SELBST A.D., *Big Data's Disparate Impact*, in *California Law Review*, 104, 2016, 671 ss.

BARRETT L., *Ban Facial Recognition Technologies For Children – And For Everyone Else*, in *Boston University Journal of Science & Technology Law*, 26, 2, 2020, 223 ss.

BARRETT L.F. ET AL., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, in *Psychological Science in the Public Interest*, 20, 1, 2019.

BARTLE I., VASS P., *Self-Regulation within the Regulatory State: Towards a New Regulatory Paradigm?*, in *Public Administration*, 85, 4, 2007, 885 ss.

BARTOLI R., *Diritto penale e prova scientifica*, in CANZIO G., LUPARIA L. (a cura di), *Prova scientifica e processo penale*, Milano, Wolters Kluwer-Cedam, 2018, 75 ss.

BARTOLI R., *La frode informatica tra modellistica, diritto vigente, diritto vivente e prospettive di riforma*, in *Il diritto dell'informazione e dell'informatica*, 3, 2011, 383 ss.

BECK U., *La società del rischio. Verso una seconda modernità*, Carocci, Roma, 2013.

BEDESSI S., *Intelligenza artificiale e fenomeni sociali. Previsioni con le reti neurali*, Maggioli, Santarcangelo di Romagna, 2019.

BENANTI P., *Le macchine sapienti, Intelligenze artificiali e decisioni umane*, Marinetti 1820, Bologna, 2018.

BENNETT C.J., BAYLEY R.M., *Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments*, in VAN DER SLOOT B., BROEDERS D., SCHRIJVERS E. (a cura di), *Exploring the Boundaries of Big Data*, Amsterdam University Press, The Hague-Amsterdam, 2016, 205 ss.

BENNETT K.A., *Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveillance Systems*, in *North Carolina Journal of Law & Technology*, 3, 1, 2001, 151 ss.

BENTHAM J., *Panopticon ovvero la casa d'ispezione*, Marsilio, Venezia, 1983.

BERLE I., *Face Recognition Technology. Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images*, Springer, Cham, 2020.

BERTOLINI A., *Artificial Intelligence and Civil Liability. Study requested by the JURI committee*, PE 621.926, luglio 2020.

BESTERS M., BROM F.W.A., *"Greedy" Information Technology: The Digitalization of the European Migration Policy*, in *European Journal of Migration & Law*, 12, 4, 2010, 462 ss.

BETZU M., *Anonimato e responsabilità in internet*, in *Costituzionalimo.it*, 2, 2011.

BIG BROTHER WATCH, *Face Off. The lawless growth of facial recognition in UK policing*, maggio 2018 [bit.ly/3uWtdyQ].

BIGNAMI M., *Chiacchiericcio sulle libertà costituzionali al tempo del coronavirus*, in *Questione Giustizia*, 7 aprile 2020.

BIN R., *Soft law, no law*, in SOMMA A. (a cura di), *Soft law e hard law nelle società postmoderne*, Giappichelli, Torino, 2009, 31 ss.

BINNS R., *Data protection impact assessments: a meta-regulatory approach*, in *International Data Privacy Law*, 7, 1, 2017, 22 ss.

BITTLE J., *Lie detectors have always been suspect. AI has made the problem worse*, in *MIT Technology Review*, 13 marzo 2020.

BLACK J., *Critical Reflections on Regulation*, in *Australian Journal of Law and Philosophy*, 1, 27, 2002, 1 ss.

BLACK J., *Decentring Regulation: Understanding the Role of Regulation and Self-regulation in a 'Post-regulatory' World*, in *Current Legal Problems*, 54, 1, 2001, 103 ss.

BLACK J., *Constitutionalising Self-Regulation*, in *Modern Law Review*, 59, 1, 1996, 24 ss.

BODEI R., *Dominio e sottomissione. Schiavi, animali, macchine, Intelligenza Artificiale*, il Mulino, Bologna, 2019.

BODEN M.A., *L'Intelligenza Artificiale*, il Mulino, Bologna, 2019.

BOGEN M., RIEKE A., *Help Wanted: An Examination Of Hiring Algorithms, Equity, And Bias*, in *Uptorn*, dicembre 2018.

BORGESIUS F.Z., *Discrimination, artificial intelligence, and algorithmic decision-making*, *Study for the Council of Europe*, 2018.

BORRELLI S., GUARISO A., LAZZERONI L., *Le discriminazioni nel rapporto di lavoro*, in BARBERA M., GUARISO A. (a cura di), *La tutela antidiscriminatoria*, Giappichelli, Torino, 2019, 165 ss.

BORRELLO R., *Riunione (diritto di)*, in *Enc. dir.*, XL, 1988, 1401 ss.

BRAITHWAITE J., BRAITHWAITE V., *The Politics of Legalism: Rules versus Standards in Nursing-Home Regulation*, in *Social and Legal Studies*, 4, 1995, 311 ss.

BRAVO F., *Le condizioni di liceità del trattamento di dati personali*,

in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia*, Zanichelli, Bologna, 2019, 110 ss.

BRENNAN-MARQUEZ K., *The Constitutional Limits of Private Surveillance*, in *Kansas Law Review*, 66, 2018, 485 ss.

BRIGHI R., *Dati informatici e modelli dei dati. Verso "una nuova dimensione della realtà"*, in BRIGHI R., ZULLO S. (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015, 281 ss.

BROGAN J.J., *Facing the Music: The Dubious Constitutionality of Facial Recognition Technology*, in *Hasting Communications and Entertainment Law Journal*, 25, 1, 2002, 65 ss.

BROUWER E., *Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection*, in *European public law*, 26, 1, 2020, 71 ss.

BROWNSWORD R., *Law, Technology and Society. Re-imagining the Regulatory Environment*, Routledge, Abingdon-New York, 2019.

BROWNSWORD R., YEUNG K. (a cura di), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Hart Publishing, Oxford, 2008.

BRUGI M., *Dall'identità personale all'identità digitale*, in *Informatica e diritto*, 1-2, 2008, 167 ss.

BRYSON J.J., *The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation*, in DUBBER M., PASQUALE F., DAS S. (a cura di), *The Oxford Handbook of Ethics of Artificial Intelligence*, Oxford University Press, Oxford, 2019, 1 ss.

BRYSON J.J., THEODOROU A., *How Society Can Maintain Human-Centric Artificial Intelligence*, in TOIVONEN M., SAARI E. (a cura di), *Human-Centered Digitalization and Services*, Springer, 2019, 305 ss.

BUCALO E., *Autorità indipendenti e* soft law*. Forme, contenuti, limiti e tutele*, Giappichelli, Torino, 2018.

BUFFONI L., *Processo e pluralismo nell'ordinamento costituzionale italiano. Apologia e limiti dell'universalismo procedurale*, Jovene, Napoli, 2012.

BUFFONI L., CARDONE A., *Il procedimento normativo precauzionale come caso paradigmatico del ravvicinamento "formale-procedurale" delle "fonti" del diritto*, in *Osservatorio sulle fonti*, 3, 2012.

BUOLAMWINI J., GEBRU T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proceedings of Machine Learning*, 81, 2018, 77 ss.

BUTTARELLI G., *Banche dati e tutela della riservatezza. La* privacy *nella Società dell'informazione*, Giuffrè, Milano, 1997.

BURR C., CRISTIANINI N., *Can Machines Read our Minds?*, in *Minds and Machines*, 29, 3, 2019, 461 ss.

BURRELL J., *How the machine 'thinks': Understanding opacity in machine learning algorithms*, in *Big Data & Society*, 3, 1, 2016, 1 ss.

BUSIA G., *Riservatezza (diritto alla)*, in *Dig. disc. pubbl.*, Agg. I, 2000, 476 ss.

BUSNELLI F.D., *La persona alla ricerca dell'identità*, in *Rivista critica del diritto privato*, 1, 2010, 7 ss.

BYGRAVE L.A., *The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects*, in *Computer Law & Security Review*, 40, 2021, in corso di pubblicazione.

CAFAGGI F., *New foundation of transnational private regulation*, in *Journal of Law and Society*, 38, 1, 2011, 20 ss.

CAGGIANO G., *L'interoperabilità fra le banche dati dell'Unione sui cittadini degli Stati terzi*, in *Diritto, Immigrazione e Cittadinanza*, 1, 2020, 170 ss.

CALIFANO L., *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, in CALIFANO L., COLAPIETRO C. (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli, 2017, 3 ss.

CALIFANO L., *Tecnologie di controllo del lavoro, diritto alla riservatezza e orientamenti del Garante per la protezione dei dati personali*, in TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati del lavoratore*, Giappichelli, Torino, 2017, 165 ss.

CALIFANO L., *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale Scientifica, Napoli, 2016.

CALO R., *Artificial Intelligence Policy: A Primer and Roadmap*, in *University of California, Davis Law Review*, 51, 2017, 399 ss.

CALO R., *Robotics and the Lessons of Cyberlaw*, in *California Law Review*, 103, 2015, 513 ss.

CALO R., *Code, Nudge, or Notice?*, in *Iowa Law Review*, 99, 2014, 773 ss.

CALO R., *Digital Market Manipulation*, in *George Washington Law Review*, 82, 2014, 995 ss.

CALZOLAIO S., *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *Federalismi.it*, 24, 2017.

CALZOLAIO S., *Protezione dei dati personali*, in *Dig. Disc. Pubbl.*, Agg. VII, 2017, 594 ss.

CAMPBELL F., *Data Scraping – What Are the Privacy Implications*, in *Privacy & Data Protection*, 20, 1, 2019, 3 ss.

CANCA C., *Human Rights and AI Ethics – Why Ethics Cannot be Replaced by the UDHR*, in *United Nations University: AI & Global Governance Articles & Insights*, luglio 2019.

CANEPA A., *I mercanti nell'era digitale. Un contributo allo studio delle piattaforme*, Giappichelli, Torino, 2020.

CARAVITA DI TORITTO B., *Principi costituzionali e intelligenza artificiale*, in RUFFOLO U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, GFL, Milano, 2020, 451 ss.

CARDON D., *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei* big data, Mondadori, Milano, 2016.

CARDONE A., *La tutela multilivello dei diritti fondamentali*, Giuffrè, Milano, 2012.

CARDONE A., *La «normalizzazione» dell'emergenza. Contributo allo studio del potere* extra ordinem *del Governo*, Giappichelli, Torino, 2011.

CARETTI P., *A ottant'anni dalle leggi razziali: non solo memoria*, in *Lo Stato*, 6, 2018, 1 ss.

CARETTI P., *Comunicazione e informazione*, in *Enc. dir.*, Ann. I, 2007, 218 ss.

CARETTI P. (a cura di), *Osservatorio sulle fonti 2003-2004. I poteri normativi delle autorità indipendenti*, Giappichelli, Torino, 2004.

CARETTI P., *La libertà personale*, in SANTANIELLO G. (diretto da), *Trattato di diritto amministrativo*, XII, Cedam, Padova, 1990, 7 ss.

CARETTI P., CARDONE A., *Diritto dell'informazione e della comunicazione nell'era della convergenza. Stampa, radiotelevisione, telecomunicazioni, internet, teatro e cinema*, il Mulino, Bologna, 2019.

CARETTI P., TARLI BARBIERI G., *I diritti fondamentali. Libertà e diritti sociali*, Giappichelli, Torino, 2017.

CARLASSARE L., *Legalità (principio di)*, in *Enc. giur.*, XVIII, 1990.

CARLASSARE L., *Legge (riserva di)*, in *Enc. giur.*, XVIII, 1990.

CARLETTI C., *Diritto alla riservatezza, protezione dei dati personali e spazio digitale nell'ordinamento internazionale*, Editoriale Scientifica, Napoli, 2020.

CARROZZA M.C. ET AL., *AI: profili tecnologici. Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'Intelligenza Artificiale*, in *BioLaw Journal*, 3, 2019, 237 ss.

CARUANA M.M., *The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement*, in *International Review of Law, Computers & Technology*, 33, 3, 2017, 249 ss.

CASONATO C., *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, in *BioLaw Journal*, Special Issue 2, 2019, 711 ss.

CASONATO C., *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Dir. pubb. comp. eur.*, f.s., 2019, 101 ss.

CATH C., WACHTER S., MITTELSTADT B., TADDEO M., FLORIDI L., *Artificial Intelligence and the 'Good Society': the US, EU, and UK approach*, in *Sci Eng Ethics*, 24, 2018, 505 ss.

CAUSARANO M.C., *GDPR e forme di autoregolamentazione privata: continuità e discontinuità nella disciplina dei codici di condotta*, in MANTELERO A., POLETTI D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, PUP, Pisa, 2018, 247 ss.

CAVOUKIAN A., *Privacy By Design: The 7 Foundational Principles*, 2011 [bit.ly/2Rgxped].

CELOTTO A., *Come regolare gli algoritmi. Il difficile bilanciamento tra scienza, etica e diritto*, in *Analisi giuridica dell'Economia*, 1, 2019, 47 ss.

CELOTTO A., *Art. 3, 1° comma*, in CELOTTO A., BIFULCO R., OLIVETTI M. (a cura di), *Commentario alla Costituzione*, cit., 65 ss.

CERRI A., *Riservatezza (diritto alla). Diritto costituzionale*, in *Enc. giur.*, XXVII, 1995.

CERRI A., *Uguaglianza (principio costituzionale di)*, in *Enc. giur.*, XXXII, 1994.

CERRI A., *Libertà personale (dir. cost.)*, in *Enc. giur.*, XXI, 1991.

CERRI A., *Riservatezza (diritto alla). Diritto comparato e straniero*, in *Enc. giur.*, XXVII, 1991.

CHELI E., *Libertà di informazione e pluralismo informativo negli indirizzi della giurisprudenza costituzionale*, in PISANESCHI A., VIOLINI L. (a cura di), *Poteri, garanzie e diritti. A sessanta anni dalla Costituzione. Scritti per Giovanni Grottanelli de' Santi*, Giuffrè, Milano 2007, 1405 ss.

CHEN Z., WHITNEY D., *Tracking the Affective State of Unseen Persons*, *Proceedings of the National Academy of Sciences*, 116, 15, 2019, 7559 ss.

CHERCHI R., DEFFENU A., *Fonti e provvedimenti dell'emergenza sanitaria covid-19: prime riflessioni*, in *Diritti regionali*, *Forum "La gestione dell'emergenza sanitaria tra Stato, Regioni ed Enti locali"*, 23 aprile 2020, 648 ss.

CHESTERMAN S., *One nation under surveillance: a new social contract to defend freedom without sacrificing liberty*, Oxford University Press, Oxford, 2011.

CINGOLANI R., *L'altra specie. Otto domande su noi e loro*, il Mulino, Bologna, 2019.

CIPOLLA P., "*Social network*", *furto di identità e reati contro il patrimonio*, in *Giurisprudenza di merito*, 2012, 12, 2672 ss.

CITRON D.K., *Tecnological Due Process*, in *Washington University Law Rev*, 85, 2008, 1249 ss.

CITRON D.K., PASQUALE F., *The Scored Society: Due Process for Automated Predictions*, in *Washington Law Review*, 89, 2014, 1 ss.

CLARKE R., *Information Technology and Dataveillance*, in *Communications of ACM*, 5, 31, maggio 1988, 498 ss.

COGLIANESE C., MENDELSON E., *Meta-Regulation and Self-Regulation*, in CAVE M., BALDWIN R., LODGE M. (a cura di), *The Oxford Handbook on Regulation*, Oxford University Press, Oxford, 2010, 146 ss.

COHEN J.E., *Examined Lives: Informational Privacy and the Subject as Object*, in Stanford Law Review, 52, 5, 2000, 1373, ss.

COHN J.F., DE LA TORRE F., *Automated Face Analysis for Affective Computing*, in CALVO R.A., D'MELLO S.K., GRATCH J., KAPPAS A. (a cura di), *The Oxford Handbook of Affective Computing*, OUP, Oxford, 211 ss.

COLAPIETRO C., *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 22, 2018.

COLAPIETRO C., *Diritti dei disabili e Costituzione*, Editoriale Scientifica, Napoli, 2011.

COLAPIETRO C., MORETTI A., *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali stampato*, in *BioLaw Journal*, 3, 2020, 359 ss.

COLAPIETRO C., IANNUZZI A., *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in CALIFANO L., COLAPIETRO C. (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, cit., 85 ss.

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, 2.0, 29 gennaio 2020.

COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, 26 novembre 2010.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Facial recognition: for a debate living up to the challenges*, 19 dicembre 2019 [bit.ly/3dBUO0Y].

COMMISSIONE DELLE CE, *Comunicazione della Commissione sul principio di precauzione*, COM(2000) 1 final, 2 febbraio 2000.

CONSIGLIO E., *Che cosa è la discriminazione? Un'introduzione teorica al diritto antidiscriminatorio*, Giappichelli, Torino, 2020.

CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on Facial Recognition*, T-PD(2020)03rev4, 28 gennaio 2021.

CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Facial Recognition: Current Situation and Challenges*, by S. Azria and F. Wickert, T-PD(2019)05rev, 13 novembre 2019.

CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on Artificial Intelligence and Data Protection*, T-PD(2017)01, 25 gennaio 2019.

CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Report on Artificial Intelligence*, by A. Mantelero, T-PD(2018)09Rev, gennaio 2019.

CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Practical guide on the use of personal data in the police sector*, T-PD(2018)01, 15 febbraio 2018.

CONTI C., *Scienza controversa e processo penale: la Cassazione e il "discorso sul metodo"*, in *Diritto penale e processo*, 6, 2019, 848 ss.

CONTI C., *Prova informatica e diritti fondamentali*, in *Diritto penale e processo*, 9, 2018, 1210 ss.

CONTI S., PERUGINELLI G., *L'impatto del regolamento europeo in materia di protezione dei dati personali sull'attività giurisdizionale*, in *Ciberspazio e Diritto*, 1-2, 2018, 123 ss.

CONTISSA G., *Information technology for the law*, Giappichelli, Torino, 2017.

COOK C.M., HOWARD J.J., SIROTIN Y.B., TIPTON J.L., VEMURY A.R., *Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems*, in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 1, 1, 2018, 32 ss.

CORDERO F., *Procedura penale*, Giuffrè, Milano, 2012.

COSTANTINI F., FRANCO G., *Decisione automatizzata, dati personali e pubblica amministrazione in Europa: verso un "*Social credit system*"?*, in *Istituzioni del Federalismo*, 3, 2019, 715 ss.

CRISAFULLI V., *Lezioni di diritto costituzionale*, II, 1, *L'ordinamento costituzionale italiano (le fonti normative)*, Cedam, Padova, 1993.

CUNIBERTI M., *Democrazie, dissenso politico e tutela dell'anonimato*, in *Il Diritto dell'informazione e dell'informatica*, 2, 2014, 111 ss.

D'ACQUISTO G., NALDI M., *Big data e privacy by design. Anonimizzazione. Pseudonimizzazione. Sicurezza*, Giappichelli, Torino, 2017.

D'ALOIA A., *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal*, 1, 2019, 3 ss.

D'AMICO M., *Una parità ambigua. Costituzione e diritti delle donne*, Raffaello Cortina Editore, Milano, 2020.

D'AMICO M., *Articolo 3*, in CLEMENTI F., CUOCOLO L., ROSA F., VIGEVANI G.E. (a cura di), *La Costituzione italiana. Commento articolo per articolo*, I, il Mulino, Bologna, 2018, 28 ss.

D'ANTONIO V., *Oblio e cancellazione dei dati nel diritto europeo*, in SICA S., D'ANTONIO V., RICCIO G.M. (a cura di), *La nuova disciplina europea della privacy*, Wolters Kluver - Cedam, Milano, 2016, 197 ss.

DAVIES B., INNES M., DAWSON A., *An evaluation of South Wales Police's use of Automated Facial Recognition*, Cardiff University, settembre 2018.

DE BÙRCA G., *The principle of proportionality and its application in EC law*, in *Yearbook of European law*, 13, 1993, 13 ss.

DE CUPIS A., *I diritti della personalità*, in CICU A., MESSINEO F. (diretto da), *Trattato di diritto civile e commerciale*, IV, I, Giuffrè, Milano, 1973.

DE GREGORIO G., TORINO R., *Privacy, protezione dei dati personali e big data*, in TOSI E. (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, GFL, Milano, 2019, 447 ss.

DE HERT P., GUTWIRTH S., *Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action*, in GUTWIRTH S., POULLET Y., HERT P.D., NOUWT J., TERWANGNE C.D. (a cura di), *Reinventing data protection?*, Springer, Berlino, 2009, 3 ss.

DE HERT P., PAPAKONSTANTINOU V., *Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should' to 'must' via* soft law *to address more than only individual harms*, in *Computer Law & Security Review*, 40, 2021, in corso di pubblicazione.

DE HERT P., PAPAKONSTANTINOU V., *The new police and criminal justice data protection directive: A first analysis*, in *New journal of European criminal law*, 7, 1, 2016, 7 ss.

DE HERT P., PAPAKONSTANTINOU V., *The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area*, *Study for the LIBE Committee*, PE 510.001, 2014.

DE MINICO G., *Towards an "Algorithm Constitutional by Design"*, in *BioLaw Journal*, 1, 2021, 381 ss.

DE MINICO G., Big Data *e la debole resistenza delle categorie giuridiche*. Privacy *e* lex mercatoria, in *Diritto pubblico*, 1, 2019, 89 ss.

DE PASQUALE P., *Verso la refusione del regolamento «Dublino III»*, in *Studi sull'integrazione europea*, 2018, 2, 267 ss.

DE SIERVO U., *Tutela dei dati personali e riservatezza*, in AA.VV., *Diritti. Nuove tecnologie. Trasformazioni sociali. Scritti in memoria di Paolo Barile*, Cedam, Padova, 2003, 297 ss.

DE SIERVO U., *La libertà di associazione*, in SANTANIELLO G. (diretto da), *Trattato di diritto amministrativo*, XII, Cedam, Padova, 1990, 191 ss.

DE TERWANGN C., *Council of Europe convention 108 +: A modernised international treaty for the protection of personal data*, in *Computer Law & Security Review*, 40, 2021, in corso di pubblicazione.

DE VANNA F., *Diritto e nuove tecnologie: il nodo (controverso) della regolazione giuridica*, in *Lo Stato*, 11, 2018, 387 ss.

DECLI F., MARANDO G., *Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia*, in PERONI F., GIALUZ M. (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, EUT, Trieste, 2009, 101 ss.

DEGOLI M.C., *I trattamenti in ambito lavorativo*, in SCAGLIARINI S. (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali*, Giappichelli, Torino, 2019, 243 ss.

DEL FEDERICO C., *Il trattamento dei dati personali relativi all'istruzione*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia*, cit., 873 ss.

DEL PUNTA R., *Diritto del lavoro*, GFL, Milano, 2020.

DEL PUNTA R., *La nuova disciplina del controllo a distanza sul lavoro (art. 23 d.lgs. n. 151/2015)*, in *Rivista italiana di diritto del lavoro*, 1, 2016, 77 ss.

DELLA TORRE J., *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della* High Court of Justice, in *Diritto Penale Contemporaneo*, 1, 2020, 231 ss.

DELMASTRO M., NICITA A., *Big data*, il Mulino, Bologna, 2019.

DELOITTE, *Study on the Feasibility of Improving Information Exchange under the Prüm Decisions. Advanced technical report*, maggio 2020.

DEMETZOU K., *Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation*, in *The computer law and security report*, 35, 6, 2019.

DETERMANN L., *Adequacy of data protection in the USA: myths and facts*, in *International Data Privacy Law*, 6, 3, 2016, 245 ss.

DEWAN M.A.A., MURSHED M., LIN F., *Engagement Detection in Online Learning: A Review*, in *Smart Learning Environments*, 6, 1, 2019, 1 ss.

DI CHIARA G., *L'imputato e il diritto di difesa: il telaio dell'art. 24 Cost. e il "nuovo" catalogo dei diritti dell'"accusato"*, in FIANDACA G.,

DI CHIARA G., *Una introduzione al sistema penale. Per una lettura costituzionalmente orientata*, Jovene, Napoli, 2003, 269 ss.

DI GENIO G., *Trasparenza e accesso ai dati personali*, in SICA S., D'ANTONIO V., RICCIO G.M. (a cura di), *La nuova disciplina europea della privacy*, cit., 161 ss.

DI PORTO F., ZUPPETTA M., *Co-regulating algorithmic disclosure for digital platforms*, in *Policy and Society*, 2020.

DI ROBILANT A., *Genealogies of Soft Law*, in *The American Journal of Comparative Law*, 54, 3, 2006, 499 ss.

DI MARTINO A., *Profili costituzionali della privacy in Europa e negli Stati Uniti*, Jovene, Napoli, 2017.

DIGNUM V. ET AL., *Ethics by Design: necessity or curse?*, in *AIES 2018. Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, 2018, 60 ss.

DOGLIANI M., GIORGI C., *Articolo 3. Costituzione italiana*, Carocci, Roma, 2017.

DONATI F., *Intelligenza artificiale e giustizia*, in *Rivista AIC*, 1, 2020, 415 ss.

DOURISH P., *Algorithms and their others: Algorithmic culture in context*, in *Big Data & Society*, 3, 2, 2016.

DRUETTA G., 9. *Trattamento di categorie particolari di dati personali*, in RICCIO G.M., SCORZA G., BELISARIO E. (a cura di), GDPR e normativa privacy. Commentario, Wolkers Kluwer, Milano, 2018, 93 ss.

DUQUE DE CARVALHO S.L., *Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108*, in *European data protection law review*, 5, 1, 2019, 54 ss.

EBERS M., *Regulating AI and Robotics: Ethical and Legal Challenges*, in EBERS M., NAVAS NAVARRO S. (a cura di), *Algorithms and Law*, Cambridge University Press, Cambridge, 2020, 37 ss.

EDWARDS L., VEALE M., *Enslaving the algorithm: from a 'right to an explanation' to a 'right to better decisions'?*, in *SSRN Electronic Journal*, gennaio 2017.

EDWARDS L., VEALE M., *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You are Looking for*, in *Duke Law & Technology Review*, 16, 1, 2017.

ELIA L., *Libertà personale e misure di prevenzione*, Giuffrè, Milano, 1962.

ELLERBROK A., *Playful biometrics: controversial technology through the lens of play*, in *Sociological Quarterly*, 52, 2011, 528 ss.

ELLIOT J.E., *Marx and Schumpeter on Capitalism's Creative Destruction: A Comparative Restatement*, in *The Quarterly Journal of Economics*, 95, 1, 1980, 45 ss.

ESPOSITO C., *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Giuffrè, Milano, 1958.

EUROPEAN COMMISSION, *A European strategy for data*, COM(2020) 66 final, 19 febbraio 2020.

EUROPEAN COMMISSION, White Paper "*On Artificial Intelligence - A European approach to excellence and trust*", COM(2020) 65 final, 19 febbraio 2020.

EUROPEAN COMMISSION, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, COM(2020) 64 final, 19 febbraio 2020.

EUROPEAN COMMISSION, Communication "*Shaping Europe's digital future*", COM(2020) 67 final, 19 febbraio 2020.

EUROPEAN COMMISSION, Communication "*Building Trust in Human-Centric Artificial Intelligence*", COM(2019) 168 final, 8 aprile 2019.

EUROPEAN COMMISSION, Communication "*Coordinated Plan on Artificial Intelligence*", COM(2018) 795 final, 7 dicembre 2018.

EUROPEAN COMMISSION, Communication "*Artificial Intelligence for Europe*", COM(2018) 237 final, 25 aprile 2018.

EUROPEAN COMMISSION, JRC, *AI Watch. Defining Artificial Intelligence*, 2020.

EUROPEAN DATA PROTECTION BOARD, *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, 12 febbraio 2019.

EUROPEAN DATA PROTECTION SUPERVISOR, *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, 19 dicembre 2019.

EUROPEAN DATA PROTECTION SUPERVISOR, *Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice*, 17 novembre 2017.

EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOL-

OGIES, *Artificial Intelligence, Robotics and 'Autonomous' Systems*, 9 marzo 2018.

Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations, Congressional Research Service (R46541), settembre 2020 [bit.ly/3msK3Ca].

FAINI F., *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, GFL, Milano, 2019.

FAINI F., *Diritto all'esistenza digitale*, in *BioLaw Journal*, 3, 2019, 91 ss.

FANTI V., *La trasparenza amministrativa tra principi costituzionali e valori dell'ordinamento europeo: a margine di una recente sentenza della Corte costituzionale (n. 20/2019)*, in *Federalismi.it*, 5, 2020, 34 ss.

FANUELE C., *L'acquisizione occulta di materiale biologico*, in SCALFATI A. (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2014, 311 ss.

FARO S., *Trattamento dei dati personali e tutela della persona*, in *Dig. disc. pubbl.*, Agg. I, Torino, 2000, 543 ss.

FASAN M., *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in *BioLaw Journal*, 1, 2019, 101 ss.

FAVILLI C., *La politica dell'Unione in materia d'immigrazione e asilo. Carenze strutturali e antagonismo tra gli Stati membri*, in *Quad. cost.*, 2, 2018, 361 ss.

FEDELE A., *Art. 23*, in BRANCA G. (a cura di), *Commentario della Costituzione*, Zanichelli - Foro italiano, Bologna-Roma, 1978, 21 ss.

FEDERAL TRADE COMMISSION, *Facing Facts: Best practices for common uses of facial recognition technologies*, ottobre 2012 [bit.ly/2PIE68o].

FELICIONI P., *La prova del DNA nel procedimento penale. Profili sistematici, dinamiche probatorie, suggestioni mediatiche*, Giuffrè, Milano, 2018.

FELICIONI P., *Art. 188*, in GIARDA A., SPANGHER G. (a cura di), *Codice di procedura penale commentato*, I, Wolters Kluwer, Milano, 2017, 1872 ss.

FELICIONI P., *L'acquisizione di materiale biologico a fini identificativi o di ricostruzione del fatto*, in SCARCELLA S. (a cura di), *Prelievo del D.N.A. e Banca dati nazionale*, Padova, 2009, 191 ss.

FELICIONI P., *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Ipsoa, Assago, 2007.

FENWICK M.D., KAAL W.A., VERMEULEN E.P.M., *Regulation Tomorrow: What Happens When Technology is Faster Than the Law?*, in *American University Business Law Review*, 6, 3, 2017, 591 ss.

FERRARIS V., *Il migrante datificato nei confini del futuro: senza potere di fronte a un oscuro potere?*, in GOZZO S., PENNISI C., ASERO V., SAMPUGNARO R. (a cura di), *Big Data e processi decisionali. Strumenti per l'analisi delle decisioni giuridiche, politiche economiche e sociali*, Egea, Milano, 2020, 135 ss.

FERRARIS V., *Eurodac e i limiti della legge: quando il diritto alla protezione dei dati personali non esiste*, in *Diritto, Immigrazione e Cittadinanza*, 2, 2017, 1 s.

FERRARIS V., *La profilazione e i suoi rischi*, in BRIGHI R., ZULLO S. (a cura di), *Filosofia del diritto e nuove tecnologie*, cit., 69 ss.

FILIPPETTA G., *La libertà personale e le libertà di domicilio, di circolazione e individuale*, in NANIA R., RIDOLA P. (a cura di), *I diritti costituzionali*, II, Giappichelli, Torino, 2006, 601 ss.

FINALE D., KIM B., *A Roadmap for a Rigorous Science of Interpretability*, in arXiv:1702.08608v2, marzo 2017.

FINOCCHIARO G., *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in EAD. (a cura di), *La protezione dei dati personali in Italia*, cit., 1 ss.

FINOCCHIARO G., *Anonimato*, in *Dig. disc. priv., sez. civ.*, Agg. V, 2010, 12 ss.

FINOCCHIARO G., *Identità personale (diritto alla)*, *Dig. disc. priv., sez. civ.*, Agg. V, 2010, 721 ss.

FINOCCHIARO G. (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, in GALGANO F. (diretto da), *Trattato di diritto commerciale e di diritto pubblico dell'economia*, XLVIII, Cedam, Padova, 2008.

FIORILLO V., *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di giustizia dell'Unione europea*, in *Federalismi.it*, 15, 2017.

FLORIDI L., *Soft Ethics and the Governance of the Digital*, in *Philosophy & Technology*, 31, 1, 2018.

FLORIDI L., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano, 2014.

FOIS S., *"Delegificazione", "riserva di legge" e principio di legalità*, in AA.VV. *Studi in onore di Manlio Mazziotti di Celso*, I, Cedam, Padova, 1995, 727 ss.

FORGÓ N., HÄNOLD S., SCHU□TZE B., *The Principle of Purpose Limitation and Big Data*, in CORRALES M., FENWICK M., FORGÓ N. (a cura di), *New Technology, Big Data and the Law*, Springer, Singapore, 2017, 17 ss.

FORMICI G., *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in *DPCE online*, 2, 2019, 1107 ss.

FOSCH VILLARONGA E., GOLIA A. JR, *Robots, standards and the law: Rivalries between private standards and public policymaking for robot governance*, in *Computer Law & Security Review*, 35, 2, 2019, 129 ss.

FOUCAULT M., *Sorvegliare e punire. Nascita della prigione*, Einaudi, Torino, 1993.

FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27 novembre 2019 [bit.ly/3uvgMd1].

FRA, *Preventing unlawful profiling today and in the future: a guide*, dicembre 2018 [bit.ly/2Rl1469].

FRA, *Opinion 1/2018. Interoperability and fundamental rights implications*, 11 aprile 2018 [bit.ly/3223HeR].

FRA, *Under watchful eyes – biometrics, EU IT-systems and fundamental rights*, 2018 [bit.ly/3utdmaL].

FROSINI T.E., *Costituzionalismo 2.0*, in *Rassegna parlamentare*, 4, 2016, 675 ss.

FROSINI V., *Informatica, diritto e società*, Giuffrè, Milano, 1992.

FUSIELLO A., *Visione computazionale: Tecniche di ricostruzione tridimensionale*, FrancoAngeli, Milano, 2018.

FUTURE OF PRIVACY FORUM, *Privacy Principles for Facial Recognition Technology in Commercial Applications*, settembre 2018 [bit.ly/31UvpdF].

GAJA G., *The Charter of Fundamental Rights in the Context of International Instruments for the Protection of Human Rights*, in *European Papers*, 1, 3, 2016, 791 ss.

GALBALLY J., FERRARA P., HARAKSIM R., PSYLLOS A., BESLAY L., *Study on Face Identification Technology for its Implementation in the Schengen Information System*, JRC-34751, luglio 2019.

GALETTA D.-U., *Il principio di proporzionalità fra diritto nazionale e diritto europeo (e con uno sguardo anche al di là dei confini dell'Unione europea)*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 6, 2019, 907 ss.

GALETTA D.-U., CORVALÁN J.G., *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 3, 2019.

GALIČ M., TIMAN T., KOOPS B.-J., *Bentham, Deleuze and Beyond: an Overview of Surveillance Theories from the Panopticon to Participation*, in *Philosophy & Technology*, 30, 1, 2017, 9 ss.

GALLI F., *Interoperable Databases: New Cooperation Dynamics in the EU AFSJ?*, in *European public law*, 26, 1, 2020, 109 ss.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento generale prescrittivo in tema di biometria*, 12 novembre 2014.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee-guida in materia di riconoscimenti biometrico e firma grafometrica. Allegato A al Provvedimento del Garante del 23 novembre 2014*, 12 novembre 2014.

GAROFANO P., *Le attività tecniche: dal prelievo alla banca dati del DNA*, in SCARCELLA S. (a cura di), *Prelievo del D.N.A. e Banca dati nazionale*, Cedam, Padova, 2009, 79 ss.

GARVIE C. ET AL., *The Perpetual Line-Up. Unregulated Police Face Recognition in America*, *Georgetown Center on Privacy & Technology*, 18 ottobre 2016 [bit.ly/3t05PQm].

GATES K.A., *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance,* New York, NYU Press, 2011.

GIACOMELLI L., *Ripensare l'eguaglianza. Gli effetti collaterali della tutela antidiscriminatoria*, Giappichelli, Torino, 2018.

GIALUZ M., *Principio di accessibilità e banche dati di "primo pilastro"*, in PERONI F., GIALUZ M. (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, EUT, Trieste, 2009, 139 ss.

GIANNANTONIO E., *Dati personali (tutela dei)*, in *Enc. dir.*, Agg. III, 1999, 483 ss.

GIANNONE CODIGLIONE G., Risk-based approach *e trattamento*

dei dati personali, in SICA S., D'ANTONIO V., RICCIO G.M. (a cura di), *La nuova disciplina europea della privacy*, cit., 55 ss.

GILAD S., *It runs in the family: Meta-regulation and its siblings*, in *Regulation & Governance*, 4, 4, 2010, 485 ss.

GIOCOLI NACCI P., *Libertà di riunione*, in SANTANIELLO G. (diretto da), *Trattato di diritto amministrativo*, XII, cit., 157 ss.

GIORGIS A., *Art. 3, 2° comma*, in CELOTTO A., BIFULCO R., OLIVETTI M. (a cura di), *Commentario alla Costituzione*, cit., 88 ss.

GIUPPONI T.F., *La sicurezza e le sue "dimensioni" costituzionali*, in S. VIDA (a cura di), *Diritti umani. Trasformazioni e reazioni*, BUP, Bologna, 2008, 275 ss.

GOODMAN B., FLAXMAN S., *European Union Regulations on algorithmic decision-making and a "Right to Explanation"*, in *AI Magazine*, 38, 3, 2017.

GOOGLE AI, *Our approach to facial recognition* [bit.ly/3uo7Whc].

GOOGLE, *AI Principles 2020. Progress update* [bit.ly/2PMlBjt].

GÖTZMANN N., BANSAL T., WRZONCKI E., POULSEN-HANSEN C., TEDALDI J., HØVSGAARD R., *Human Rights Impact Assessment. Guidance and Toolbox*, The Danish Institute for Human Rights, 2016.

GRASSI S., *Prime osservazioni sul "principio di precauzione" come norma di diritto positivo*, in *Dir. gest. amb.*, 1, 2001, 37 ss.

GRASSO G., *Le autorità amministrative indipendenti della Repubblica. Tra legittimità costituzionale e legittimazione democratica*, Giuffrè, Milano, 2006.

GRATTERI A., SACCO G.A., *Senza distinzione. Per il superamento della parola razza*, in *Nomos*, 2, 2018.

GRAZIADEI M., *La regolazione del rischio e il principio di precauzione: Stati Uniti ed Europa a confronto*, in *Sistemi intelligenti*, 2, 2017, 499 ss.

GREEN B, CHEN Y., *Disparate Interactions: An Algorithm-in-the-Loop Analysis of Fairness in Risk Assessments*, *Conference on Fairness, Accountability, and Transparency (FAT* '19), 29–31 gennaio 2019*.

GREENWALD G., *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, Rizzoli, Milano, 2014.

GROPPI T., *Alle frontiere dello stato costituzionale: innovazione tecnologica e intelligenza artificiale*, in *Consulta Online*, 3, 2020, 675 ss.

GROSSI P., *L'Europa del diritto*, Laterza, Roma-Bari, 2007.

GROTHER P., NGAN M., HANAOKA K., *Face Recognition Vendor Test (FRVT). Part 1: Verification*, NIST, 18 dicembre 2020 [bit.ly/3mwlBjE].

GROTHER P., NGAN M., HANAOKA K., *Face Recognition Vendor Test (FRVT). Part 2: Identification*, NIST, dicembre 2020, [bit.ly/39RPGFf].

GROTHER P. ET AL., *Face Recognition Vendor Test (FRVT) Part 5: Face Image Quality Assessment*, Draft NIST Interagency Report, 6 marzo 2020.

GROTHER P., NGAN M., HANAOKA K., *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*, NIST, dicembre 2019 [bit.ly/3s5p89O].

GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679*, 11 aprile 2018.

GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, 10 aprile 2018.

GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 6 febbraio 2018.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, WP 258, 29 novembre 2017.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 2/2017 sul trattamento dei dati sul posto di lavoro*, WP 249, 8 giugno 2017.

GRUPPO DI LAVORO ARTICOLO 29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, 4 aprile 2017.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 03/2015 sulla proposta di direttiva concernente la tutela 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, e la libera circolazione di tali dati*, WP233, 1 dicembre 2015.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI,

Parere 3/2012 sugli sviluppi nelle tecnologie biometriche, WP193, 27 aprile 2012.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile*, WP 192, 22 marzo 2012.

GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2010 sul principio di responsabilità*, WP 173, 13 luglio 2010.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 4/2007 sul concetto di dati personali*, WP 136, 20 giugno 2007.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 4/2004 relativo al trattamento dei dati personali mediante videosorveglianza*, WP89, 11 febbraio 2004.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Documento di lavoro sulla biometria*, WP 80, 1 agosto 2003.

GUASTINI R., *Teoria e dogmatica delle fonti*, Giuffrè, Milano, 1998.

GUASTINI R., *Legge (riserva di)*, in *Dig. disc. pubbl.*, IX, 1997, 163 ss.

GUASTINI R., *Legalità (principio di)*, in *Dig. disc. pubbl.*, IX, 1991, 84 ss.

GUERRA G., *La sicurezza degli artefatti robotici in prospettiva comparatistica. Dal cambiamento tecnologico all'adattamento giuridico*, il Mulino, Bologna, 2018.

GUNNINGHAM N., REES J., *Industry Self-Regulation: An Institutional Perspective*, in *Law & Policy*, 19, 1997, 363 ss.

GUROVICH Y. ET AL., *Identifying facial phenotypes of genetic disorders using deep learning*, in *Nature Medicine*, 25, 2019, 60 ss.

GÜVEN K., *Facial Recognition Technology: Lawfulness of Processing under the GDPR in Employment, Digital Signage and Retail Context*, Tilburg University, 2019 [bit.ly/3cWmNcD].

HACKER P., *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law*, in *Common Market Law Review*, 55, 4, 2018, 143 ss.

HASAN A., *2019 Proved We Can Stop Face Recognition Surveillance*, in *ACLU*, 17 gennaio 2020 [bit.ly/3cYk3vp].

HAO K., HOWELL O'NEILL P., *The hack that could make face recognition think someone else is you*, in *MIT Technology Review*, 5 agosto 2020.

HILDEBRANDT M., *A Vision of Ambient Law*, in BROWNSWORD R., YEUNG K. (a cura di), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, cit., 175 ss.

HILDEBRANDT M., *Saved by Design? The Case of Legal Protection by Design*, in *Nanoethics*, 11, 2017, 307 ss.

HILDEBRANDT M., *Smart technologies and the End(s) of Law. Novel Entanglements of Law and Technology*, Edward Elgar, Cheltenham, 2015.

HILDEBRANDT M., *Legal Protection by Design: Objections and Refutations*, in *Legisprudence*, 5, 2, 2011, 223 ss.

HILDEBRANDT M., *Defining Profiling: A New Type of Knowledge?*, in HILDEBRANDT M., GUTWIRTH S. (a cura di), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008, 17 ss.

HIROSE M., *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, in *Connecticut Law Review*, 49, 5, 2017, 1591 ss.

HIRSCH D., *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, in *Seattle University Law Review*, 34, 2011, 439 ss.

HOFFMANN-RIEM W., *Artificial Intelligence as a Challenge for Law and Regulation*, in WISCHMEYER T., RADEMACHER T. (a cura di), *Regulating Artificial Intelligence*, Springer, 2020, 1 ss.

HOOD C.C., MARGETTS H.Z., *The Tools of Government in the Digital Age*, Palgrave Macmillan, Basingstoke, 2007.

HUANG T., XIONG Z., ZHANGE Z., *Face Recognition Applications*, in LI S.Z., JAIN A.K. (a cura di), *The Handbook of Face Recognition*, Springer, New York, 617 ss.

HUMAN RIGHTS COUNCIL, *Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, A/HRC/41/35, 28 maggio 2019.

IANNUZZI A., *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale Scientifica, Napoli, 2018.

IANNUZZI A., FILOSA F., *Il trattamento dei dati genetici e biometrici*, in *Dirittifondamentali.it*, 2, 2019.

INFORMATION COMMISSIONER'S OFFICE, *Regulatory Sandbox Final Report: Heathrow Airport Ltd.*, giugno 2020 [bit.ly/3s21FWK].

INFORMATION COMMISSIONER'S OFFICE, *ICO investigation into how the police use facial recognition technology in public places*, 31 ottobre 2019 [bit.ly/3uuBaei].

IRAOLA R., *Lights, Camera, Action! – Surveillance Cameras, Facial Recognition Systems and the Constitution*, in *Loyola Law Review*, 49, 4, 2003, 773 ss.

IRTI N., SEVERINO E., *Dialogo su diritto e tecnica*, Laterza, Roma-Bari, 2001.

JAIN A.K., ROSS A.A., *Introduction to Biometrics*, in JAIN A.K., FLYNN P., ROSS A.A. (a cura di), *Handbook of Biometrics*, Springer, New York, 2008, 1 ss.

JANSSEN H.L., *An approach for a fundamental rights impact assessment to automated decision-making*, in *International data privacy law*, 10, 1, 2020, 76 ss.

KACHUR A. ET AL., *Assessing the big five personality traits using real-life static facial images*, in *Nature Scientific Reports*, 10, 2020.

KAFKA F., *Il processo*, Garzanti, Milano, 1984.

KAMARA L., *Co-regulation in EU personal data protection: The case of technical standards and the privacy by design standardisation 'mandate'*, in *European Journal of Law and Technology*, 8, 1, 2017.

KAPLAN J., *Intelligenza artificiale. Guida al futuro prossimo*, Luiss, Roma, 2017.

KATYAL N.K., *Disruptive Technologies and the Law*, in *The Georgetown Law Journal*, 102, 2014, 1685 ss.

KEYES O., *The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition*, *Proceedings of the ACM on Human-Computer Interaction,* 2, novembre 2018.

KIM P.T., *Data-Driven Discrimination at Work*, in *William & Mary Law Review*, 58, 3, 2016-2017, 857 ss.

KINDT E.J., *Having yes, using no? About the new legal regime for biometric data*, in *The computer law and security report*, 34, 3, 2018, 523 ss.

KLARE B.F., BURGE M.J., KLONTZ J.C., VORDER BRUEGGE R.W., JAIN A.K., *Face recognition performance: Role of demographic information*, in *IEEE Transactions on Information Forensics and Security*, 7, 6, 2012, 1789 ss.

KOOPS B.-J., *Criteria for Normative Technology: The Acceptability*

of 'Code as law' in Light of Democratic and Constitutional Values, in BROWNSWORD R., YEUNG K. (a cura di), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, cit., 157 ss

KOOPS B.-J., *The (In)flexibility of Techno-Regulation and the Case of Purpose-Binding*, in *Legisprudence*, 5, 2012, 171 ss.

KOOPS B.-J., *Ten dimensions of technology regulation. Finding your bearings in the research space of an emerging discipline*, in GOODWIN M.E.A., KOOPS B.-J., LEENES R.E. (a cura di), *Dimensions of technology regulation*, Nijmegen, Wolf Legal Publishers, 2010, 309 ss.

KOOPS B.-J. ET AL., *A Typology of Privacy*, in *University of Pennsylvania Journal of International Law*, 38, 2017, 483 ss.

KOOPS B.-J., LEENES R., *Privacy Regulation Cannot be Hardcoded. A Critical Comment on the "Privacy By Design" Provision in Data-Protection Law*, in *International Review of Law, Computers & Technology*, 28, 2, 2014, 159 ss.

KOSINSKI M., *Facial recognition technology can expose political orientation from naturalistic facial images*, in *Nature Scientific Reports*, 100, 2021.

KOSINSKI M., STILLWELL D., GRAEPEL T., *Private traits and attributes are predictable from digital records of human behavior*, in *PNAS*, 110, 15, 9 aprile 2013, 5802 ss.

KOSTKA G., *China's social credit systems and public opinion: Explaining high levels of approval*, in *New media & society*, 21, 7, 2019, 1565 ss.

KOZINSKI A., *Two Faces of Anonymity*, in *Capital University Law Review*, 43, 1, 2015.

KRITHIKA L.B., VENKATESH K., RATHORE S., HARISH KUMAR M., *Facial recognition in education system*, in *IOP Conference Series: Materials Science and Engineering*, 263, 4, 2017.

KROENER I., WRIGHT D., *A Strategy for Operationalizing Privacy by Design*, in *The Information Society*, 30, 5, 2014, 355 ss.

KROLL J.A., HUEY J., BAROCAS S., FELTEN E.W., REIDENBERG J.R., ROBINSON D.G., YU H., *Accountable Algorithms*, in *University of Pennsylvania Law Review*, 165, 2017, 633 ss.

KUIJPER P.J., *Some legal problems Associated with the Communitarization of Policy on Visas, Asylum and Immigration under the Amsterdam Treaty and Incorporation of the Schengen Acquis*, in *Common Market Law Review*, 37, 2, 2000, 345 ss.

LAGIOIA F., SARTOR G., *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *Federalismi.it*, 11, 2020, 85 ss.

LAMARQUE E., *Prima i bambini. Il principio dei* best interests of the child *nella prospettiva costituzionale*, FrancoAngeli, Milano, 2016.

LANDINI S., *Identità digitale tra tutela della persona e proprietà intellettuale*, in *Rivista di diritto industriale*, 4-5, 2017, 180 ss.

LAPERRUQUE J. (a cura di), *Facing the Future of Surveillance. Task Force on Facial Recognition Surveillance*, *Project On Government Oversight (POGO)*, 4 marzo 2019 [bit.ly/3rZlKgi].

LATOUR B., VENN C., *Morality and Technology: The End of the Means*, in *Theory, Culture & Society*, 19, 5-6, 2002, 247 ss.

LAZZERINI N., *La Carta dei diritti fondamentali dell'Unione europea. I limiti di applicazione*, FrancoAngeli, Milano, 2018.

LEARNED-MILLER E., ORDÓÑEZ V., MORGENSTERN J., BUOLAMWINI J., *Facial Recognition Technologies in the Wild: A Call for a Federal Office*, 29 maggio 2020 [bit.ly/3dHCcwS].

LEARNED-MILLER E., ORDÓÑEZ V., MORGENSTERN J., BUOLAMWINI J., *Facial Recognition Technologies in the Wild: A Primer*, 29 maggio 2020 [bit.ly/2OtyK06].

LEENES R., *Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology*, in *Legisprudence*, 5, 2011, 150 ss.

LEENES R., LUCIVERO F., *Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design*, in *Law, Innovation and Technology*, 6, 2, 2014, 193 ss.

LESLIE D., *Understanding bias in facial recognition technologies: an explainer*, *The Alan Turing Institute*, 2020 [bit.ly/2OsKRuk].

LESSIG L., *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

LESSIG L., *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, 113, 1999, 501 ss.

LEVI A. (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act*, Giuffrè, Milano, 2016.

LI S.Z., JAIN A.K., *Introduction*, in LI S.Z., JAIN A.K. (a cura di), *The Handbook of Face Recognition*, Springer, New York, 1 ss.

LI X., ET AL., T*owards Reading Hidden Emotions: A comparative Study of Spontaneous Micro-expression Spotting and Recognition Methods*, in *arXiv:1511.00423v2 [cs.CV]*, 8 febbraio 2018.

LIANG F., DAS V., KOSTYUK N., HUSSAIN M.M., *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, in *Policy and Internet*, 4, 10, 2018, 415 ss.

LIPPE P., KATZ D.M., JACKSON D., *Legal by Design: A New Paradigm for Handling Complexity in Banking Regulation and Elsewhere in Law*, in *Oregon Law Review*, 93, 4, 2015, 833 ss.

LONGO A., SCORZA G., *Intelligenza artificiale. L'impatto sulle nostre vite, diritti e libertà*, Mondadori, Milano, 2020.

LONGO E., *Dai* big data *alle «bolle filtro»: nuovi rischi per i sistemi democratici*, in *Percorsi costituzionali*, 2, 2019, 29 ss.

LOPEZ R., *La rappresentazione facciale tramite* software, in SCALFATI A. (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2019, 239 ss.

LUCIANI M., *La decisione giudiziaria robotica*, in *Rivista AIC*, 3, 2018, 872 ss.

LUHMANN N., *Sociologia del rischio*, Mondadori, Milano, 1996.

LUPO N., PICCIRILLI G., *European Court of Human Rights and the Quality of Legislation: Shifting to a Substantial Concept of 'Law'?*, in *Legisprudence*, 6, 2, 2012, 229 ss.

LYON D., *La cultura della sorveglianza. Come la società del controllo ci ha reso tutti controllori*, Luiss University Press, Roma, 2020.

LYON D., *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002.

MACCABIANI N., *An empirical approach to the Rule of Law: the case of Regulatory Sandboxes*, in *Osservatorio sulle fonti*, 2, 2020, 742 ss

MAESTRI E., *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio*, ESI, Napoli, 2015.

MAKRIDIS M., MATTAS K., CIUFFO B., ALONSO M., *Assessing the Impact of Connected and Automated Vehicles. A Freeway Scenario*, in ZACHÄUS C., MÜLLER B., MEYER G. (a cura di), *Advanced Microsystems for Automotive Applications 2017*, Springer, 2018, 213 ss.

MALGIERI G., *Il furto di "identità digitale": una tutela "patrimoniale" della personalità*, in FALCINELLI D., FLOR R., MARCOLINI S. (a cura di), *La giustizia penale nella "rete". Le nuove sfide della società dell'informazione nell'epoca di Internet*, Diplap, Mila-no, 2015, 37 ss.

MALGIERI G., COMANDÉ G., *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 7, 4, 2017, 243 ss.

MANETTI M., *Libertà di pensiero e anonimato in rete*, in *Il Diritto dell'informazione e dell'informatica*, 2, 2014, 139 ss.

MANFREDI G., *Note sull'attuazione del principio di precauzione in diritto pubblico*, in *Diritto pubblico*, 3, 2004, 1075 ss.

MANN M., SMITH M., *Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight*, in *University of New South Wales Law Journal*, 40, 1, 2017, 121 ss.

MANTELERO A., *The future of data protection: Gold standard vs. global standard*, in *Computer Law & Security Review*, 40, 2021, in corso di pubblicazione.

MANTELERO A., *La gestione del rischio*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia*, cit., 473 ss.

MANTELERO A., *AI and big data: a blueprint for a human rights, social and ethical impact assessment*, in *Computer Law & Security Review*, 34, 4, 2018, 754 ss.

MANTELERO A., *Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection*, in *Computer Law & Security Review*, 32, 2, 2016, 238 ss.

MANTELERO A., *The Future of Consumer Data Protection in the E.U. Rethinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics*, in *Computer Law and Security Review*, 30, 2014, 643 ss.

MANTOVANI F., *Il problema della criminalità. Compendio di scienze criminali*, Cedam, Padova, 1984.

MARCUSE H., *L'uomo a una dimensione. L'ideologia della società industriale avanzata*, Einaudi, Torino, 1974.

MARESCA A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati del lavoratore*, cit., 1 ss.

MARESCA A., CIUCCIOVINO S., ALVINO I., *Regolamento UE 2016/679 e rapporto di lavoro*, in CALIFANO L., COLAPIETRO C. (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, cit., 311 ss.

MARQUENIE T., *The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework*, in *Computer Law & Security Review*, 33, 3, 2017, 324 ss.

MARTINICO G., *Art. 7. Rispetto della vita privata e della vita fami-*

liare, in AA.VV., *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017, 119 ss.

MARWICK A., BOYD D., *Networked Privacy: How Teenagers Negotiate Context in Social Media*, in *New Media & Society*, 16, 7, 2014, 1051 ss.

MARX G.T., STEEVES V., *From the Beginning: Children as Subjects and Agents of Surveillance*, in *Surveillance & Society*, 7, 3/4, 2010, 192 ss.

MASUCCI A., *Digitalizzazione dell'amministrazione e servizi pubblici on line. Lineamenti del disegno normativo*, in *Diritto pubblico*, 1, 2019, 117 ss.

MAYER-SCHÖNBERGER V., CUKIER K., *Big Data: A Revolution that will Transform How We Live, Work and Think*, John Murray, London, 2013.

MAYER-SCHÖNBERGER V., PADOVA Y., *Regime Change? Enabling Big Data through Europe's New Data Protection Regulation*, in *The Columbia Science & Technology Law Review*, 17, 2016, 315 ss.

MAYNTZ R., *La teoria della governance: sfide e prospettive*, in *Rivista italiana di Scienza politica*, 1, 1993, 3 ss.

MCCOY S., *O'Big Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology*, in *The John Marshall Journal of Information Technology & Privacy Law*,, 20, 3, 2002, 471 ss.

MERLER M., RATHA N., FERIS R.S., SMITH J.R., *Diversity in faces*, in *arXiv:1901.10436v6*, 2019.

MICROSOFT CORPORATION, S*ix Principles for Developing and Deploying Facial Recognition Technology*, dicembre 2018 [bit.ly/3fNnp6o].

MIDIRI M., PIVA S., *L'interesse pubblico come base giuridica e come finalità del trattamento dei dati personali*, in SCAGLIARINI S. (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali*, cit., 21 ss.

MILAZZO P., *La Direttiva UE 2016/680 e la protezione dei dati personali nell'ambito della sicurezza pubblica e della giustizia penale*, in CALIFANO L., COLAPIETRO C. (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, cit., 709 ss.

MING-HSUAN Y., KRIEGMAN D. J., AHUJa N., *Detecting Faces in*

Images: A Survey, in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24, 1, 2002, 34 ss.

MITROU L., *Data Protection, Artificial Intelligence and Cognitive Services. Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?*, in *SSRN*, dicembre 2018.

MODUGNO F., *I "nuovi diritti" nella giurisprudenza costituzionale*, Giappichelli, Torino, 1995.

MONTALDO R., *Le dinamiche della rappresentanza tra nuove tecnologie, populismo, e riforme costituzionali*, in *Quad. cost.*, 4, 2019, 789 ss.

MORAES T.G., ALMEIDA E.C., DE PEREIRA J.R.L., *Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-)public spaces*, in *AI Ethics*, 2020.

MORANA D., *Articolo 23*, in CLEMENTI F., CUOCOLO L., ROSA F., VIGEVANI G.E. (a cura di), *La Costituzione italiana. Commento articolo per articolo*, I, cit., 160 ss.

MORANA D., *Libertà costituzionali e prestazioni personali imposte. L'art. 23 Cost. come norma di chiusura*, Giuffrè, Milano, 2007.

MORGESE G., *La riforma del sistema Dublino: il problema della condivisione delle responsabilità*, in *Diritto pubblico*, 2, 2020, 97 ss.

MORO P., *Macchine come noi. Natura e limiti della soggettività robotica*, in RUFFOLO U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., 45 ss.

MORO P., Libertà del *robot?* Sull'etica delle macchine intelligenti, in BRIGHI R., ZULLO S. (a cura di), *Filosofia del diritto e nuove tecnologie*, cit., 525 ss.

MORRIS J., *Defining the Precautionary Principle*, in ID. (a cura di), *Rethinking Risk and the Precautionary Principle*, Oxford, Butterworth-Heinemann, 2000, 1 ss.

MORTATI C., *Istituzioni di diritto pubblico*, Cedam, Padova, 1976.

MOSCARINI A., *Principio costituzionale di eguaglianza e diritti fondamentali*, in NANIA R., RIDOLA P. (a cura di), *I diritti costituzionali*, I, cit., 365 ss.

MOSTACCI E., *La* soft law *nel sistema delle fonti: uno studio comparato*, Cedam, Padova, 2008.

MUNDIE C., *Privacy Pragmatism: Focus on Data Use, Not on Data Collection*, in *Foreign Affairs*, 94, 2, 2014, 28 ss.

MUSSELLI L., *Alcune prime considerazioni sui sistemi di scambio di*

informazioni nello spazio di libertà, sicurezza e giustizia: securitization, function creep e tutela dei diritti, Centro Studi sul Federalismo, Research Paper, maggio 2013.

NAKAR S., GREENBAUM D., *Now you see me. Now you still do: facial recognition technology and the growing lack of privacy*, in *Boston University Journal of Science & Technology Law*, 23, 2017, 88 ss.

NAPOLI C., *Algoritmi, intelligenza artificiale e formazione della volontà pubblica: la decisione amministrativa e quella giudiziaria*, in *Rivista AIC*, 3, 2020, 318 ss.

NERONI REZENDE I., *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, in *New Journal of European Criminal Law*, 11, 3, 2020, 375 ss.

NICOTRA I.A., *Privacy vs trasparenza, Il Parlamento tace e il punto di equilibrio lo trova la Corte*, in *Federalismi.it*, 7, 2019, 7 ss.

NICOTRA I.A., VARONE V., *L'algoritmo, intelligente ma non troppo*, in *Rivista AIC*, 4, 2019, 86 ss.

NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006.

NOBILI M., *Art. 188 c.p.p.*, in M. CHIAVARIO (diretto da), *Commento al nuovo codice di procedura penale*, II, Utet, Torino, 1990, 396 s.

NUZZO V., *La protezione del lavoratore dai controlli impersonali*, Editoriale Scientifica, Napoli, 2018.

O'NEIL C., *Armi di distruzione matematica*, Giunti-Bompiani, Firenze-Milano, 2017.

OLIVETTI M., *Diritti fondamentali*, Giappichelli, Torino, 2018.

OLOYEDE M.O., HANCKE G.P., *Unimodal and Multimodal Biometric Sensing Systems: A Review*, in *IEEE access*, 4, 2016, 7532 ss.

ORWELL G., *1984*, Mondadori, Milano, 1950.

PACE A., *Problematica delle libertà costituzionali. Parte speciale*, Cedam, Padova, 1992.

PACE A., *Il c.d. diritto all'identità personale e gli artt. 2 e 21 della Costituzione*, in ALPA G., BESSONE M., BONESCHI L. (a cura di), *Il diritto alla identità personale*, Cedam, Padova, 1981, 36 ss.

PACILEO P., *Profilazione e diritto di opposizione*, in SICA S., D'ANTONIO V., RICCIO G.M. (a cura di), *La nuova disciplina europea della privacy*, cit., 177 ss.

PAGALLO U., *Etica e diritto dell'Intelligenza Artificiale nella governance digitale: il* Middle-out Approach, in RUFFOLO U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., 29 ss.

PAGALLO U., *Intelligenza Artificiale e diritto. Linee guida per un oculato intervento normativo*, in *Sistemi intelligenti*, 3, 2017, 615 ss.

PAGALLO U., *LegalAIze: Tackling the Normative Challenges of Artificial Intelligence and Robotics Through the Secondary Rules of Law*, in M. CORRALES, M. FENWICK, N. FORGÓ (a cura di.), *New Technology, Big Data and the Law*, Springer, Singapore, 2017, 281 ss.

PAGALLO U., *Il diritto nell'età dell'informazione*, Giappichelli, Torino, 2014.

PAGALLO U., DURANTE M., *The Pros and Cons of Legal Automation and its Governance*, in *European Journal of Risk Regulation*, 2, 2016, 323 ss.

PAJNO A. ET AL. *AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal*, 3, 2019, 205 ss.

PALADIN L., *Eguaglianza (dir. cost.)*, in *Enc. dir.*, XIV, 1965, 519 ss.

PANNIA P., *"Institutional uncertainty" as a technique of migration governance. A comparative legal perspective*, *in DPCE Online*, 41, 4, 2019, 5136 ss.

PAOLUCCI F., *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *MediaLaws*, 1, 2021.

PARDOLESI R., *Diritto alla riservatezza e circolazione dei dati personali: una storia di evoluzione e discontinuità,* in PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, I, Giuffrè, Milano, 2003, 1 ss.

PARISER E., *The filter bubble: What the Internet is hiding from you*, Penguin, London, 2011.

PARLAMENTO EUROPEO, *Una politica industriale europea globale in materia di robotica e intelligenza artificiale* (2018/2088(INI)), 12 febbraio 2019.

PARLAMENTO EUROPEO, *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica* (2015/2103(INL)), 16 febbraio 2017.

PASQUALE F., *The Black Box Society. The Secret Algorithms That Control Money and Information,* Harvard University Press, Cambridge-London, 2015.

PASQUINO T., *Identità digitale della persona, diritto all'immagine e reputazione*, in TOSI E. (a cura di), *Privacy digitale*, cit., 93 ss.

PASSAGLIA P., *Internet nella Costituzione italiana: considerazioni introduttive*, in *Consulta OnLine*, 2013.

PASSAGNOLI G., *Il diritto civile al tempo dell'intelligenza artificiale: spunti per una problematizzazione*, in DORIGO S. (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit, 67 ss.

PATERNITI F., *Figli e ordinamento costituzionale*, Editoriale Scientifica, Napoli, 2019.

PAULETTO C., *Options towards a global standard for the protection of individuals with regard to the processing of personal data*, in *Computer Law & Security Review*, 40, 2021, in corso di pubblicazione.

PELLECCHIA E., *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, in *Le nuove leggi civili commentate*, 5, 2018, 1210 ss.

PENTLAND A., CHOUDHURY T., *Personalizing Smart Environments: Face Recognition for Human Interaction*, in *Computer*, 33, 2000, 50 ss.

PERRI P., *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, GFL, Milano, 2020.

PHILLIPS P.J., JIANG F., NARVEKAR A., AYYAD J., O'TOOLE A.J., *An Other-Race Effect for Face Recognition Algorithms*, in *ACM Transactions on Applied Perception*, 14, febbraio 2011.

PICARD R.V., *Affective computing*, MIT Press, Cambridge, 1997.

PICCIRILLI G., *La "riserva di legge". Evoluzioni costituzionali, influenze sovrastatuali*, Giappichelli, Torino, 2019.

PIETERS W., *Explanation and trust: What to tell the user in security and AI?*, in *Ethics and Information Technology*, 13, 2011, 53 ss.

PIN A., *Non esiste la "pallottola d'argento": l'"*artificial face recognition*" al vaglio giudiziario per la prima volta*, in *DPCE online*, 4, 2019, 3175 ss.

PINO G., *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, il Mulino, Bologna, 2009.

PIRNI A., CARNAVALE A., *The challenge of regulating emerging technologies. A philosophical framework*, in PALMERINI E., STRADELLA E. (a cura di), *Law and Technology. The Challenge of Regulating Technological Development*, PUP, Pisa, 2013, 27 ss.

PITTMAN C., *"Shopping While Black": Black consumers' management of racial stigma and racial profiling in retail settings*, in *Journal of Consumer Culture*, 20, 1, 2017, 3 ss.

PIZZETTI F., *GDPR e Intelligenza artificiale. Codici di condotta, certificazioni, sigilli, marchi e altri poteri di soft law previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA*, in MANTELERO A., POLETTI D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali*, cit., 69 ss.

PIZZETTI F., *La protezione dei dati personali e le sfide dell'Intelligenza Artificiale*, in PIZZETTI F. ET AL., *Intelligenza artificiale, protezione dati personali e regolazione*, Giappichelli, Torino, 2018, 5 ss.

POGGI A., *Soft law nell'ordinamento comunitario*, in AA.VV., *Associazione Italiana dei Costituzionalisti. Annuario 2005. Atti del XX Convegno Annuale, Catania 14-15 ottobre 2005*, Cedam, Padova, 2007, 369 ss.

POLETTI D., *Comprendere il Reg. UE 2016/679: un'introduzione*, in MANTELERO A., POLETTI D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali*, cit., 9 ss.

POLLICINO O., *L' ''autunno caldo'' della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *Federalismi.it*, 19, 2019.

POLLICINO O., BASSINI M., *Art. 8. Protezione dei dati di carattere personale*, in AA.VV., *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017, 132 ss.

POLLICINO O., RESTA F., *Visibilità del potere, riservatezza individuale e tecnologia digitale. Il bilanciamento delineato dalla Corte*, in *Il diritto dell'informazione e dell'informatica*, 1, 2019, 110 ss.

POPOLI A.R., "*Social network" e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, in *Il Diritto dell'informazione e dell'informatica*, 6, 2014, 981 ss.

POPOLI A.R., *L'adeguamento dei social network sites al GDPR: un percorso non ancora ultimato*, in *Il Diritto dell'informazione e dell'informatica*, 6, 2019, 1289 ss.

POPOLI A.R., *Codici di condotta e certificazioni*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia*, cit., 527 ss.

PORTER S. ET AL., *Is the Face a Window to the Soul? Investigation of the Accuracy of Intuitive Judgments of the Trustworthiness of Human Faces*, in *Canadian Journal of Behavioural Science*, 40, 3, 2008, 171 ss.

PREDIERI A., *Le norme tecniche nello Stato pluralista e prefederativo*, in *Il diritto dell'economia*, 1996, 251 ss.

PUGLIESE J., *Biometrics. Bodies, Technologies, Biopolitics*, Routledge, New York-Oxon, 2010.

PUTHEA K., HARTANTO R., HIDAYAT R., *A Review Paper on Attendance Marking System Based on Face Recognition*, in *IEEE 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 8 febbraio 2018, 304 ss.

RAAB T., *Germany. Video Surveillance and Face Recognition: Current Developments*, in *European Data Protection Law Review*, 5, 2019, 544 ss.

RAJI I.D., BUOLAMWINI J., *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, gennaio 2019.

RALEY R., *Dataveillance and Countervailance*, in GITELMAN L. (a cura di), *'Raw Data' is an Oxymoron*, MIT Press, Cambridge, 2013, 121 ss.

RAMAJOLI M., Self regulation*,* soft regulation *e* hard regulation *nei mercati finanziari*, in *Rivista della Regolazione dei mercati*, 2, 2016, 53 ss.

RAMANATHAN N., CHELLAPPA R., BISWAS S., *Computational methods for modelling facial aging: A survey*, in *Journal of Visual Languages and Computing*, 20, 2009, 131 ss.

REIDENBERG J.R., *Privacy in Public*, in *University of Miami Law Review*, 69, 1, 2014, 141 ss.

REIDENBERG J.R., *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, in *Texas Law Review*, 76, 3, 1998, 553 ss.

REIDENBERG J.R. ET AL., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, in *I/S: A Journal of Law and Policy for the Information Society*, 11, 2, 2015, 485 ss.

REISMAN D., SCHULTZ J., CRAWFORD K., WHITTAKER M., *Algorithmic impact assessments: a practical framework for public agency accountability*, AI Now Institute, 2018 [bit.ly/39S1OWC].

RESCIGNO G.U., *Sul principio di legalità*, in *Diritto pubblico*, 1995, 247 ss.

RESCIGNO P., *Personalità (diritto della)*, in *Enc. giur.*, XXIII, 1991.

RESTA G., *Identità personale e identità digitale*, in *Il diritto dell'informazione e dell'informatica*, 3, 2017, 511 ss.

RESTA G., *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, in *Il Diritto dell'informazione e dell'informatica*, 2, 2014, 171 ss.

RHODES R.A.W., *The New Governance: Governing without Government'*, in *Political Studies*, 44, 1996, 652 ss.

RICCI A., *I diritti dell'interessato*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia*, cit., 392 ss.

RICCI A., *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati. Riflessioni sul d.lgs. 18 maggio 2018, n. 51, di attuazione della dir. 2016/680/UE*, in *Le Nuove leggi civili commentate*, 3, 2019, 565 ss.

RICHARDS N.M., *The Dangers of Surveillance*, in *Harvard Law Review*, 126, 2013, 1934 ss.

RIDOLA P., *Libertà e diritti nello sviluppo storico del costituzionalismo*, in NANIA R., RIDOLA P. (a cura di), *I diritti costituzionali*, I, cit., 3 ss.

RIGANO F., *Art. 18 Cost.*, in CELOTTO A., BIFULCO R., OLIVETTI M. (a cura di), *Commentario alla Costituzione*, Utet, Torino, 2006, 404 ss.

RODOTÀ S., *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012.

RODOTÀ S., *Riservatezza*, in *Enc. it.*, VII App., 2007, versione *online*.

RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica del diritto privato*, 4, 1997, 583 ss.

RODOTÀ S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997.

RODOTÀ S., *Tecnologie e diritti*, il Mulino, Bologna, 1995.

ROMANO B., *Algoritmi al potere. Calcolo giudizio pensiero*, Giappichelli, Torino, 2018.

ROSSI F., *Intelligenza Artificiale benefica e sicura: iniziative accademiche, governative e industriali*, in *Sistemi intelligenti*, 3, 2017, 545 ss.

ROSSI L.S., *I rapporti fra la Carta dei diritti fondamentali e la CE-*

DU nella giurisprudenza delle rispettive Corti, in *AISDUE*, 30 dicembre 2020, 41 ss.

RUBECHI M., *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *Federalismi.it*, 23, 2016.

RUBINSTEIN I.S., *Big Data: The End of Privacy or a New Beginning?*, in *International Data Privacy Law*, 3, 2, 2013, 74 ss.

RUBINSTEIN I.S., *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, in *I/S: A Journal of Law and Policy for the Information Society*, 6, 3, 2011, 355 ss.

RUBINSTEIN I., GOOD N., *Privacy by Design: a Counterfactual Analysis of Google and Facebook Privacy Incidents*, in *Berkeley Technology Law Journal*, 28, 2, 2013, 1333 ss.

RUFFOLO U., *La "personalità elettronica"*, in ID. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., 213 ss.

RUFFOLO U., *La responsabilità da* artificial intelligence*, algoritmo e* smart product*: per i fondamenti di un diritto dell'intelligenza artificiale* self-learning, in ID. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., 93 ss.

RUGANI G., *La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della Direttiva (Ue) 2016/680: frammentazione ed incertezze applicative*, in *Freedom, Security & Justice: European Legal Studies*, 1, 2019, 75 ss.

RUGGERI A., *Il coronavirus contagia anche le categorie costituzionali e ne mette a dura prova la capacità di tenuta*, in *Diritti regionali*, 1, 2020, 368 ss.

RUOTOLO M., *La libertà di riunione e di associazione*, in NANIA R., RIDOLA P. (a cura di), *I diritti costituzionali*, II, cit., 677 ss.

RUSSELL S.J., NORVIG P., *Intelligenza artificiale. Un approccio moderno*, I, Pearson Prentice Hall, Milano-Torino, 2010.

SALERNO G., *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in NANIA R., RIDOLA P. (a cura di), *I diritti costituzionali*, II, cit., 617 ss.

SALERNO G.M., *Riserva di legge e principio di legalità nel processo di integrazione europea*, in MODUGNO F. (a cura di), *Trasformazioni della funzione legislativa. II. Crisi della legge e sistema delle fonti*, Giuffrè, Milano, 2000, 307 ss.

SALIMBENI M.T., *La riforma dell'articolo 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, in *Rivista italiana di diritto del lavoro*, 1, 2016, 589 ss.

SANTOSUOSSO A., *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Mondadori, Milano, 2020.

SANTOSUOSSO A., *Diritto, scienza, nuove tecnologie*, Wolters Kluwer-Cedam, Padova, 2016.

SARPI F., *La regolazione di domani. Come adeguare il processo normativo alle sfide dell'innovazione*, in *Rivista Italiana di Politiche Pubbliche*, 3, 2018, 435 ss.

SARRA C., *Il mondo-dato. Saggi su datificazione e diritto*, Cleup, Padova, 2019.

SARTOR G., LAGIOIA F., *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, Panel for the Future of Science and Technology, STOA, PE 641.5 30, giugno 2020.

SASSI S., *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, in *Analisi Giuridica dell'Economia*, 1, 2019, 109 ss.

SAURWEIN F, *Regulatory Choice for Alternative Modes of Regulation: How Context Matters*, in *Law & Policy*, 33, 3, 2011, 334 ss.

SAUTER W., *Proportionality in EU law: A balancing act?*, in BARNARD C., ALBORS-LLORENC A., GEHRING M.W., SCHÜTZE R. (a cura di), *Cambridge yearbook of European legal studies 2012-2013*, Hart Publishing, Oxford, 2013, 439 ss.

SCAFFARDI L., *Giustizia genetica e tutela della persona. Uno studio comparato sull'uso (e abuso) delle banche dati del DNA a fini giudiziari*, Wolters Kluwer, Milano, 2017.

SCAFFARDI L., Next Generation Prüm *e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, in *Federalismi.it*, 8, 2021, 200 ss.

SCAGLIARINI S., *Dal "vecchio" al "nuovo" Codice della privacy*, in ID. (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali*, cit., 1 ss.

SCAGLIARINI S., *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Aracne, Roma, 2013.

SCALISI A., *Il diritto alla riservatezza: diritto all'immagine, il diritto al segreto, la tutela dei dati personali, il diritto alle vicende della vita privata, gli strumenti di tutela,* Giuffrè, Milano, 2002.

SCANTAMBURLO T., CHARLESWORTH A., CRISTIANINI N., *Machine Decisions and Human Consequences*, in YEUNG K., LODGE M. (a cura di), *Algorithmic Regulation*, Oxford University Press, 2019, 49 ss.

SCAPARONE M., *Elementi di procedura penale. I princìpi costituzionali*, Giuffrè, Milano, 1999.

SCHERER M.U., *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, in *Harvard Journal of Law and Technology,* 29, 2, 2016, 353 ss.

SCHUMPETER J.A., *Capitalism, Socialism and Democracy*, Harper, New York, 1950.

SCIA F., *Diritti dei minori e responsabilità dei genitori nell'era digitale*, ESI, Napoli, 2020,

SCOTT C., *Regulation in the Age of Governance. The Rise of the Post-Regulatory State*, in JACINT J., LEVI-FAUR D. (a cura di), *The Politics of Regulation*, Edward Elgar, Cheltenham, 2004, 145 ss.

SCOTT C., *Standard-Setting in Regulatory Regimes*, in CAVE M., BALDWIN R., LODGE M. (a cura di), *The Oxford Handbook on Regulation*, Oxford University Press, Oxford, 2010, 104 ss.

SELBST A.D., *Disparate Impact in Big Data Policing*, in *Georgia Law Review*, 52, 2017, 109 ss.

SELBST A.D., POWLES J., *Meaningful information and the right to explanation*, in *International Data Privacy Law*, 7, 2017, 233 ss.

SENDEN L., *Soft Law, Self-regulation and Co-regulation in European Law: Where Do They Meet?*, in *Electronic Journal of Comparative Law*, 9, 1, 2005, 1 ss.

SHAFFER K., *Data versus Democracy: How Big Data Algorithms Shape Opinions and Alter the Course of History*, Apress, Colorado, 2019.

SHEEHAN M.J., NACHMAN M.W., *Morphological and Population Genomic Evidence that Human Faces Have Evolved to Signal Individual Identity*, in *Nature Communication*, 5, 2014, 1 ss.

SICA S., *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in SICA S., D'ANTONIO V., RICCIO G.M. (a cura di), *La nuova disciplina europea della privacy*, cit., 1 ss.

SICA S., *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Rivista di Diritto Civile*, 6, 2001, 621 ss.

SICA S., GIANNONE CODIGLIONE G., *La libertà fragile. Pubblico e privato al tempo della rete*, ESI, Napoli, 2014.

SILEONI S., *Autori delle proprie regole. I codici di condotta per il trattamento dei dati personali e il sistema delle fonti*, Cedam, Padova, 2011,

SILVER N., *The Signal and the Noise. Why So Many Predictions Fail – but Some Don't*, Penguin, New York, 2012,

SIMONCINI A., *Amministrazione digitale algoritmica. Il quadro costituzionale*, in CAVALLO PERIN R., GALLETTA D.-U. (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Giappichelli, Torino, 2020, 1 ss.

SIMONCINI A, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1, 2019, 63 ss.

SIMONCINI A., *Profili costituzionali dell'amministrazione algoritmica*, in *Rivista trimestrale di diritto pubblico*, 4, 2019, 1149 ss.

SIMONCINI A., *Sovranità e potere nell'era digitale*, in FROSINI T.E., POLLICINO O., APA E., BASSINI M. (a cura di), *Diritti e libertà in Internet*, Le Monnier, Firenze, 2017, 19 ss.

SIMONCINI A., *I* codici deontologici *di protezione dei dati personali nel sistema delle fonti. L'emersione di un nuovo «paradigma» normativo?*, in DE SIERVO U. (a cura di), *Osservatorio sulle fonti 1999*, Giappichelli, Torino, 2000, 277 ss.

SIMONCINI A., *Il sistema delle fonti di disciplina del trattamento di dati personali*, in CUFFARO V., RICCIUTO L. (a cura di), *Il trattamento dei dati personali*, II, Giappichelli, Torino, 1999, 11 ss.

SIMONCINI A., SUWEIS S., *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista Internazionale di Filosofia del Diritto*, 1, 2019, 87 ss.

SOLOVE D.J., *Nothing to hide: the false trade off between privacy and security*, New Haven-London, Yale University Press, 2011.

SOLOVE D.J., *A Taxonomy Of Privacy*, in *University of Pennsylvania Law Review*, 154, 3, 2006, 477 ss.

SOLOVE D.J., CITRON D.K., *Risk and Anxiety: A Theory of Data-Breach Harms*, in *Texas Law Review*, 96, 2018, 737.

SORRENTINO F., *Lezioni sul principio di legalità*, Giappichelli, Torino, 2007.

SORRENTINO F., *Lezioni sulla riserva di legge*, I, Cooperativa libraria universitaria, Genova, 1980.

SPIVACK J., GARVIE C., *A Taxonomy of Legislative Approaches to Face Recognition in the United States*, in KAK A. (a cura di), *Regulating Biometrics: Global Approaches and Urgent Questions*, AI Now Institute, settembre 2020, 89 ss.

STANZIONE M.G., *Genesi ed ambito di applicazione*, in SICA S., D'ANTONIO V., RICCIO G.M. (a cura di), *La nuova disciplina europea della privacy*, cit., 13 ss.

STOA, *Data subjects, digital surveillance, AI and the future of work*, PE 656.305, dicembre 2020.

STRADELLA E., *La regolazione della Robotica e dell'Intelligenza artificiale: il dibattito, le proposte, le prospettive. Alcuni spunti di riflessione*, in *Media Laws*, 1, 2019, 73 ss.

SUNSTEIN C.R., *Il diritto della paura*, il Mulino, Bologna, 2010.

SUNSTEIN C.R., THALER R.H., *Nudge. Improving decisions about health, wealth, and happiness*, Penguin, London, 2009.

SWAN M., *The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery*, in *Big Data*, 1, 2, 2013, 85 ss.

TALLACCHINI M.C., *Ambiente e diritto della scienza incerta*, in GRASSI S., CECCHETTI M., A. ANDRONIO, *Ambiente e diritto*, I, Olschi, Firenze, 1999, 57 ss.

TARDIA I., *L'identità digitale tra memoria ed oblio*, ESI, Napoli, 2017.

TEGMARK M., *Vita 3.0. Essere umani nell'era dell'intelligenza artificiale*, Raffaello Cortina Editore, Milano, 2018.

TERRASI A., *Il rapporto tra diritto alla privacy e protezione dei dati personali tra Corte di giustizia dell'Unione europea e Corte europea dei diritti dell'uomo*, in DISTEFANO M. (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Editoriale Scientifica, Napoli, 2017, 127 ss.

TEUBNER G., *Soggetti giuridici digitali*, ESI, Napoli, 2019.

THOMAS V., *Report on Artificial Intelligence: Part I –the existing regulatory landscape*, 14 maggio 2018 [bit.ly/3uwmPy1].

THORNBURG R.H., *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment*, in *The John Marshall Journal of Information Technology & Privacy Law*, 20, 2, 2002, 321 ss.

TIMIANI M., *Un contributo allo studio sul diritto alla riservatezza*, in *Studi parlamentari e di politica costituzionale*, 2, 2012, 51 ss.

TINCANI P., *Sorveglianza e potere. Disavventure dell'asimmetria cognitiva*, in *Ragion pratica*, 1, 2018, 51 ss.

TINCANI P., *Controllo e sorveglianza*, in BRIGHI R., ZULLO S. (a cura di), *Filosofia del diritto e nuove tecnologie*, cit., 19 ss.

TJONG TJIN TAI E., *Liability for (Semi)Autonomous Systems: Robots and Algorithms*, in MAK V., TJONG TJIN TAI E., BERLEE A. (a cura di), *Research Handbook on Data Science and Law*, Edward Elgar, Cheltenham-Northampton, 2018, 55 ss.

TOFFALORI C., BOLOGNA C., *Algoritmi. Raccontare la matematica*, il Mulino, Bologna, 2015.

TOMASI M., *Genetica e Costituzione. Esercizio di eguaglianza solidarietà e responsabilità*, Editoriale Scientifica, Napoli, 2019.

TOMBS S., *Making better regulation, making regulation better?*, in *Policy Studies*, 4, 2016, 332 ss.

TOMMASINI R., *L'identità dei soggetti tra apparenza e realtà: aspetti di una ulteriore ipotesi di tutela della persona,* in ALPA G., BESSONE M., BONESCHI L. (a cura di), *Il diritto alla identità personale*, cit., 78 ss.

TONINI P., *Manuale di procedura penale*, GFL, Milano, 2019.

TONINI P., La *Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza*, in *Diritto penale e processo*, 11, 2011, 1341 ss.

TONINI P., CONTI C., *Il diritto delle prove penali*, Giuffrè, Milano, 2014.

TORRE M., Privacy *e indagini penali*, GFL, Milano, 2018.

TRIDIMAS T., *Proportionality in Community Law: Searching for the Appropriate Standard of Scrutinity*, in ELLIS E. (a cura di), *The Principle of Proportionality in the Laws of Europe*, Hart Publishing, Oxford-Portland, 1999, 65 ss.

TROISI P., *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, in SICA S., D'ANTONIO V., RICCIO G.M. (a cura di), *La nuova disciplina europea della privacy*, cit., 314 ss.

TROTTIER D., *Social Media as Surveillance. Rethinking Visibility in a Converging World*, London - New York, Routledge, 2016.

TRUCCO L., *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Giappichelli, Torino, 2004.

TZANOU M., *The EU as an emerging "Surveillance Society": The function creep case study and challenges to privacy and data protection*,

in *Vienna Journal on International Constitutional Law*, 4, 3, 2010, 407 ss.

U.S. CHAMBER OF COMMERCE, *Facial Recognition Policy Principles*, dicembre 2019 [bit.ly/3t3D718].

U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522, 11 agosto 2020 [bit.ly/3rUuT9X].

VALERA J., VALERA J., GELOGO Y., *A Review on Facial Recognition for Online Learning Authentication*, in *IEEE 2015 8th International Conference on Bio-Science and Bio-Technology (BSBT)*, 14 marzo 2016, 16 ss.

VALLI R.V.O., *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati da immagini*, in *il Penalista*, 16 gennaio 2019.

VAN DER PLOEG I., *Biometric identification technologies: ethical implications of the informatization of the body. Biometric Technology & Ethics, BITE Policy Paper no.1*, 2005.

VAN DIJCK J., *Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology*, in *Surveillance & Society*, 12, 2, 2014, 197 ss.

VAN DIJK N., GELLERT R., ROMMETVEIT K., *A Risk to a Right: Beyond Data Protection Risk Assessments*, in *Computer Law & Security Review*, 32, 2, 2016, 286 ss.

VAN NATTA ET AL., *The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic*, in *Journal of Law and the Biosciences*, 7, 1, gennaio-giugno 2020.

VANONI L.P., *L'applicazione del Bill of Rights europeo tra bilanciamento asimmetrico e paradosso federale: il caso della privacy digitale*, in *DPCE online*, 2, 2019, 1209 ss.

VASSALLI G., *Il diritto alla libertà morale (Contributo alla teoria dei diritti della personalità)*, in *Studi in memoria di Filippo Vassalli*, II, UTET, Torino, 1960, 1629 ss.

VAVOULA N., *Databases for Non-EU Nationals and the Right to Private Life: Towards a System of Generalised Surveillance of Movement?*, in BIGNAMI F. (a cura di), *EU Law in Populist Times*, Cambridge University Press, Cambridge, 2020, 227 ss.

VAVOULA N., *Interoperability of EU Information Systems: The*

Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?, in *European public law*, 26, 1, 2020, 131-156

VAVOULA N., *Police Information Exchange The future developments regarding Prüm and the API Directive*, PE 658.542, *Study Requested by the LIBE committee*, settembre 2020.

VEALE M., BINNS R., *Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data*, in *Big Data & Society*, 4, 2017.

VENANZONI A., *Intersezioni costituzionali – Internet e Intelligenze Artificiali tra ordine spontaneo, natura delle cose digitale e garanzia dei diritti fondamentali*, in *Forum di Quaderni Cost.*, 27 aprile 2018.

VERMEULE A., *The Constitution of Risk*, Cambridge, New York, 2014.

VESPIGNANI A., *L'algoritmo e l'oracolo. Come la scienza predice il futuro e ci aiuta a cambiarlo*, Il Saggiatore, Milano, 2019.

VIGANO L., MAGAZZENI D., *Explainable Security*, in arXiv:1807.04178 [cs.CR], 2018.

VIGEVANI G.E., *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, in *Il Diritto dell'informazione e dell'informatica*, 2, 2014, 207 ss.

VINAY A. ET AL., *Cloud Based Big Data Analytics Framework for Face Recognition in Social Networks using Machine Learning*, in *Procedia Computer Science*, 50, 2015, 623 ss.

VIOLA P., JONES M., *Rapid Object Detection Using a Boosted Cascade of Simple Features*, in *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2001, 511 ss.

VISINTINI G., *Dal diritto alla riservatezza alla protezione dei dati personali*, in *Il Diritto dell'informazione e dell'informatica*, 1, 2019, 1 ss.

WACHTER S., MITTELSTADT B., FLORIDI L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 7, 2, 2016, 76 ss.

WAGNER B., *Ethics as an Escape from Regulation: From Ethics-Washing to Ethics-Shopping?*, in BAYAMLIOĞLU E., BARALIUC I., JANSSENS L., HILDEBRANDT M. (a cura di), *Being Profiling. Cogitas ergo sum. 10 Years of Profiling the European Citizen*, Amsterdam University Press, Amsterdam, 2018, 84 ss.

WALTL B., VOGL R., *Explainable Artificial Intelligence – the New Frontier in Legal Informatics*, in *Jusletter IT*, 22 febbraio 2018.

WANG R., CAMPBELL A.T., ZHOU X., *Using Opportunistic Face Logging from Smartphone to Infer Mental Health: Challenges and Future Directions*, in *UbiComp/ISWC'15 Adjunct*, settembre 2015, 683 ss.

WANG Y., KOSINSKI M., *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images*, in *Journal of Personality and Social Psychology*, 114, 2, 2018, 246 ss.

WELINDER Y., *Face Recognition Privacy in Social Networks under German Law*, in *Communications Law Bulletin*, 31, 1, 2012.

WENG Y.-H., SUGAHARA Y., HASHIMOTO K., TAKANISHI A., *Intersection of "Tokku" Special Zone, Robots, and the Law: A Case Study on Legal Impacts to Humanoid Robots*, in *International Journal of Social Robotics*, 7, 5, 2015, 841 ss.

WESTIN A.F., *Privacy and Freedom*, Athenum, New York, 1967.

WIESE SCHARTUM D., *Making privacy by design operative*, in *International Journal of Law and Information Technology*, 24, 2, 2016, 151 ss.

WISCHMEYER T., RADEMACHER T. (a cura di), *Regulating Artificial Intelligence*, Springer, 2020.

WRIGHT E., *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, in *Fordham Intellectual Property, Media and Entertainment Law Journal*, 29, 2, 2019, 611 ss.

WU X., ZHANG X., *Automated inference on criminality using face images*, in *arXiv:1611.04135v1 [cs.CV]*, 26 maggio 2017.

XANTHAKI H., *European Union Legislative Quality After the Lisbon Treaty: The Challenges of Smart Regulation*, in *Statute Law Review*, 1, 2013, 66 ss.

YEUNG K., *Algorithmic Regulation: A Critical Interrogation*, in *Regulation & Governance*, 12, 2018, 505 ss.

YEUNG K., *'Hypernudge': Big Data as a mode of regulation by design*, in *Information, Communication & Society*, 20, 1, 2017, 118 ss.

YORDANOV A., *Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation*, in *European Data Protection Law Review*, 3, 4, 2017, 486 ss.

ZAGREBELSKY G., *Manuale di diritto costituzionale. I, Il sistema delle fonti del diritto*, Utet, Torino, 1988.

ZARSKY T.Z., *Incompatible: The GDPR in the Age of Big Data*, in *Seton Hall Law Review*, 47, 2017, 995 ss.

ZARSKY T.Z., *Understanding Discrimination in the Scored Society*, in *Washington Law Review*, 89, 2014, 1375.

ZEI A., *Principio di precauzione*, in *Dig. disc. pubbl.*, Agg. III, II, 2008, 670 ss.

ZENO ZENCOVICH V., Big data *e epistemologia giuridica*, in FARO S., FROSINI T.E., PERUGINELLI G. (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, il Mulino, Bologna, 2019, 13 ss.

ZENO-ZENCOVICH V., *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium iuris*, 1997, 466 ss.

ZENO-ZENCOVICH V., *Personalità (diritti della)*, in *Dig. disc. priv., sez. civ.*, XIII, 1995, 430 ss.

ZENO-ZENCOVICH V., *Identità personale*, in *Dig. disc. priv., sez. civ.*, IX, 1993, 294 ss.

ZICCARDI G., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, Milano, 2015.

ZUBOFF S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma, 2019.

ZUDDAS P., *Intelligenza artificiale e discriminazioni*, in *Consulta Online - Liber amicorum per Pasquale Costanzo*, 16 marzo 2020.

ZUDDAS P., *Pregiudizi digitali e principio di precauzione*, in *Consulta online*, 2, 2020, 408 ss.

ZUO F., DE WITH P.H.N.. *Real-time embedded face recognition for smart home*, in *IEEE Transactions on Consumer Electronics*, 51, 1, febbraio 2005, 183 ss.

Collana *Ricerche Giuridiche*

1. Vincenzo Atripaldi, *Diritto allo studio*, 1975
2. Massimo Panebianco, *Ugo Grozio e la tradizione storica del Diritto Internazionale*, 1975
3. Fulvio Fenucci, *L'assistenza scolastica nelle leggi delle regioni ad autonomia ordinaria*, 1976
4. P. Rescigno, V. Atripaldi, F. Fichera, A. Budetta, M. Panebianco, M. De Dominicis, S. De Val Aurisicchio, *Strutture di potere, democrazia e partecipazione*, 1975
5. Enzo Maria Marenghi, *Aspetti delle competenze regionali in materia urbanistica*, 1976
6. Vincenzo Patalano, *Il delitto di mancanza alla chiamata delle armi*, 1976
7. E. Pacelli, A. Saraceni, *Nuova disciplina della edificabilità dei suoli*, 1977
8. A.M. Allagrande, G. Barbirotti, M. Della Casa, V. Grillo, A. Vitale, *Le proposte della commissione Gonella-Casaroli per la revisione del Concordato*, 1977
9. Giuliana Ziccardi Capaldo, *Le situazioni territoriali illegittime nel Diritto Internazionale*, 1977
10. Vincenzo Mileo, *Le comunioni tacite familiari*, 1977
11. Maria Vittoria Lupò Avagliano, *Regioni e riforma sanitaria*, 1978
12. Maria Vittoria Lupò Avagliano, *L'autonomia contabile regionale*, 1979
13. Francesco Caruso, *Le* Anstalten *nell'ordinamento italiano*, 1979
14. Vito Gallotta, *La formazione professionale nel quadro delle competenze delle regioni ad autonomia ordinaria*, 1979
15. Antonio Pistone, *La giurisdizione contabile della Corte dei Conti*, 1981
16. Silvio Lugnano, *Argomenti per uno studio di politica criminale*, 1982
17. Mario La Monica, *Oggetto giuridico e tipicità del delitto di ricorso abusivo al credito*, 1983
18. Mario La Monica, *Sul significato normativo del termine "reato"*, 1983
19. Antonio Pistone, *Il contenzioso tributario: un'ipotesi di riforma*, 1983
20. Giuseppe Maria Ruggiero, *L'organo internazionale*, 1984
21. Bartolomeo Selleri, *Il diritto di accesso agli atti del procedimento amministrativo*, 1984
22. Arturo De Luca, *Giustizia e legalità nella filosofia giuridica di Kant*, 1984
23. Francesco Domenico Riccioli, *La successione internazionale degli Stati al debito pubblico*, 1984
24. Bartolomeo Selleri, *Pubblica amministrazione e cittadino: alla ricerca della parità*, 1984
25. Giovanni Esposito, *La chiamata in correità*, 1988
26. Antonio Abet, *La guerra sociale. Potere e autorità nei rapporti tra ordinamento giuridico e comunità nazionale*, 1987
27. Sergio Moccia, *Carpzov e Grozio. Dalla concezione teocratica alla concezione laica del diritto penale*, 1988
28. Guido Clemente di San Luca, *Three papers*, 1990
29. Pasquale Landi, *Diritto ed economia. Saggio sulla "Riduzione della filosofia del diritto alla filosofia dell'economia"*, 1996
30. Cosimo Silvestro, *Contributo allo studio dell'inquadramento previdenziale*, 1996
31. Francesco Bertolini, *Rappresentanza parlamentare e attività di governo*, 1997

32. Maria Elisabetta de Franciscis, *Il Presidente degli Stati Uniti d'America. Costituzione e prassi*, 1996
33. Maria Luisa Tufano, *La c.d. eccezione di invalidità degli atti comunitari*, 1996
34. Raffaele Titomanlio, *Contributo in tema di risarcibilità dell'interesse legittimo*, 1996
35. Renata Spagnuolo Vigorita, *La liberalizzazione delle telecomunicazioni: dal monopolio alla concorrenza regolata*, 1998
36. Ferdinando Lignola, *L'applicazione della pena su richiesta delle parti La natura della sentenza. Questioni applicative*, 2000
37. Alfredo Contieri, *La programmazione negoziata. La consensualità per lo sviluppo. I principi*, 2000
38. Simone Valiante, *Pluralità dell'informazione e sistema radiotelevisivo*, 2001
39. Daniele Marrama, *La pubblicità ingannevole. Il giudice amministrativo e la natura giuridica delle decisioni delle* authorities, 2002
40. Giuliana Di Fiore, *Autorità di garanzia e interesse pubblico nelle comunicazioni integrate*, 2002
41. Chiara Orrei, *La tutela risarcitoria dell'interesse legittimo. Sviluppi giurisprudenziali e profili dogmatici*, 2002
42. Nino Paolantonio, *Contributo sul tema della rinuncia in diritto amministrativo*, 2003
43. Antonio Leo Tarasco, *La consuetudine nell'ordinamento amministrativo. Contributo allo studio delle fonti non scritte*, 2003
44. Simona D'Antonio, *Teoria e prassi nella tutela risarcitoria dell'interesse legittimo*, 2003
45. Alberto Zito, *Il danno da illegittimo esercizio della funzione amministrativa. Riflessioni sulla tutela dell'interesse legittimo*, 2003
46. Giancarlo Sorrentino, *Diritti e partecipazione nell'amministrazione di risultato*, 2003
47. Renata Spagnuolo Vigorita, *Politiche pubbliche del servizio sanitario*, 2003
48. Antonio Leo Tarasco, *Beni patrimonio e attività culturali: attori privati e autonomie territoriali*, 2004
49. Marco Calabrò, *Potere amministrativo e partecipazione procedimentale. Il caso ambiente*, 2004
50. Vincenzo Metafora, *Il danno non patrimoniale e la sua riconduzione nell'alveo dell'art. 2043 c.c. L'art. 2059 c.c. come sanzione civile indiretta*, 2004
51. Loredana Giani, *Funzione amministrativa ed obblighi di correttezza. Profili di tutela del privato*, 2005
52. Mariaconcetta D'Arienzo, *Profili costituzionali e regimi amministrativi nell'assetto del sistema radiotelevisivo*, 2005
53. Andrea Crismani, *I controlli esterni sulle pubbliche amministrazioni. Contributo alla sistemazione metodologica del procedimento di controllo sulla gestione*, 2005
54. Fortunato Gambardella, *Trasformazione urbana e modelli privatistici. Profili ricostruttivi delle società di trasformazione urbana*, 2005
55. Domenico D'Orsogna, *Contributo allo studio dell'operazione amministrativa*, 2005
56. Marialaura Cunzio, *La criminalità organizzata in Campania*, 2005
57. Francesca Attanasio, *Partecipazione di società di capitali in società di persone alla luce della riforma societaria*, 2005

58. Marina Speca, *Il processo di ristrutturazione del debito negli enti locali. Analisi degli strumenti più utilizzati e delle procedure da attivare*, 2005
59. Laura Lamberti, *Riflessioni sulle funzioni amministrative delle Regioni e degli Enti locali*, 2006
60. Alessandro Martini, *Profili giuridici della procreazione medicalmente assistita*, 2006
61. Maria Gabriella Ivone, *Riflessioni in tema di unioni di fatto. Le esperienze italiana e francese a confronto*, 2006
62. Luisa Marin, *Il principio di mutuo riconoscimento nello spazio penale europeo*, 2006
63. Salvatore Dettori, *Il rapporto di presupposizione nel diritto amministrativo. Contributo allo studio della funzione complessa*, 2006
64. Carla Acocella, *Pubblico e privato nella gestione dei servizi pubblici. Il contratto di servizio*, 2007
65. Luca Pardi, *Contributo allo studio del contratto di* leasing *per la realizzazione delle opere pubbliche per la realizzazione delle opere pubbliche*, 2007
66. Annalisa Giusti, *Contributo allo studio di un concetto ancora indeterminato: la discrezionalità tecnica della pubblica amministrazione*, 2007
67. Camillo Patriarca, *La distribuzione degli utili in natura*, 2008
68. Angelo Lalli, *Disciplina della concorrenza e diritto amministrativo*, 2008
69. Ivan Ingravallo, *Le amministrazioni territoriali dell'ONU*, 2008
70. Gabriella Ferranti, *La cooperazione giudiziaria in materia penale nelle convenzioni del Consiglio d'Europa e nel diritto dell'Unione europea*, 2008
71. Fulvio Maria Palombino, *Gli effetti della sentenza internazionale nei giudizi interni*, 2008
72. Gerardo Soricelli, *Il responsabile del procedimento amministrativo*, 2009
73. Giancarlo Sorrentino, *Interesse legittimo e pregiudizialità amministrativa*, 2010
74. Ilaria Amelia Caggiano, *Circolazione del denaro e strumenti di tutela*, 2010
75. Marta Simoncini, *La regolazione del rischio e il sistema degli standard. Elementi per una teoria dell'azione amministrativa attraverso i casi del terrorismo e dell'ambiente*, 2010
76. Anna Lazzaro, *Contributo in tema di risarcimento del danno da ritardo*, 2011
77. Loredana Strianese, *Il contratto preliminare tra vincoli civilistici ed evoluzione dell'ordinamento tributario*, 2011
78. Diego Rossano, *Mediazione, Camera di conciliazione, Arbitro bancario finanziario*, 2012
79. Luca Pardi, *Gli strumenti di mercato a tutela dell'ambiente.* Nuove *forme di partecipazione responsabile e sussidiaria, dei privati all'esercizio delle funzioni*, 2012
80. Marta Tigano, *Tra economie dello Stato ed «economia» della Chiesa: i beni culturali d'interesse religioso*, 2012
81. Dario Bevilacqua, *Il* Free-Trade *e l'*Agorà, *Interessi in conflitto, regolazione globale e democrazia partecipativa*, 2012
82. Mario Quaranta, *Concertazione sociale e regole del lavoro,* 2012
83. Alfonso Maria Cecere, *Prime riflessioni sul potere amministrativo di coazione. Dalle restrizioni alle coercizioni nei confronti dei privati*, 2012
84. Alessandro Auletta, *Gli ausili pubblici tra autorità e consenso*, 2012
85. Giovanni Cocozza, *La decisione plurale in conferenza di servizi*, 2012

86. Francesca Di Lascio, *Le ispezioni amministrative sulle imprese. Analisi teorica e diritto positivo*, 2012
87. Simona D'Antonio, *Il commissario ad acta nel processo amministrativo. Qualificazione dell'organo e regime processuale degli atti*, 2012
88. Simona Di Stasio, *La politica migratoria europea: da Tampere a Lampedusa*, 2012
89. Fortunato Gambardella, *Contributo allo studio del regime giuridico dei bandi da gara*, 2012
90. Pierluigi Simone, *Origini e sviluppo della cooperazione internazionale ed europea di polizia. Modelli e soluzioni operative*, 2012
91. Tiziana di Iorio, *Società multietnica e libertà religiosa del minore tra affidamento e autodeterminazione*, 2013
92. Gianluca Bellomo, *Le normazioni tecniche volontarie nel diritto pubblico ambientale*, 2013
93. Francesca Perrini, *La protezione diplomatica delle società*, 2013
94. Paola Saracini, *Contratto a termine e stabilità del lavoro*, 2013
95. Carlo Iannello, *Il diritto all'acqua. Proprietà collettiva e Costituzione*, 2013
96. Marco Tiberi, *La tutela dell'interesse legittimo nella pluralità delle azioni*, 2013
97. Claudio Valerio Cogliandro, *Tutela della* privacy *e accesso ad internet nell'opera di Stefano Rodotà*, 2013
98. Anna Pitrone, *Le responsabilità internazionale delle organizzazioni intergovernative*, 2013
99. Francesca Ferraro, *Lo spazio giuridico europeo tra sovranità e diritti fondamentali. Democrazia, valori e* rule of law *nell'Unione al tempo della crisi*, 2014
100. Lorenzo Zoppoli, Antonello Zoppoli, Massimiliano Delfino (a cura di), *Una nuova Costituzione per il sistema di relazioni sindacali?*, 2014
101. Massimo Luigi Ferrante, *Principio di libertà personale e sistema penale italiano*, 2014
102. Gabriele Pepe, *La primazia negli organi collegiali pubblici*, 2014
103. Luca Buscema, *Lo stato di guerra in tempo di pace*, 2014
104. Francesco Rotondo, *Itinerari alla periferia di Lombroso. Pietro Gori e la "Criminologia moderna" in Argentina*, 2014
105. Paola Torretta, *L'incandidabilità al mandato parlamentare. La "legge Severino" oltre il "caso Berlusconi"*, 2015
106. Sara Valaguzza, *Sustainable Development in Public Contracts. An example of Strategic Regulation*, 2016
107. Luca Buscema (a cura di), *Identità nazionale e multiculturalismo*, 2016
108. Annamaria Gigli, *Nuove prospettive di tutela del legittimo affidamento nei confronti del potere amministrativo*, 2016
109. Tania Abbiate, *La partecipazione popolare ai processi costituenti: l'esperienza tunisina*, 2016
110. Andrea Patroni Griffi, *Le regole della bioetica tra legislatore e giudici*, 2016
111. Francesco Monceri*, La semplificazione dell'amministrazione nella crisi delle economie di mercato*, 2016
112. Gabriella De Maio, *Semplificazione e digitalizzazione: un nuovo modello burocratico*, 2016

113. Maria Teresa Stile, *La responsabilità dello Stato giudice e del magistrato tra garanzie costituzionali e moniti europei*, 2016
114. Gennaro Ferraiuolo, *Costituzione. Federalismo. Secessione. Un itinerario*, 2016
115. Massimiliano Delfino, *Salario legale. Contrattazione collettiva e concorrenza*, 2016
116. Silvia Tuccillo, *Contributo allo studio della funzione amministrativa come dovere*, 2016
117. Adele Del Guercio, *La protezione dei richiedenti asilo nel diritto internazionale europeo*, 2017
118. Alessandro F. Di Sciascio, *L'intervento sostitutivo nell'esercizio dell'attività amministrativa. Profili statici e dinamici*, 2017
119. Francesco Santoro, *L'abuso nel diritto civile e tributario*, 2017
120. Paola Bozzao, *Anzianità, lavori e diritti*, 2017
121. Gabriele Sabato, *La* Governance *per la rigenerazione dei siti contaminati. Il caso italiano de*i Brownfields, 2017
122. Fabiana Di Porto, *La regolazione degli obblighi informativi. Le sfide delle scienze cognitive e* dei big data, 2017
123. Francesco D'Ambrosi, *Consob e sistema di vigilanza*, 2017
124. Filomena Manganiello, *Interesse nazionale, interessi europei e vincoli alla potestà normativa regionale*, 2017
125. Eugenio D'Apuzzo, *Profili della cessazione della materia del contendere nel processo amministrativo*, 2017
126. Luca Calcaterra, *La somministrazione di lavoro. Teorie e ideologie*, 2017
127. Marcello Di Francesco Torregrossa, *La pubblica amministrazione nella società digitale*, 2017
128. Giovanni Cocozza, *Il percorso conformativo dell'eccesso di potere giurisdizionale. Una ricerca sul vizio della funzione e sul suo giudice*, 2017
129. Gabriele Pepe, *The Notion of* primus inter pares *in Italian public life today*, 2017
130. Luca Longhi, *Studio sulla responsabilità disciplinare dei magistrati*, 2017
131. Paola Saracini, Lorenzo Zoppoli (a cura di), *Riforme del lavoro e contratti a termine*, 2017
132. Eleonora Sirsi, *OGM e agricoltura. Evoluzione del quadro normativo, strategie di comunicazione, prospettive dell'innovazione*, 2017
133. Alfonso Vuolo, La *legge elettorale. Decisone politica, controlli, produzione giurisprudenziale*, 2017
134. Giorgia Bevilacqua, *Criminalità e sicurezza in alto mare*, 2017
135. Stefania Romeo, *«Usus auctoritas». Le XII tavole e la tutela dell'«apparenza» della proprietà,* 2017
136. Fiorenzo Liguori, Silvia Tuccillo (a cura di), *Contratti pubblici. Trasformazioni e problemi*, 2017
137. Maria Assunta Icolari, *Per una dogmatica dell'imposta ambientale*, 2018
138. Sara Lieto, *Giudizio costituzionale incidentale. Adattamenti, contaminazioni, trasformazioni*, 2018
139. Valeria Nuzzo, *La protezione del lavoratore dai controlli impersonali*, 2018
140. Luca Gori, *Le elezioni primarie nell'ordinamento costituzionale*, 2018

141. Antonio Loffredo, *Democrazia aziendale, imprese transnazionali e* dumping *sociale*, 2018
142. Donatella Loprieno, *"Trattenere e punire". La detenzione amministrativa dello straniero*, 2018
143. Elisabetta Codazzi, *La* società in house. *La configurazione giuridica tra autonomia e strumentalità*, 2018
144. Valentina Gastaldo, *L'*Astreinte *nel processo amministrativo*, 2018
145. Giovanni Martini, *Potere sanzionatorio della P.A. e diritti dell'uomo. I vincoli CEDU all'amministrazione repressiva*, 2018
146. Carlo Ferruccio Ferrajoli, *Rappresentanza politica e responsabilità. La crisi della forma di governo parlamentare in Italia*, 2018
147. Vittorio Minervini, *Insolvenza e mercato. Itinerari per la modernizzazione delle discipline sulla crisi d'impresa*, 2018
148. Renata Spagnuolo Vigorita, *Il conflitto tra pubblica amministrazione e privati. Modelli per la composizione*, 2018
149. Giovanni Poggeschi, *La Catalogna: dalla nazione storica alla repubblica immaginaria*, 2018
150. Umberto Ronga, *La legislazione negoziata. Autonomia e regolazione nei processi di decisione pubblica*, 2018
151. Guerino Fares, *Prestazioni sociali tra garanzie e vincoli*, 2018
152. Fabio Francesco Pagano, *Legittimo affidamento e attività legislativa*, 2018
153. Giuseppe Micciarelli, Commoning. *Beni comuni urbani come nuove istituzioni. Materiali per una teoria dell'autorganizzazione*, 2018
154. Giacomo D'Amico, *Azione di accertamento e accesso al giudizio di legittimità costituzionale*, 2018
155. Sveva Bocchini, *Lo statuto del sito contaminato e il vincolo ambientale ripristinatorio*, 2018
156. Francesca Biondi Dal Monte, *Dopo la legge. Tendenze e prospettive dell'attuazione e delle fonti primarie tra Governo e Parlamento*, 2018
157. Alessandro Morelli (a cura di), *Dal "Contratto di Governo" alla formazione del Governo Conte. Analisi di una crisi istituzionale senza precedenti*, 2018
158. Alessandro Morelli, *Rappresentanza politica e libertà del mandato parlamentare*, 2018
159. Massimiliano Delfino, *Salario legale e contrattazione collettive e concorrenza*, 2018
160. Irene Coppola, *Contributo allo studio del processo civile* in *appello*, 2018
161. Marta Ferrara, *Capo dello Stato, vincoli europei e obblighi internazionali. Nuove mappe della garanzia presidenziale*, 2019
162. Giuseppe Allegri, Alessandro Sterpa, Nicola Viceconte (a cura di), *Questioni costituzionali al tempo del populismo e del sovranismo*, 2019
163. Monica Cocconi (a cura di), *Sostenibilità, responsabilità sociale d'impresa e nuove aspettative dei consumatori: nuovi paradigmi di qualità?*, 2019
164. Luca Di Majo, *La qualità della legislazione tra regole e garanzie*, 2019
165. Irene Coppola, *Capitale umano o sistemi robotici. Un nuovo processo in Italia*, 2019
166. Pamela Lattanzi, *I prodotti di frontiera. Il caso degli «integratori alimentari botanici»*, 2019

167. Sergio Marotta, *Le forme dell'acqua. Economia e politiche del diritto nella gestione delle risorse idriche*, 2019
168. Donatella Illuminato, *Inadempimento non imputabile e impossibilità sopravvenuta. Un'endiadi nel diritto?* 2019
169. Giuseppe Papale, Raffaele Gaetano Crisileo, *Storia dell'oratoria forense. Comunicazione e persuasione*, 2019
170. Ubaldo Perfetti (a cura di), *Il punto sui così detti danni punitivi*, 2019
171. Francesca Martines, *La funzione d'iniziativa della Commissione nel processo legislativo dell'Unione europea*, 2019
172. Giacomo Gargano, *Lo Stato e gli Enti di diritto pubblico quali soggetti passivi del rapporto giuridico tributario*, 2019
173. Emma A. Imparato, *L'eccezione nella regola*, 2019
174. Adriano Maffeo, *Diritto dell'Unione europea e processo civile nazionale*, 2019
175. Antonio Ignazio Arena, *L'esternazione del pubblico potere*, 2019
176. Francesco Paterniti, *Figli e ordinamento costituzionale*, 2019
177. Francesco Raffaello De Martino, *Presidente della Repubblica e scioglimento delle camere*, 2019
178. Giacomo Delledonne, *Costituzione e legge elettorale*, 2019
179. Ferdinando Franceschelli, *L'impatto dei cambiamenti climatici nel diritto internazionale*, 2019
180. Luca Pedullà, *La costituzionalizzazione del giusto procedimento*, 2019
181. Sara Poli, *Le misure restrittive autonome dell'Unione europea*, 2019
182. Gabriella Di Maio, *Fiscalità energetica e cambiamento climatico. Il ruolo del diritto tributario nella società moderna*, 2020
183. Eloísa Carbonell Porras, Giuseppe Piperata (a cura di), *La reforma del gobierno local en España e Italia*, 2020
184. Anna Gragnani, *La codificazione del diritto ambientale: il modello tedesco e la prospettiva italiana*, 2020
185. Mena Minafra, *Osservazioni sulla "chiamata in correità"*, 2020
186. Antonio Mitrotti, *L'interesse nazionale nell'ordinamento italiano*, 2020
187. Giacomo D'Amico, *La libertà "capovolta"*, 2020
188. Viviana Di Capua, *L'auotorizzazione integrata ambientale*, 2020
189. Alessandro Sterpa, Alessandra Coiante (a cura di), *Sicurezza, legalità ed economia*, 2020
190. Sara Lieto, *Processo e partecipazione nel controllo di costituzionalità*, 2020
191. Cristiana Carletti, *Diritto alla riservatezza, protezione dei dati personale e spazio digitale nell'ordinamento internazionale*, 2020
192. Roberta Alfano, *Sanzioni amministrative tributarie e tutela del contribuente*, 2020
193. Maria Teresa Stile, *Discrezionalità legislativa e discrezionalità giurisdizionale nei processi evolutivi del costituzionalismo*, 2020
194. Shkelzen Hasanaj, *Diritti delle minoranze. Tra immigrazione e globalizzazione*, 2020
195. Stefano Aru, *La continuità del regionalismo italiano*, 2020
196. Laura Tebano, *Lavoro, potere direttivo e trasformazioni organizzative*, 2020

197. Giovanni Cocozza, *Contributo a uno studio sulla motivazione del provvedimento come essenza della funzione amministrativa*, 2020
198. Maria Antonella Gliatta, *La dialettica della centralità. Studio sull'iniziativa legislativa del Governo*, 2020
199. Stefano D'Alfonso, *Potere d'inchiesta parlamentare e sistema di protezione dei diritti*, 2020
200. Costanza Nardocci, *Il "diritto" al giudice costituzionale*, 2020
201. Michela Troisi, *Le pronunce che costano. Poteri istruttori della Corte costituzionale e modulazione delle conseguenze finanziarie delle decisioni*, 2020
202. Umberto Ronga, *La delega legislativa. Recente rendimento del modello*, 2020
203. Carlo Iannello, *Salute e libertà. Il* fondamentale diritto *all'autodetrminazione individuale*, 2020
204. Massimo Cavino, Lucilla Conte, Simone Mallardo, Massimiliano Malvicini, *Un'imprevista emergenza nazionale. L'Italia di fronte al COVID-19*, 2020
205. Vito Breda, Matteo Frau (a cura di), *La contrattazione Costituizionale dei livelli di autonomia. Modelli per una comparazione*, 2020
206. Katia La Regina (a cura di), *La custodia cautelare in carcere*, 2020
207. Giovanna Petrillo, *I limiti di proporzionalità nella disciplina fiscale delle società di comodo*, 2020
208. Andrea Maltoni (a cura di), *I contratti pubblici: la difficile stabilizzazione delle regole e la dinamica degli interessi*, 2020
209. Stefania Cecchini, *La Corte costituzionale paladina dell'eguaglianza di genere*, 2020
210. Paola Mazzina, *L'autonomia politica regionale tra modelli costituzionali e sistema dei partiti*, 2020
211. Mario Iannella, *La* governance *economica cooperativa. Autonomia e raccordi negli Stati Uniti e nell'Eurozona*, 2020
212. Virgilia Fogliame, *Parità di genere e rappresentanza. Il rendimento delle misure legislative promozionali*, 2020
213. Armando de Crescenzo, *Indirizzo politico: una categoria tra complessità e trasformazione,* 2020
214. Tiziana Montecchiari, *Il biotestamento e l'amministrazione di sostegno*, 2020
215. Rosa Casillo, *Diritto al lavoro e dignità*, 2020
216. Gianluca Bellomo, *Profili pubblicistici del* Data Protection Officer *nel sistema multilivello di tutela della* privacy, 2020
217. Lucilla Conte, *La famiglia. Istituti e istituzioni nella prospettva costituzionale*, 2020
218. Arianna Carminati*, Oltre la leale collaborazione. Al crocevia delle attribuzioni costituzionali dello Stato*, 2020
219. Antonello Tarzia, *Il giudice e lo straniero. Linguaggi e culture nei percorsi giurisdizionali*, 2020
220. Maria Laura Rea, *Public e Private enforcement Antitrust. La tutela della concorrenza tra riforme europee e ordinament italiano*, 2020
221. Erik Furno, *Il presidente della Repubblica al tempo delle crisi*, 2021
222. Luca Galli, *Rethinking Integration Contracts. The role of admistrative law in building an intercultural society*, 2021

223. Antoni Ignazio Arena, *Libertà e pluralismo nella formazione delle leggi costituzionali*, 2021

Finito di stampare nel mese di aprile 2021
presso la *Grafica Elettronica* (Na)