PROFILI SISTEMATICI DELLE TECNOLOGIE DI RICONOSCIMENTO FACCIALE AUTOMATIZZATO, ANCHE ALLA LUCE DEI FUTURIBILI SVILUPPI NORMATIVI SUL FRONTE EUROUNITARIO

di Gianluca Borgia

(Assegnista di ricerca in Diritto processuale penale, Università di Pisa)

SOMMARIO: 1. Introduzione. – 2. La posizione del Garante nazionale per la protezione dei dati personali sul “*Sistema Automatico di Riconoscimento delle Immagini*” (SARI). 3. Tecnologie di riconoscimento facciale e accertamento penale: possibili scenari. 3.1. Il fascino irresistibile dell’art. 189 Cpp – 3.2. L’imprescindibile valorizzazione del diritto alla *privacy*, anche in pubblico. – 3.3. Auspicabili prospettive: la proposta di regolamento della Commissione UE sull’intelligenza artificiale. – 4. Conclusioni.

1. La profonda disillusione con cui ormai molti guardano ai vieppiù frequenti impieghi delle tecnologie basate sull’intelligenza artificiale per finalità di *law enforcement*¹ non ha risparmiato neppure quei congegni – sviluppati in tempi relativamente recenti – che consentono l’identificazione automatica di un individuo mediante il confronto tra la fotografia o il video che ne raffigurano il volto e le

¹ Si pensi alle reazioni suscitate dalla pronuncia resa dalla Corte Suprema del Wisconsin nel celebre caso *Loomis*. In proposito e, più in generale, sugli interrogativi posti dai cc.dd. “*risk assessment tools*”, cfr. S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings, A Framework for A European Legal Discussion*, Cham 2020, 156 ss.; Ead., *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale “predittiva”*, in *CP* 2019, 1750 ss.; M. Gialuz, *Quando la giustizia penale incontra l’intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *www.penalecontemporaneo.it*, 29.5.2019, 6 ss.; G. Contissa, G. Lasagni e G. Sartor, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di Internet* 2019, f. 4., 622 ss.; F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *www.dirittopenaleuomo.org*, 29.9.2019, 21 ss.; L. Maldonato, *Algoritmi predittivi e discrezionalità del giudice: una nuova sfida per la giustizia penale*, in *DPenCont* 2019, f. 2, 403 ss.; e, più di recente, G. Canzio, *Intelligenza artificiale, algoritmi e giustizia penale*, in *www.sistemapenale.it*, 8.1.2021; A. M. Maugeri, *L’uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali*, in *www.archiviopenale.it*, 17.5.2021, 13 s. e 19 ss.; E. Nagni, *Artificial intelligence, l’innovativo rapporto di (in)compatibilità fra machina sapiens e processo penale*, in *SP* 2021, f. 7, 5 ss.

Si ponga mente altresì all’intervento normativo con cui il legislatore francese ha criminalizzato il c.d. “*judge profiling*”; cfr. F. G’sell, *Les progrès à petits pas de la «justice prédictive» en France*, in *ERA Forum* 2020, f. 21, 303 ss. e, nella letteratura interna, B. Galgani, *Considerazioni sui “precedenti” dell’imputato e del giudice al cospetto dell’IA nel processo penale*, in *SP* 2020, f. 4, 87 ss.

immagini contenute in un database di riferimento².

Nello specifico, il funzionamento delle cc.dd. “Automated Facial Recognition Technologies” (da qui in avanti: “AFRTs”), alla stregua degli altri sistemi che si avvalgono della biometria³, si articola in una prima fase di acquisizione del “dato biometrico grezzo” rappresentato, appunto, dall’immagine di un volto umano. Successivamente, il sistema rileva talune caratteristiche del viso⁴ funzionali alla creazione di un “template” o “modello biometrico”, che viene poi comparato con i dati archiviati⁵. Nel caso in cui, all’esito dell’operazione di raffronto, emerga con una certa probabilità che le due immagini si riferiscono alla stessa persona⁶, si avrà il c.d.

² V. Article 29 Data Protection Working Party, *Opinion 02/2012 on facial recognition in online and mobile services*, 22.3.2012, p. 2 (reperibile al seguente link: <https://www.pdpjournals.com/docs/87997.pdf>).

³ Per la definizione di “biometria” quale «disciplina che studia le grandezze biofisiche allo scopo di identificarne i meccanismi di funzionamento, di misurarne il valore e di indurre un comportamento desiderato in specifici sistemi tecnologici» v. voce “Biometria”, in *Enciclopedia Treccani online*, (<https://www.treccani.it/enciclopedia/biometria/>).

Con riferimento ai sistemi di riconoscimento biometrico più diffusi v. E. Sacchetto, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *DPenCont* 2019, f. 2, 469 ss., nonché il volume a cura di M. Tistarelli-C. Champod, *Handbook of Biometrics for Forensic Science*, Cham 2017.

⁴ In particolare, viene in considerazione «la posizione degli occhi, del naso, delle narici, del mento e delle orecchie»: R. Lopez, *Riconoscimento facciale tramite software e individuazione del sospettato*, in *Le Pre-investigazioni*, a cura di A. Scalfati, Torino 2020, 298. Sul punto v. altresì E. Sacchetto, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in www.la legislazione penale.eu, 16.10.2020, 3, nota n. 12.

⁵ V., più diffusamente, Article 29 Data Protection Working Party, *Opinion 02/2012 on facial recognition in online and mobile services*, cit., 2, dove si afferma che «[t]he process of facial recognition itself is comprised of a number of discrete sub-processes:

a) *Image acquisition: The process of capturing the face of an individual and converting to a digital form (the digital image). In an online and mobile service the image may have been acquired in a different system, e.g. taking a photograph with a digital camera which is then transferred to an online service.*

b) *Face detection: The process of detecting for the presence of a face within a digital image and marking the area.*

c) *Normalisation: The process to smooth variations across detected facial regions, e.g. converting to a standard size, rotating or aligning colour distributions.*

d) *Feature extraction: The processing of isolating and outputting repeatable and distinctive readings from the digital image of an individual. Feature extraction can be holistic², feature-based³ or a combination of the two methods⁴. The set of key features may be stored for later comparison in a reference template⁵.*

e) *Enrolment: If this is the first time an individual has encountered the facial recognition system the image and/or reference template may be stored as a record for later comparison.*

f) *Comparison: The process of measuring the similarity between a set of features (the sample) with one previously enrolled in the system. The main purposes of comparison are identification and authentication/verification. A third purpose of comparison is categorisation which is the process of extracting features from an image of an individual in order to classify that individual in one or several broad categories (e.g. age, gender, colour of clothes, etc). It is not necessary for a categorisation system to have an enrolment process».*

⁶ Cfr. il documento elaborato dalla European Union Agency for Fundamental Rights intitolato “Facial recognition technology: fundamental rights considerations in the context of law enforcement”, 7 (consultabile al seguente indirizzo: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-

“*matching*”⁷.

Le tecnologie in questione possono essere impiegate tanto in chiave di “verifica”, quanto di “identificazione” biometrica. Nel primo caso, viene operato un «confronto “uno a uno”» tra il modello biometrico rilevato e quello già in possesso dell’autorità associato ad un nominativo che si intende appunto verificare. Nel secondo, mediante la comparazione «“uno a molti”» tra il *template* registrato e quelli disponibili, si mira a scoprire l’identità di un individuo⁸.

Le potenzialità dischiuse dalle *AFRTs*, sia in prospettiva di prevenzione che di repressione dei reati, sono senza dubbio notevoli.

Si consideri che, a differenza di altre metodiche di identificazione biometrica, prima fra tutte quella basata sul DNA, il riconoscimento facciale «ha il vantaggio di non essere invasivo», potendosi prescindere dalla collaborazione del soggetto destinatario della rilevazione⁹. Detto altrimenti – e segnatamente con le parole utilizzate dal *New York City Bar Association’s Criminal Courts Committee* – le *AFRTs* risultano particolarmente performanti in quanto il volto è «qualcosa che è difficile da nascondere e», al contempo, «facile da osservare in luoghi aperti»¹⁰.

A ciò deve aggiungersi che l’implementazione di dette tecnologie risulta agevolata dalla possibilità di avvalersi delle «reti di telecamere preesistenti»¹¹.

Allo stesso modo, per quanto riguarda il “bacino” di informazioni da cui attingere per l’operazione di raffronto, è possibile ricorrere a «banche dati costituite» per finalità “altre”, come nel caso di quelle «relative alle licenze di guida»¹².

A quest’ultimo proposito, occorre sottolineare che i sistemi di ultima generazione hanno determinato una rottura degli argini entro cui era tradizionalmente confinata l’operatività dei *software* di riconoscimento facciale. Il riferimento corre a quelle tecnologie come l’*app* sviluppata dalla *start-up* Clearview AI che, in luogo di sfruttare i fotogrammi contenuti nei database gestiti dalle autorità

[technology-focus-paper.pdf](#)), in cui si rileva criticamente che i «*[f]acial recognition technology algorithms never provide a definitive result, but only probabilities that two faces appertain to the same person*» (34). Nello stesso senso R. Lopez, *Riconoscimento facciale tramite software e individuazione del sospettato*, cit., 316.

⁷ E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in www.dirittopenaleuomo.org, 19. 5.2021, 3, nota n. 3.

⁸ R. Lopez, *Riconoscimento facciale tramite software e individuazione del sospettato*, cit., 298.

⁹ E. Sacchetto, *Face to face*, cit., 1 s., la quale sottolinea altresì che «il sistema non risulta nemmeno assoggettabile a cambiamenti comportamentali, volontari o meno, da parte dell’individuo sottoposto al riconoscimento».

¹⁰ New York City Bar Association’s Criminal Courts Committee, “*Power, Pervasiveness and Potential: The Brave New World of Facial Recognition Through a Criminal Law Lens (and Beyond)*”, 2, (traduzione a cura nostra), consultabile all’indirizzo <https://s3.amazonaws.com/documents.nycbar.org/files/2020662-BiometricsWhitePaper.pdf>.

¹¹ *Ibidem* (traduzione a cura nostra).

¹² *Ibidem* (traduzione a cura nostra).

statali, utilizzano le immagini reperibili sul web anche attraverso social networks quali Facebook, Twitter, Instagram, YouTube e LinkedIn¹³.

Ancora si pensi che, accanto a strumenti concepiti per condurre l'analisi di volti rappresentati in immagini statiche, ve ne sono altri in grado di processare in diretta più flussi video provenienti sia da telecamere fisse, sia da dispositivi mobili come *body cameras* o droni. La modalità c.d. “*real time*” permette, dunque, di conoscere immediatamente se un determinato individuo sospettato di aver commesso o, addirittura, di poter commettere un reato, si trovi nel luogo sottoposto a osservazione¹⁴. Va da sé che in questo caso il sistema è in grado di immagazzinare informazioni relative ad «un numero indeterminato di soggetti» «spesso estranei all'attività di indagine»¹⁵.

Ebbene, se per un verso non stupisce che i *tools* di cui si va trattando abbiano riscosso grande successo in molti ordinamenti a livello globale, per l'altro è apparso chiaro fin da subito come l'utilizzo delle *AFRTs* non sia a costo zero per i diritti e le libertà fondamentali.

Come si avrà modo di osservare dallo specifico angolo visuale del diritto processuale penale, le principali criticità riguardano i profili dell'affidabilità, della trasparenza, nonché il rispetto dei principi di legalità e proporzionalità¹⁶.

2. Lo spunto per occuparci della tematica con riferimento all'ordinamento italiano è offerto dal parere del Garante nazionale della privacy reso lo scorso 25 marzo in merito al “*SARI-Real Time*”¹⁷, ossia lo strumento di riconoscimento facciale in tempo reale che il Ministero dell'Interno si apprestava ad attivare.

La questione non è del tutto nuova, in quanto l'Autorità per la protezione dei dati personali aveva già avuto modo di pronunciarsi sullo scenario statico del

¹³ Cfr. I. Neroni Rezende, *Facial recognition in police hands: Assessing the “Clearview case” from a European perspective*, in *NJECL* 2020, vol. 11, n. 3, 375 ss., secondo la quale «Clearview now combines its technology with a database of three billion images published on internet» (376).

¹⁴ J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *DPenCont* 2020, f. 1, 232 s.

¹⁵ E. Currao, *op. cit.*, 5.

¹⁶ Per un'analisi ad ampio spettro delle problematiche poste dalle *AFRTs* si rinvia, con riguardo rispettivamente al panorama eurounitario ed a quello statunitense, allo studio condotto dall'Agenzia dell'Unione europea per i diritti fondamentali intitolato “*Facial recognition technology: fundamental rights considerations in the context of law enforcement*”, 7 (consultabile al seguente indirizzo: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf); e al citato documento del New York City Bar Association's Criminal Courts Committee (v. *supra*, nota n. 10).

¹⁷ Garante per la protezione dei dati personali, *Parere sul sistema Sari Real Time*, 2.3.2021. In proposito cfr. G. Fasano, *Riconoscimento facciale: per il Garante il sistema del Viminale non è conforme alla normativa privacy*, in www.ntplusdiritto.ilsole24ore.com, 20.4.2021; A. Fonsi, *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in www.penaledp.it, 13.5.2021.

medesimo *software* denominato “SARI-Enterprise”¹⁸. A questo riguardo, era stata esclusa qualsiasi violazione della disciplina prevista dalla direttiva 2016/680/UE¹⁹, così come attuata nel nostro ordinamento dal d. lgs. 18.5.2018 n. 51²⁰, sul presupposto che non si sarebbe realizzato «un nuovo trattamento di dati personali», bensì «una nuova modalità di trattamento»²¹. Invero, si è affermato che se in precedenza le ricerche a fini identificativi nella banca dati A.F.I.S. – S.S.A.²² venivano condotte mediante l’inserimento manuale da parte dell’operatore dei connotati identificativi del soggetto da identificare o verificare, da quel momento in poi, siffatta operazione sarebbe avvenuta in automatico attraverso l’immissione nel sistema dell’immagine fotografica²³.

Sulla base di questa premessa, le disposizioni che disciplinano la suddetta banca dati sono state considerate sufficienti a soddisfare quanto stabilito dall’art. 7 d. lgs. 51/2018, secondo cui, il trattamento dei «dati biometrici intesi a identificare in modo univoco una persona fisica», in quanto *species* del *genus* «dati particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali», deve essere «specificamente previsto dal diritto dell’Unione europea o da legge o, nei casi previsti dalla legge, da regolamento»²⁴.

¹⁸ Garante per la protezione dei dati personali, *Sistema automatico di ricerca dell’identità di un volto*, 26.7.2018. Cfr. R. Lopez, *La rappresentazione facciale tramite software*, in *Le indagini atipiche*², a cura di A. Scalfati, Torino 2019, 248 ss.

¹⁹ Sulla c.d. “direttiva law enforcement” v. C. Di Francesco Maesa, *Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)*, in www.rivista.eurojus.it, 24.5.2016 e S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino 2018, 87 ss.

²⁰ In ordine ai contenuti di tale provvedimento normativo cfr., dallo specifico angolo visuale dei diritti fondamentali in gioco, B. Galgani, *Giudizio penale, habeas data e garanzie fondamentali*, in www.archiviopenale.it, 8.2.2019, nonché, volendo, anche per il raffronto con la disciplina previgente, G. Borgia, *Il trattamento di dati personali a fini di prevenzione, di indagine, di accertamento e di perseguimento di reati o di esecuzione di sanzioni penali: quali passi avanti alla luce dei recenti sviluppi?*, in *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, a cura di A. Mantelero e D. Poletti, Pisa 2018, 495 ss.

²¹ Garante per la protezione dei dati personali, *Sistema automatico di ricerca dell’identità di un volto*, cit., 2.

²² Si tratta dell’«Automated finger print identification system», «ovvero il sistema automatizzato di identificazione delle impronte digitali» integrato dal Sottosistema anagrafico, «contenente oltre le foto segnaletiche dei pregiudicati, anche i dati anagrafici e le informazioni riguardanti le loro caratteristiche biometriche, acquisiti in sede di foto segnalamento. Le funzionalità delle due banche dati in questione sono state, pertanto, implementate e replicate all’interno del S.A.R.I. *Enterprise* con l’obiettivo di garantire una soluzione applicativa unica, in grado di articolare la ricerca su un triplice livello: su base volto, cioè in riferimento all’immagine del volto; su base anagrafica/descrittiva, ossia tenendo conto delle informazioni anagrafiche o descrittive associate alle immagini nella banca dati dei foto segnalati; infine, su base combinata, in quanto elaborata tramite integrazione di entrambe le tipologie di dati»; R. Lopez, *Riconoscimento facciale tramite software e individuazione del sospettato*, cit., 300.

²³ *Ibidem*.

²⁴ L’attenzione del Garante si è poi appuntata sul successivo art. 8 d. lgs. 51/2018, a mente del quale, è vietato adottare decisioni basate unicamente su un trattamento automatizzato di dati biometrici, compresa la

Di segno opposto è, invece, l'opinione espressa con riferimento allo scenario operativo *Real Time*, che costituisce uno strumento del tutto inedito per la nostra esperienza, dal momento che «l'identificazione di una persona» «comporta il trattamento biometrico di tutte le persone che circolano nello spazio pubblico monitorato». Pertanto, prosegue il Garante, «si determina 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»²⁵.

Alla luce di questa premessa, nell'esaminare le diverse fonti indicate dal Ministero ai fini del rispetto, innanzitutto, del principio di legalità del trattamento ex art. 7 d. lgs. 51/2018, l'Autorità per la protezione dei dati personali chiarisce in primo luogo che, a differenza di quanto sostenuto dal Viminale, la base legale non può essere ravvista nello stesso d. lgs. 51/2018: non occorre, infatti, scomodare la teoria generale del diritto per comprendere che se una normativa rinvia ad un'altra disciplina per legittimare lo svolgimento di una determinata attività, siffatta legittimazione non può rintracciarsi nella prima fonte, dal momento che, altrimenti, il rinvio perderebbe di significato.

Quanto all'art. 1 del TuLPS, si sottolinea che tale disposizione stabilisce i compiti generali secondo cui si articola l'attività dell'Autorità di pubblica sicurezza e, pertanto, non può costituire una previsione che «autorizza specificamente» il trattamento in questione²⁶.

Rispetto al d.P.R. 15.1.2018 n. 15 relativo al trattamento dei dati attraverso sistemi di videosorveglianza e di ripresa fotografica, audio e video, se ne esclude la rilevanza in quanto «ontologicamente diversi da quelli» in esame. A supporto di tale affermazione viene richiamato il regolamento 2016/679/UE, a cui la direttiva 2016/680/UE – come noto – è legata da un rapporto di complementarità. Nello specifico, il c.d. “GDPR”, al considerando n. 51, chiarisce che «le fotografie» non

profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano in vigore misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato (co. 3) e sempre che la profilazione non sia finalizzata alla discriminazione di persone fisiche (co. 4) (cfr., B. Galgani, *Giudizio penale, habeas data e garanzie fondamentali*, cit., 20 ss.). Ribadito che il *SARI-Enterprise* rappresenta un «mero ausilio all'agire umano, avente lo scopo di velocizzare l'identificazione, da parte della polizia, di un soggetto ricercato della cui immagine si disponga», e «ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato» si deve concludere che «il trattamento in esame non può ritenersi riconducibile alle disposizioni di cui al citato articolo 8 e pertanto, anche sotto tale profilo, non si ravvisano elementi ostativi» (Garante per la protezione dei dati personali, *Sistema automatico di ricerca dell'identità di un volto*, cit., 2 s.).

²⁵ Garante per la protezione dei dati personali, *Parere sul sistema Sari Real Time*, cit., 3. Sulle caratteristiche della c.d. “sorveglianza di massa” v., da ultimo, W. Nocerino, *Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio*, Milano 2019, 327 ss.

²⁶ Garante per la protezione dei dati personali, *Parere sul sistema Sari Real Time*, cit., 4.

«rientrano» sempre e comunque «nella definizione di dati biometrici», ma «soltanto quando s[ono] trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca [...] di una persona fisica»²⁷.

Rilevato che il *SARI-Real Time* risulta concepito non solo per «coadiuvare» le «Forze di Polizia nella gestione dell'ordine e della sicurezza pubblica», ma anche per rispondere «a specifiche esigenze di Polizia Giudiziaria», il Garante si sofferma da ultimo sui molteplici articoli del codice di rito richiamati nella documentazione ministeriale (artt. 134 co. 4, 234, 266 e 431 co. 1 lett. *b* e artt. 55, 348, 354 e 370 Cpp), evidenziando che nessuno di essi prevede il trattamento di dati biometrici e, pertanto, non possono integrare «quella fonte normativa specifica richiesta dall'art. 7» d. lgs. 51/2018²⁸.

In definitiva, allo stato attuale non si rinviene una «base giuridica idonea»²⁹, il che rende l'implementazione del *SARI-Real Time* non conforme alla normativa eurounitaria in tema di trattamento dei dati personali per finalità di *law enforcement*³⁰.

3. Il parere negativo del Garante della privacy in ordine all'implementazione del *SARI-Real Time* – a cui ha fatto eco un disegno di legge volto a bandire l'utilizzo delle tecnologie in questione³¹ – non vale ad escludere che anche tale strumento possa essere

²⁷ *Ibidem*.

²⁸ *Ibidem*.

²⁹ *Ibidem*.

³⁰ Cfr. altresì Garante per la protezione dei dati personali, *Parere sulla valutazione di impatto del Ministero dell'Interno relativo ad un sistema di telecamere indossabili (body-cam), da Reparti mobili della Polizia di Stato, per la documentazione audio e video di situazioni critiche per l'ordine e la sicurezza, in occasione di eventi o manifestazioni pubbliche*, 22.7.2021, 7, con cui, per un verso, si è ritenuta conforme alla disciplina in materia di protezione dei dati personali l'iniziativa promossa dal Ministero dell'Interno, per l'altro, si è escluso che i dispositivi in questione possano essere impiegati in funzione di «identificazione univoca [...] o autenticazione di una persona fisica (facial recognition)».

³¹ Si tratta del d.d.l. AC 3009 del 12.4.2021, nel cui preambolo si legge che, preso atto di come sono «ormai molti i comuni italiani, compresi i grandi capoluoghi, che progettano di trasformare i loro sistemi di videosorveglianza in veri e propri sistemi di riconoscimento facciale» pur «in assenza di un quadro normativo che consenta di uniformare le condizioni per l'utilizzo dei dati biometrici da parte degli enti territoriali, in particolare per le funzioni di polizia giudiziaria riservate alla polizia locale», il disegno di legge propone di introdurre una «moratoria dell'utilizzo dei sistemi di riconoscimento facciale nei luoghi pubblici o aperti al pubblico [...] fino a quando non sarà adottata una normativa che assicuri il pieno rispetto dei diritti costituzionali dei cittadini, conformemente alle indicazioni delle autorità nazionali ed europee per la protezione dei dati personali».

Nelle more della pubblicazione del presente contributo, la suddetta iniziativa si è effettivamente tradotta in legge. Nello specifico, ciò è avvenuto in sede di conversione del d.l. 8.11.2021 n. 139 (c.d. «Capienze»). In attesa della pubblicazione in Gazzetta Ufficiale del provvedimento, per un primo commento v. A. Longo, *Italia primo Paese a vietare il riconoscimento facciale (con eccezioni)*, in www.ilsole24ore.com, 2.12.2021, il quale sottolinea in termini critici come, a fronte di un divieto generalizzato di impiego delle AFRTs da parte di «autorità pubbliche e soggetti privati» sino al 31 dicembre 2023, sia prevista un'eccezione di non poco momento, in quanto il divieto in parola non si applica «ai trattamenti (di dati personali per il riconoscimento biometrico, ndr.) effettuati dalle

impiegato nel processo penale, alla stregua di quanto sembra essere accaduto già in diverse occasioni in relazione al *SARI-Enterprise*³². Com'è stato osservato di recente proprio in tema di sistemi automatici di identificazione facciale, la disciplina in materia di trattamento di dati personali è irrilevante ai fini della «spendibilità processuale della prova raccolta mediante algoritmi di intelligenza artificiale»³³: infatti, l'art. 160-bis, inserito nel d. lgs. 30.6.2003 n. 196 (c.d. “codice della *privacy*”) dal d. lgs. 10.8.2018 n. 101, prevede che «[l]a validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali»³⁴.

Ne deriva che, per stabilire se e a quali condizioni una siffatta prova potrebbe essere utilizzata in sede di accertamento penale, occorre guardare al codice di rito.

3.1. A questo proposito, è legittimo attendersi che l'approccio che caratterizzerà la giurisprudenza, anche della Suprema Corte, sarà lo stesso adottato nei confronti delle altre «tecniche investigative inedite» di volta in volta scoperte e collaudate dalla «prassi poliziesca». Ed invero, si è opportunamente rimarcato come la tendenza pressoché costante sia quella di qualificare tali attività «alla stregua di mezzi atipici ma nel contempo legittimi di ricerca probatoria»³⁵.

In tale prospettiva merita quindi soffermarsi sulla lettura proposta da alcuni Autori, secondo i quali la prova in questione dovrebbe essere ricondotta al novero delle cc.dd. “nuove prove scientifiche”³⁶.

autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali di cui al decreto legislativo 18 maggio 2018, n. 51, in presenza, salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero, di parere favorevole del Garante reso ai sensi dell'articolo 24, comma 1, lettera b), del medesimo decreto legislativo n. 51 del 2018».

³² Risale al 7 settembre 2018 la notizia, diffusa da diverse testate giornalistiche, dell'arresto di due ladri a Brescia resa possibile dall'utilizzo del *SARI-Enterprise*.

³³ M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *DPP* 2021, 1052.

³⁴ Id., *Protezione dei dati personali, processo penale e intercettazioni*, ivi 2019, 167. In giurisprudenza, v., da ultimo, Cass., 2.12.2020, Carmina, in *CEDCass.*, m. 281638-01, secondo cui, «[i]n tema di prova documentale, sono utilizzabili i filmati che, realizzati mediante videoriprese legittimamente effettuate, sono stati conservati per un tempo superiore a quello consentito dall'art. 11 del d.lgs. 30 giugno 2003, n. 196, atteso che la protezione accordata dalla legge alla riservatezza non è assoluta ed è subvalente rispetto all'esigenza di acquisizione probatoria propria del processo penale. (Fattispecie in cui sono stati ritenuti utilizzabili i filmati degli impianti di videosorveglianza posti a presidio della sicurezza di una caserma, acquisiti e conservati per diversi mesi senza l'adozione di alcun provvedimento di sequestro e senza informare la Procura)».

³⁵ D. Negri, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *RIDPP* 2020, f. 1, 26. Nello stesso senso, più recentemente, N. Triggiani, *Legalità opaca: raccolta atipica e pre-investigazioni*, in www.archiviopenale.it, 15.3.2021,14.

³⁶ R. V. O. Valli, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in*

Più in particolare, si è affermato che il sistema automatico di riconoscimento «sembra in grado di poter svolgere» «funzioni giuridicamente sussumibili nel *genus*» dell'individuazione ex art. 361 Cpp e della ricognizione di persone prevista dagli artt. 213 ss. Cpp, a seconda che vengano in rilievo scopi, rispettivamente, investigativi o probatori in senso stretto³⁷.

Senonché, la natura “artificiale” e non “umana” del riconoscitore indurrebbe a qualificare tali mezzi istruttori come prove atipiche, con la conseguenza che dovrebbe trovare applicazione l'art. 189 Cpp³⁸.

Da qui, la necessità di considerare, anzitutto, il primo requisito richiesto dalla disposizione *de qua*, quello cioè dell'idoneità accertativa del fatto³⁹, che è stato ritenuto

immagini, in *www.ilpenalista.it*, 16.1.2019, § 3; conf. M. Torre, *Nuove tecnologie e trattamento dei dati personali*, cit., 1043, secondo il quale si tratta di un «sottoinsiem[e] della nuova prova scientifica di natura informatica». In giurisprudenza, non si può fare a meno di richiamare l'unica decisione della Suprema Corte di cassazione che, seppur incidentalmente, si è occupata della questione. Ed invero, nel rigettare le doglianze difensive con cui si contestava il mancato accoglimento in sede di gravame della richiesta di rinnovazione dell'istruttoria al fine di «procedere al riconoscimento facciale dell'imputato tramite la moderna tecnica S.A.R.I.», i giudici di Piazza Cavour hanno avallato il comportamento tenuto dalla Corte d'Appello, sottolineando come la «difesa non ave[ss]e in alcun modo documentato la valenza scientifica dell'anzidetta tecnologia» (Cass. 18.6.2019 n. 39731, in *DeJure*).

Sulla nozione di “prova scientifica nuova” v. O. Dominioni, *Prova scientifica (dir. proc. pen.)*, in *ED, Annali II* (t. I) 2008, 984 ss.; P. P. Rivello, *La prova scientifica*, Milano 2014, 109 ss.; nonché, dal particolare angolo prospettico del giudizio di revisione, R. Del Coco, *Giudicato, progresso scientifico e prova nuova. Limiti e prospettive del giudizio di revisione*, in *Errori giudiziari e background processuale*, a cura di L. Lupária, L. Marafioti e G. Paolozzi, Torino 2017, 109 ss.

³⁷ M. Torre, *Nuove tecnologie e trattamento dei dati personali*, cit., 1052, il quale sottolinea altresì che «[l]addove il riconoscimento abbia una finalità di mera *identificazione*, esso rientrerà nei poteri coercitivi della polizia (art. 4 Testo Unico delle leggi di pubblica sicurezza) oppure nelle prerogative investigative della polizia giudiziaria (art. 349 c.p.p.), a seconda che l'attività venga svolta, rispettivamente, per fini di pubblica sicurezza o per finalità processuali: *nulla quaestio*».

³⁸ *Ibidem*.

Sull'art. 189 Cpp v. M. Nobili, sub *art. 189 Cpp*, in *Commento Chiavario*, II, Torino 1990, 397 ss., nonché C. Conti, sub *art. 189 Cpp*, in *Codice di procedura penale*, a cura di A. Giarda e G. Spangher, Milano 2017, 1880 ss.

In ordine agli ambiti di “sovrapposizione” tra prova atipica e prova scientifica cfr. S. Marcolini, *Prove atipiche (dir. proc. pen.)*, in *ED, Annali X* 2017, 700.

³⁹ Oltre a un vaglio *ex ante*, di cui ci si occuperà nel prosieguo, è altresì necessario condurre una verifica *ex post*: anche laddove si addivenisse a constatare l'affidabilità del sistema automatico di riconoscimento facciale, occorrerebbe pur sempre escludere che l'«attendibilità della rilevazione sia stata» in qualche modo «compromessa tramite strumentazioni esterne»; così C. Fanuele, *La localizzazione satellitare nelle investigazioni penali*, Milano 2019, 30. Nello stesso senso, M. Chiavario, *Diritto processuale penale*⁷, Torino 2019, 497, il quale parla di una «dimostrazione positiva di idoneità, in concreto e *a priori*, “ad assicurare l'accertamento dei fatti”». In proposito v. altresì, B. Galgani, *Un test di elevata “scientificità” e un inedito banco di prova per la “civiltà” del processo*, in *Nuove tecnologie e processo penale*, a cura di M. Chiavario, Torino 2006, 43 la quale, in tema di prova genetica, afferma che «la “scientificità” del test del DNA non equivale affatto ad una sua affidabilità *iuris et de iure*. Al contrario, se è vero che, astrattamente, i principi scientifici sottesi alla prova genetica sono affidabili e validati, altrettanto certo è che nel singolo caso concreto l'accertamento può condurre a risultati fallaci».

Con riferimento alle tecnologie in esame, la questione assume particolare rilevanza quando si tratti di

– non senza aspre critiche⁴⁰ – in grado di recepire i parametri individuati nel celebre caso *Daubert* deciso dalla Corte Suprema degli Stati Uniti agli inizi degli anni Novanta⁴¹ e fatti propri, con alcuni “aggiustamenti”, dalla nostra giurisprudenza⁴².

In proposito è stato sottolineato che, nonostante il *SARI-Enterprise* sia in uso alle forze di polizia da diverso tempo, nessuna informazione circa il suo funzionamento è stata resa pubblica. Infatti, non si conoscono «i dati di ricerca con i quali opera il sistema, [...] i test svolti in merito all’effettiva capacità di riconoscimento dei volti analizzati, [...] i tassi di falsi positivi e di falsi negativi», nonché «come sia stata effettuata la validazione del sistema (dimensione del campione test, procedura impiegata per misurare l’accuratezza di predizione dei volti)»⁴³.

Di sicuro, però, non sono confortanti le indicazioni che pervengono dalle esperienze in corso in altri ordinamenti.

Nell’ambito di un sistema come quello nordamericano che si è sempre distinto tra le democrazie liberali per un atteggiamento di assoluta apertura verso l’utilizzo dei congegni di IA in funzione sia preventiva che di accertamento⁴⁴, non si può fare a meno

immagini reperite sul *web*. Nello specifico, dovrà escludersi che il processo di identificazione biometrica non sia stato condizionato da eventuali contromisure adottate dagli utenti proprio per “sviare” o “confondere” l’algoritmo. Risale infatti al 2017 la notizia dell’ideazione di un tessuto che, se indossato dal soggetto destinatario della rilevazione, confonde i sistemi inducendoli a rilevare numerosi falsi positivi (cfr. S. Cosimi, *Hyperface, contro il riconoscimento facciale: ecco il tessuto che manda in tilt i social*, in *la Repubblica*, 9.1.2017).

⁴⁰ Sull’idoneità dell’art. 189 Cpp a consentire l’ingresso delle prove scientifiche nuove o controverse nel processo penale v., O. Dominioni, *op. cit.*, 985 s.; G. Canzio, *Intelligenza artificiale e processo penale*, in *CP 2021*, 802; e, in termini critici, M. Caianiello, *L’ammissione della prova scientifica nel processo italiano*, in *Prova scientifica e processo penale*, a cura di G. Canzio e L. Lupária, Milano 2018, 205 ss.; P. Felicioni, *Prova scientifica, DigDPen*, I Agg., 2014, in *Leggi d’Italia*, § 4; G. Garofalo, *Le prove atipiche fra “apertura” e “limite” al potere giudiziale di conoscere*, in *Incontri ravvicinati’ con la prova penale*, a cura di L. Marafioti e G. Paolozzi, Torino 2014, 133 ss.; P. P. Rivello, *op.cit.*, 112 ss.; F. Caprioli, *La scienza “cattiva maestra”: le insidie della prova scientifica nel processo penale*, in *CP 2008*, 3529; G. Ubertis, *La prova scientifica e la nottola di Minerva*, in *Argomenti di procedura penale*, vol. II, Milano 2006, 204 ss.

⁴¹ Sentenza *Daubert v. Merrel Dow Pharmaceuticals Inc.*, 509 U.S. 579 (1993), in cui furono elaborati i seguenti criteri: «verifica sulla scientificità della teoria su cui si fonda la prova scientifica mediante verifica e falsificazione (*testability*)»; «individuazione del margine di errore (*rate of error*)»; «revisione critica della teoria o tecnica in esame da parte di esperti (*peer review*)»; «generale consenso della comunità scientifica di riferimento (*general acceptance*) che, tuttavia, assume un carattere complementare» (Così P. Felicioni, *op. cit.*, § 4)

⁴² Il riferimento è alle note sentenze Cass. S.U. 10.7.2002 Franzese, in *CP 2002*, 3643 e Cass. 17.9.2010 Cozzini, in *DPP 2011*, 1341.

⁴³ R. V. O. Valli, *op.cit.*, § 3, il quale aggiunge che «sia per l’assoluta novità del sistema sia soprattutto per la non conoscibilità degli elementi ora indicati, si capisce come non si sia formato un consenso della comunità scientifica sulla validità del metodo utilizzato».

⁴⁴ Con precipuo riguardo ai congegni di riconoscimento facciale, è sufficiente considerare che, dal 2019 ad oggi, la sola applicazione di riconoscimento facciale automatizzato di Clearview AI è stata acquistata da più di 600 agenzie di *law enforcement*; cfr. I. Neroni Rezende, *op. cit.*, 376.

Per una panoramica aggiornata v. H. J. Dixon, *Artificial Intelligence: Benefits and Unknown Risks*, 21 gennaio 2021, pubblicato sul sito dell’ABA (American Bar Association) e reperibile al seguente [link](#):

di menzionare la vicenda che ha interessato un cittadino statunitense afroamericano indagato per il furto di alcuni orologi di valore. In effetti, l'errore della "macchina"⁴⁵, ovvero del *software* di riconoscimento facciale in uso alla Polizia di Detroit, che ha rinvenuto una corrispondenza tra l'immagine ripresa dalle videocamere di sorveglianza e quella contenuta nella banca dati delle licenze di guida poi dimostratasi inesatta, è costato al sig. Robert Williams ben 30 ore di privazione della libertà personale. Così, lo scorso 13 aprile, la *Civil Rights Litigation Initiative* della *University of Michigan Law School* e l'organizzazione non governativa *American Civil Liberties Union* hanno promosso un'azione legale volta ad ottenere non solo il risarcimento del danno patito per l'ingiusta privazione della libertà personale, ma anche un provvedimento che impedisca l'impiego del sistema di riconoscimento facciale in questione, «*so long as it misidentifies individuals at materially different rates depending on race, ethnicity, or skin tone*»⁴⁶. In particolare, nell'atto introduttivo si legge che l'errata identificazione dell'autore del reato sarebbe frutto innanzitutto dell'utilizzo di una tecnologia che produrrebbe un tasso di falsi positivi notevolmente più alto nei confronti delle persone di colore⁴⁷. Ciò sarebbe essenzialmente dovuto alla circostanza che la maggior parte degli algoritmi sono costruiti sulla base di *datasets* che si compongono principalmente di volti di maschi bianchi adulti⁴⁸.

Analoghe indicazioni si ricavano da quanto occorso nel Regno Unito. Proprio la giurisprudenza britannica è stata chiamata per prima a fare i conti con gli interrogativi posti dalle *AFRTs* sotto il profilo delle garanzie. Segnatamente, la *High Court of Justice of England and Wales*⁴⁹ e, successivamente, in sede di impugnazione, la *Court of Appeal*

https://www.americanbar.org/groups/judicial/publications/judges_journal/2021/winter/artificial-intelligence-benefits-and-unknown-risks/.

⁴⁵ ... unitamente – occorre sottolinearlo – ad un approccio alquanto disinvolto, se non addirittura negligente, da parte del Dipartimento di Polizia di Detroit, tant'è che gli stessi vertici delle forze dell'ordine, seppur al fine di non vedersi privati di uno strumento dal loro punto di vista evidentemente indispensabile, hanno ammesso che l'arresto è stato frutto «non di una tecnologia difettosa», bensì «di un'attività di indagine scadente»: T. Ryan-Mosley, *The new lawsuit that shows facial recognition is officially a civil rights issue*, in *www.technologyreview.com*, 14.4.2021 (traduzione a cura nostra). V. altresì E. White, *Detroit says 'shoddy' work led to wrongful arrest tied to facial recognition technology*, in *Detroit Free Press*, 26.6.2020.

⁴⁶ *Williams v. City of Detroit et al.*, Case no.:2:2021cv10827 (https://www.aclumich.org/profiles/aclu_affiliates/libraries/pdf.js/web/viewer.html?file=https%3A%2F%2Fwww.aclumich.org%2Fsites%2Fdefault%2Ffiles%2Ffield_documents%2F001_complaint_1.pdf#page=1&zoom=auto,-12,798).

⁴⁷ Ciò, in evidente contrasto col § 37.2302(a) dell'*Elliot-Larsen Civil Rights Act* dello Stato del Michigan, «*which demands that no governmental entity deny an individual the full and equal enjoyment of its public services on the basis of race*» (*Williams v. City of Detroit et al.*, cit., § 10).

⁴⁸ *Williams v. City of Detroit et al.*, cit., § 41.

⁴⁹ *High Court of Justice, Queen's Bench Division, Divisional Court*, Case No: CO/4085/2018, (<https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf>), annotata da J. Della Torre, *Novità dal Regno Unito*, cit., 231 ss.

of England and Wales⁵⁰ si sono occupate dell'AFR Locate, ovvero uno strumento di riconoscimento facciale in tempo reale in dotazione alla South Wales Police nell'ambito di un progetto pilota, cui il sig. Edward Bridges lamentava di essere stato illegittimamente sottoposto in due occasioni mentre si trovava nella città di Cardiff, contestando la violazione di diverse disposizioni, comprese quelle contenute nell'Equality Act del 2010, giusta la tendenza pure di questo congegno a produrre un tasso di falsi positivi notevolmente più alto per coloro che appartengono a minoranze etniche, nonché in relazione alle persone di sesso femminile.

In proposito, è interessante notare come le conclusioni del giudice d'appello, il quale, a differenza di quello di primo grado, ha accolto la doglianza fondata sulla disparità di trattamento realizzata dal software, abbiano condizionato anche il giudizio del nostro Garante della privacy: accertata – come visto⁵¹ – l'inesistenza di una base giuridica idonea, l'Autorità domestica per la protezione dei dati personali si lascia andare ad una sorta di monito per l'eventualità in cui tale base giuridica venisse effettivamente adottata. Nello specifico, si afferma che la bozza di valutazione di impatto del SARI-Real Time – al cui esame il Garante non ha proceduto, trattandosi di un profilo assorbito dal rilevato difetto di legalità del trattamento – dovrà assicurare l'«accuratezza» e la «capacità di discriminare» del software; caratteristiche, queste, che devono essere «verificate per accertare che anche nei confronti di appartenenti a minoranze etniche il sistema sia pienamente adeguato»⁵².

Inoltre, è opportuno sottolineare un passaggio della pronuncia emessa dalla Court of Appeal, da cui emergere come la questione dell'accessibilità delle informazioni relative ai software, che – va da sé – costituisce il presupposto per qualsiasi tentativo difensivo di mettere in discussione l'affidabilità del sistema utilizzato⁵³, rappresenti uno dei profili più controversi e di difficile risoluzione in tema di IA⁵⁴. Dall'analisi delle dichiarazioni rese dai due expert witness intervenuti risulta chiaramente che è questo il terreno su cui le esigenze di trasparenza si scontrano con le istanze di tutela «della proprietà intellettuale e del trade secret»⁵⁵. Da un lato, è stato sottolineato che, senza

⁵⁰ Court of Appeal (Civil Division), Case No: C1/2019/2670 (<https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf>); cfr. J. Purshouse e L. Cambell, Automated facial recognition and policing: a Bridge too far?, in Legal Studies, 27.8.2021.

⁵¹ V. supra, § 2.

⁵² Garante per la protezione dei dati personali, Parere sul sistema Sari Real Time, cit., 4.

⁵³ M. Torre, Nuove tecnologie e trattamento dei dati personali, cit., 1053. Nella letteratura statunitense v. G. M. Haddad, Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom, in Vanderbilt Journal of Entertainment & Technology Law 2021, vol. 23, n. 4, 908 ss.; R. D. Goldberg, You can see my face, why can't I? Facial recognition and Brady, in HRLR Online, 12.4.2021, 263 ss.

⁵⁴ Sulla tematica cfr. S. Quattrocolo, Artificial Intelligence, Computational Modelling and Criminal Proceedings, cit., 93 ss.; Ead., An introduction to AI and criminal justice in Europe, in Rev. Bras. de Direito Processual Penal 2019, vol. 5, n. 3, 1525 ss.

⁵⁵ Ead., Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente

poter conoscere i *datasets* utilizzati per sviluppare l'AFR *Locate*, è difficile, se non impossibile, verificare se esso sia effettivamente imparziale. Dall'altro, occorre tenere in considerazione che «*the precise makeup, scale and sources of the training data used are commercially sensitive*» e non possono dunque essere diffusi⁵⁶.

Tra le soluzioni proposte spicca quella della Commissione europea per l'efficienza della giustizia (d'ora in poi: "CEPEJ") nell'ormai celebre Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi ripresa anche dallo stesso giudice britannico. Posto l'obiettivo di raggiungere un equilibrio «tra la proprietà intellettuale di alcune metodologie di trattamento e l'esigenza di trasparenza (accesso al processo creativo), imparzialità (assenza di pregiudizi), equità e integrità intellettuale (privilegiare gli interessi della giustizia)»; e preso atto altresì dell'impraticabilità della via della totale trasparenza tecnica per le ragioni legate alla tutela del segreto industriale, si suggerisce di incaricare «[a]utorità o esperti indipendenti» del compito di «certificare e verificare le metodologie di trattamento o di fornire consulenza anticipatamente». Una volta concessa, tale certificazione dovrebbe essere poi «riesaminata regolarmente»⁵⁷.

La medesima impostazione è stata ribadita, sempre nell'ambito del Consiglio d'Europa, dal Comitato consultivo della c.d. "Convenzione 108 sulla protezione dei dati", il quale, il 28 gennaio 2021, ha emanato le proprie *Guidelines on Facial Recognition*: nella parte I, indirizzata espressamente a «*legislators and decision-makers*», si afferma infatti che l'istituzione di meccanismi di certificazione indipendenti e qualificati è un elemento indispensabile⁵⁸.

Se questo sia sufficiente a soddisfare le istanze di garanzia proprie del nostro processo penale è tutto da dimostrare⁵⁹, anche tenuto conto dell'atteggiamento assunto dalla giurisprudenza amministrativa domestica, la quale, con riferimento a questioni che evidentemente non coinvolgevano la libertà personale, si è orientata nel

discussione tra scienze penali e informatiche, in www.la legislazione penale.eu, 18.12.2018, 7.

⁵⁶ Court of Appeal (Civil Division), Case No: C1/2019/2670, § 196.

⁵⁷ CEPEJ, Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi adottata dalla CEPEJ nel corso della sua 31^a Riunione plenaria (Strasburgo, 3-4 dicembre 2018), 3.12.2018, 11 (<https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348>).

Per il commento della previsione in tema di trasparenza si rinvia all'analisi condotta da S. Quattrocchio, *Intelligenza artificiale e giustizia*, cit., 7 ss. Circa le differenti vie percorribili v. G. Contissa, G. Lasagni e G. Sartor, *op. cit.*, 625 ss.

⁵⁸ Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Convention 108, *Guidelines on Facial Recognition*, 8 (<https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3>).

⁵⁹ Sull'importanza di garantire, con riferimento alle prove scientifiche, «un meccanismo di *discovery* semmai potenziato (e non certo indebolito) rispetto a quello che si esplica sulle prove per così dire "tradizionali"», nonché «un confronto ampio tra gli esperti» v. B. Galgani, *Un test di elevata "scientificità"*, cit., 49.

senso di esigere la totale trasparenza tecnica⁶⁰.

Quand'anche fosse accertabile ed accertato «che l'attività automatizzata di ricognizione superi per affidabilità di risultati, quella tradizionalmente riservata alla capacità mnemonica dell'uomo»⁶¹, occorrerebbe comunque considerare il secondo limite di ammissibilità fissato dall'art. 189 Cpp concernente il rispetto della libertà morale.

A questo riguardo, si è sostenuto che, nella modalità *Enterprise*, il SARI non presenta particolari criticità: è infatti da escludersi qualsivoglia «alterazione della libertà morale» dal momento che i «dati biometrici eventualmente utilizzati per essere confrontati con quelli della persona indagata o sospettata sono acquisiti sulla base di una normativa *ad hoc*, che ne garantisce l'utilizzo trasparente e per fini legittimi»⁶².

Viceversa, per quanto concerne la versione *Real Time*, è stato rilevato che, quando la tecnologia *de qua* è impiegata come mezzo di ricerca della prova, se, per un verso, nessun individuo è in grado di sapere se e dove la propria impronta facciale verrà captata⁶³, per l'altro, la sola conoscenza del fatto che il sistema potrebbe essere utilizzato, unitamente all'assenza di una previsione che stabilisce casi e modi di impiego, metterebbe «a rischio la stessa libertà morale della persona fonte di prova, intesa come facoltà di autodeterminarsi rispetto agli stimoli»⁶⁴.

Sul punto, non si può fare a meno di richiamare l'elaborazione dottrinale nordamericana in tema di c.d. "*right to public anonymity*". La questione è di estrema attualità, in quanto è sempre più diffusa la convinzione che l'utilizzo delle *AFRTs* abbia contribuito a esacerbare i conflitti⁶⁵, non solo per la propensione di questi congegni a realizzare – come visto – inammissibili disparità di trattamento: l'impiego degli strumenti di riconoscimento facciale *real time* in occasione, ad esempio, delle manifestazioni che sono seguite all'omicidio di George Floyd ha finito per offrire un'argomentazione in più a quanti sostengono da tempo che le tecnologie di videosorveglianza in generale e, data la loro maggiore intrusività, quelle di identificazione biometrica basate sui tratti caratteristici del volto in particolare

⁶⁰ Cfr. Cons. Stato Sez. VI 4.2.2020 n. 881, in *RDPr* 2021, 710 ss. con nota di J. Della Torre, *Le decisioni algoritmiche all'esame del Consiglio di Stato*, al quale si rinvia anche per alcuni spunti proprio in tema di *AFRTs*. Sul punto v. inoltre G. Contissa, G. Lasagni e G. Sartor, *op. cit.*, 626.

⁶¹ In questo senso R. Lopez, *La rappresentazione facciale tramite software*, cit., 313.

⁶² M. Torre, *Nuove tecnologie e trattamento dei dati personali*, cit., 1054.

⁶³ Cfr. J. Della Torre, *Novità dal Regno Unito*, cit., 242, il quale sottolinea che «in Italia non vi è come nel Regno Unito una mera attività di sperimentazione del riconoscimento facciale *live* in luoghi ben circoscritti (di cui è dato avviso man mano al pubblico in vari modi). Tutt'al contrario: la tecnologia in questione è, invece, potenzialmente in dotazione delle autorità di *law enforcement* sull'intero territorio nazionale, senza che la collettività sia in alcun modo informata via web o in altro modo dell'attività captativa»

⁶⁴ Ancora M. Torre, *Nuove tecnologie e trattamento dei dati personali*, cit., 1054. Nello stesso senso E. Currao, *op. cit.*, 11.

⁶⁵ New York City Bar Association's Criminal Courts Committee, "*Power, Pervasiveness and Potential: The Brave New World of Facial Recognition Through a Criminal Law Lens (and Beyond)*", cit., 4.

possono determinare nei consociati un atteggiamento di auto-censura, venendo ad impattare, anzitutto, sulla libertà di manifestazione del pensiero e di associazione garantita dal I Emendamento⁶⁶.

Detto altrimenti, il timore dei partecipanti di essere identificati durante una manifestazione pubblica può indurre un «effetto inibitore» (“*chilling-effect*”) «notoriamente scatenato nell’animo dall’idea di essere sotto osservazione»⁶⁷. E lo stesso può affermarsi in relazione alla libertà di *movement and repose* di cui al XIV Emendamento: «la frequentazione di un luogo, infatti, quasi mai è neutra, ma rileva abitudini, gusti, affiliazioni a gruppi, insomma tutta una serie di informazioni che contribuiscono a costruire l’identità della persona»⁶⁸.

L’«oggetto ultimo di tutela» del diritto all’anonimato verrebbe a coincidere, in definitiva, proprio con la «libertà di autodeterminazione dell’individuo, che è la radice di ogni libertà e la precondizione essenziale per la realizzazione di una società aperta e democratica»⁶⁹.

Tuttavia, si potrebbe comunque avere la sensazione che, superata la questione – allo stato, come visto, ancora irrisolta – dell’idoneità ad assicurare la ricostruzione giudiziale dei fatti, non residui alcun ostacolo all’impiego diffuso dei sistemi di riconoscimento facciale automatizzato⁷⁰: è noto, infatti, l’atteggiamento di *laissez faire*

⁶⁶ C. Slobogin, *Public Privacy: Camera Surveillance of Public Spaces and The Right to Anonymity*, in *Mississippi Law Journal* 2002, vol. 72, 257.

⁶⁷ ... «effetto icasticamente raffigurato dal *Panopticon* benthamiano», «le cui implicazioni sono state rielaborate in chiave moderna da Foucault»: così, in relazione, più in generale, ai sistemi di videosorveglianza di spazi pubblici o aperti in pubblico, G. Di Paolo, “*Tecnologie del controllo*” e prova penale. *L’esperienza statunitense e spunti per la comparazione*, Milano 2008, 147. V. altresì F. Paolucci, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *MediaLaws-Riv. dir. media* 2021, f. 1, 214.

⁶⁸ G. Di Paolo, *op. cit.*, 151, nota n. 181.

⁶⁹ Ancora, Ead., *ivi*, 153, la quale definisce il diritto all’anonimato come il «diritto di restare una parte anonima e indistinta della folla, almeno fino a quando non vengano realizzate condotte tali da meritare l’attenzione dell’autorità» (153). Per l’individuazione del fondamento costituzionale del diritto in questione, oltre al citato lavoro di C. Slobogin, *op. cit.*, 237 ss., v., più di recente, J. Turley, *Anonymity, Obscurity, and Technology: Reconsidering Privacy in the Age of Biometrics*, in *Boston University Law Review* 2020, vol. 100, 2232 ss.

⁷⁰ Anche per quanto riguarda la condizione di natura procedurale prevista dall’ultimo inciso dell’art. 189 Cpp, che assume particolare rilevanza allorquando le *AFRTs* siano impiegate come mezzi di ricerca della prova, le *chances* difensive risultano alquanto limitate. In proposito meritano di essere richiamati i rilievi di R. Lopez, *La rappresentazione facciale tramite software*, *cit.*, 312 s., la quale sostiene che «la nomina di un consulente tecnico per confutare la certificazione dell’*output* da parte della polizia scientifica può rivelarsi inefficace; in particolare, quando la corrispondenza tra i volti comparati sia espressa per grado di similarità, non risultando *ictu oculi* attendibile o inattendibile, il relativo risultato, frutto di una tecnologia automatizzata, rischia di “ammaliare” con le sue suggestioni l’operatore, probabilmente restio, magari anche incoscientemente, ad abbandonare l’ipotesi del *software*.

Il limite del S.A.R.I., [...] così come di ogni altro programma di riconoscimento facciale da impiegare in ambito investigativo, sembra risiedere proprio in una ripetibilità solo apparente dell’atto identificativo. Infatti, per quanto l’operazione automatizzata risulti sempre replicabile, potendo la medesima immagine fotografica essere processata dal *software* un numero indefinito di volte senza pregiudizio per la sua integrità, la ripetizione del

assunto dalla giurisprudenza di legittimità e condiviso da una parte della dottrina italiana in relazione ad uno strumento investigativo come la localizzazione satellitare, che, sotto questo profilo, presenta caratteristiche omologhe a quelle delle AFRTs⁷¹ in quanto anch'esso idoneo a incidere «su libertà fondamentali destinate, per loro natura, a venir estrinsecate pubblicamente»⁷².

3.2. Nondimeno, facendo un passo indietro, occorre verificare se il prospettato ampliamento del catalogo di attività riconducibili all'art. 189 Cpp possa o meno risolversi nell'elusione delle garanzie previste dalla Costituzione e – per ciò che più rileva in questa sede – dalle altre Carte dei diritti poste a presidio delle prerogative fondamentali della persona⁷³. Infatti, «se così fosse, l'uso probatorio dei risultati ottenuti dovrebbe ritenersi comunque precluso; anche qualora l'ammissione processuale dei medesimi dati» non confliggesse con le condizioni dettate per la prova atipica⁷⁴.

Da questo punto di vista, si è convinti che a rilevare sia il proteiforme diritto alla privacy riconosciuto e tutelato dagli artt. 8 Cedu e 7 e 8 CDFUE⁷⁵; e, ciò, nonostante sia ancora diffusa l'idea che la natura pubblica del luogo in cui avviene la rilevazione determinerebbe un'implicita rinuncia alla riservatezza⁷⁶.

Per la verità, da un punto di vista generale, si può legittimamente dubitare che

riconoscimento resta, comunque, di dominio esclusivo della “macchina” e dell'operatore che la interroga: l'attività che è off limits per la difesa, preclude ogni tentativo di falsificazione del relativo risultato in contraddittorio. Unico oggetto di confronto dialettico con l'accusa riguarderà soltanto la fonte mediata, ossia la relazione della polizia scientifica illustrativa della verifica di affidabilità dell'output, attraverso gli *standard* identificativi classici, fondati su parametri discriminatori sia metrici [...], che fisionomici».

⁷¹ Ci si riferisce all'impostazione secondo cui il pedinamento GPS non sarebbe in grado di limitare in alcun modo la libertà morale dell'indagato, dal momento che questi è ignaro dell'attività in corso. Su questo aspetto v. diffusamente C. Fanuele, *op. cit.*, 30, cui si rinvia anche per la dottrina citata *sub* nota n. 39. In giurisprudenza, cfr., *ex multis*, Cass. 10.3.2010 n. 9667, in *DPP* 2010, 1464; Cass. 11.12.2007 n. 15396, in *CP* 2009, 2534.

⁷² C. Fanuele, *op. cit.*, 31.

⁷³ Cfr., *ex multis*, O. Mazza, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *DPenCont* 2013, f. 3, 11 ss.; C. Conti, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova 2007, 275.

⁷⁴ C. Fanuele, *op. cit.*, 34. Nello stesso senso, T. Bene, *Il pedinamento elettronico: truismi e problemi*, in *Le Pre-investigazioni*, cit., 355; L. Agostino, *Giurisprudenza creativa e pedinamento satellitare*, in “*Diritto dei giudici*” e *sistema delle fonti* a cura di E. Ceccherini e M. Miraglia, Genova, in corso di pubblicazione.

⁷⁵ Sullo «sdoppiamento di binario» che caratterizza la Carta di Nizza, in cui al diritto alla protezione dei dati personali viene riservata un'autonoma sede normativa (art. 8) rispetto a quello alla riservatezza (art. 7), v. O. Pollicino, *sub art. 8 CDFUE, Carta dei diritti fondamentali dell'Unione europea*, a cura di R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo e O. Razzolini, Milano 2017, 135 ss. In ordine alla difficoltà di individuare un fondamento del diritto all'autodeterminazione informativa nella nostra Carta costituzionale cfr. S. Carnevale, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale*, a cura di D. Negri, Roma 2007, 9 ss.

⁷⁶ V., sempre in tema di pedinamento satellitare, la giurisprudenza citata *supra*, § 3.1, nota n. 69.

il sol fatto di esporsi agli sguardi del pubblico faccia venir meno qualsiasi ragionevole aspettativa di riservatezza⁷⁷.

Da tempo, la Corte di Strasburgo ha adottato un'interpretazione della nozione di "vita privata" che va oltre gli «angusti limiti propri delle garanzie offerte dall'ordinamento interno»⁷⁸, attribuendo rilevanza anche al diritto di ciascuna persona di avvicinare gli altri per instaurare e sviluppare rapporti con loro e con il mondo esterno, ovvero al diritto a una "vita sociale privata"⁷⁹.

Inoltre, con particolare riguardo alle AFRTs ci si accorge che il novero di informazioni ricavabili tramite l'impiego di tali congegni non coincide ed è notevolmente più ampio di quello che rivela la semplice esposizione di un soggetto in pubblico.

In proposito, meritano di essere richiamate le riflessioni svolte dalla letteratura statunitense per scongiurare l'assoggettamento delle tecnologie in esame all'orientamento giurisprudenziale tradizionale che esclude dalla nozione costituzionale di "search" le forme di sorveglianza implicanti l'osservazione di attività pubbliche e non ritiene pertanto necessario, a questi fini, l'emissione di uno *warrant* fondato su una *probable cause*⁸⁰. Attraverso un paragone con le tecniche di sorveglianza della circolazione stradale, si è infatti efficacemente affermato che «[p]eople do not walk around with signs announcing our identifying information. Indeed, the privacy interest implicated by the identification of people walking on the street is far greater than the interest implicated by license plate look-ups, because people do not, and are not required to, walk around with signs displaying identification information that they registered to the government»⁸¹.

Spostando l'attenzione dal contesto d'oltreoceano a quello d'oltremarica, è

⁷⁷ Cfr. G. Di Paolo, *op. cit.*, 142.

⁷⁸ F. Nicolichia, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Milano 2020, 52.

⁷⁹ Tra le numerose decisioni in cui la Corte ha ritenuto sussistente, anche in un contesto pubblico, una zona di interazione della persona con gli altri che deve essere compresa nella nozione di "vita privata", v. C. eur. GC, 5.9.2017, *Bărbulescu c. Romania*, § 71; C. eur. GC, 7.2.2012, *Von Hannover c. Germania*, § 95; C. eur., 2.9.2010, *Uzun c. Germania*, § 43; C. eur., 28.1.2003, *Peck c. Regno Unito*, § 62.

⁸⁰ Il riferimento corre, in particolare, alle note pronunce *United States v. Jones*, 565 U.S. 400, 412; *United States v. Knotts*, 460 U.S. 276, 281-82 (1983) e *Katz v. United States*, 389 U.S. 347, 351 (1967). Per una ricognizione delle decisioni più rilevanti cfr. H. Ruhrmann, *Facing the Future: Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement. Case Studies from the United Kingdom and the United States*, 53 ss. reperibile al seguente link: https://citrispolicylab.org/wp-content/uploads/2019/09/Facing-the-Future_Ruhrmann_CITRIS-Policy-Lab.pdf.

Sulla nozione di perquisizione, con particolare riguardo ai nuovi mezzi tecnologici, v. M. Miraglia, *Garanzie costituzionali nel processo penale statunitense: tendenze e riflessioni*, Torino 2008, 12 ss.

⁸¹ M. Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, in *Connecticut Law Review* 2017, vol. 49, n. 5, 1607.

inevitabile intrattenersi sul già citato caso *Bridges*, dal momento che le censure del ricorrente avevano riguardato anche la violazione dell'art. 8 Cedu⁸².

Ebbene, tanto la *High Court*, quanto la *Court of Appeal*, non hanno mostrato incertezze nel riconoscere che l'utilizzo del sistema in discussione aveva certamente realizzato un'ingerenza nel diritto alla riservatezza del ricorrente.

Il punto di partenza è rappresentato dalla pronuncia della C. eur. *S. and Marper c. Regno Unito*, con cui il Giudice di Strasburgo ha affermato che sia il DNA sia le impronte digitali contengono informazioni uniche, permettendo l'identificazione di un soggetto in una vasta gamma di circostanze. Pertanto, si deve ritenere che le relative metodiche di identificazione sono senz'altro in grado di incidere negativamente sul diritto al rispetto della vita privata dell'interessato, così come, nella stessa prospettiva, la conservazione di siffatti dati biometrici senza il consenso di quest'ultimo non può essere considerata neutra o insignificante. Gli stessi rilievi valgono per i sistemi automatici di riconoscimento facciale, in quanto consentono l'estrazione «*of unique information and identifiers about an individual allowing his or her identification with precision in a wide range of circumstances. Taken alone or together with other recorded metadata, AFR-derived biometric data is an important source of personal information*». Alla stregua delle impronte digitali e del DNA, le informazioni trattate dalle AFRs hanno un «*“intrinsically private” character*» che non viene certamente meno in ragione del fatto che «*the biometric data is derived from a person's facial features that are “manifest in public”*»: ciò che importa è che «*[t]he facial biometric identifiers too, are precise and unique*»⁸³.

Un simile approccio – prosegue la *High Court*⁸⁴ – si riscontra anche nel *case-law* della Corte di Giustizia dell'Unione europea, la quale, nel caso *Schwarz* concernente un individuo rifiutatosi di fornire le proprie impronte digitali nella procedura prevista per il rilascio del passaporto, ha posto in relazione l'acquisizione di *fingerprints and facial images* con il diritto al «rispetto della vita privata con riguardo al trattamento dei dati personali», che concerne «ogni informazione relativa ad una persona fisica identificata o identificabile»⁸⁵.

Assunte a referenti della materia le previsioni convenzionali e del Trattato di

⁸² *High Court of Justice, Queen's Bench Division, Divisional Court*, Case No: CO/4085/2018, § 57.

⁸³ Riportandosi alla pronuncia poc'anzi menzionata, la *High Court* si è premurata altresì di precisare come, la circostanza che, nell'ipotesi in cui non abbia luogo il *matching*, le informazioni captate dall'AFR *Locate* sono trattenute per il solo periodo di tempo necessario alla verifica dell'esistenza di una corrispondenza e successivamente cancellate, non faccia venir meno l'intrusione nella sfera privata: «*[t]he application of Article 8 is not dependent on the long-term retention of biometric data. It is sufficient if biometric data is captured, stored and processed, even momentarily*». Detto altrimenti, «*[t]he mere storing of biometric data is enough to trigger article 8 and the subsequent use (or discarding) of the stored information has no bearing*» (§ 59).

⁸⁴ *High Court of Justice, Queen's Bench Division, Divisional Court*, Case No: CO/4085/2018, § 43.

⁸⁵ C.G.U.E, 17.10.2013, *Schwarz*, Causa C-291/12, § 48.

Nizza a salvaguardia del *right to privacy*, occorre concentrarsi su quanto richiesto, rispettivamente, dagli artt. 8 § 2 Cedu e 52 CDFUE.

In questo senso, si può legittimamente dubitare che l'art. 189 Cpp soddisfi i principi di legalità e proporzionalità cui deve sottostare ogni ingerenza nel diritto in questione.

Dal primo punto di vista, le criticità non riguardano la *natura* della fonte normativa, posto che la C.eur. attribuisce al termine «legge» un significato autonomo e differente da quello tipico dei Paesi di *civil law*, capace di ricomprendervi, ad esempio, anche la giurisprudenza⁸⁶. A rilevare è, piuttosto, la *qualità* della base giuridica, che, al fine di assicurare la certezza del diritto, deve presentare i caratteri della accessibilità e della prevedibilità⁸⁷.

Per dirla con le parole utilizzate dalla *Court of Appeal*, ciò non significa che tale fonte non possa attribuire all'autorità un margine discrezionalità, quanto piuttosto che «*the “law” must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity*», specificando, fra l'altro, chi può essere inserito nella *watchlist* («*“who question”*») e quali siano i criteri sulla cui base individuare i luoghi da sottoporre a osservazione («*“where question”*»). Il tutto, «*to give the individual adequate protection against arbitrary interference*»⁸⁸.

⁸⁶ Cfr. L. Tomasi, sub art. 8 Cedu, in *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali* a cura di S. Bartole, P. De Sena e V. Zagrebelsky, *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Milano 2012, 304 ss. e, in termini critici, F. Nicolichia, *op cit.*, 54, il quale afferma che «[d]al punto di vista teorico, non pare in verità condivisibile estendere la nozione di legge ex art. 8 § 2 Conv. e.d.u. sino a ricomprendervi anche semplici statuizioni pretorie, quantomeno nel contesto di sistemi continentali in cui il rango di fonte del diritto capace di modulare l'estensione delle prerogative fondamentali è istituzionalmente riservato alla norma parlamentare. Ritenere soddisfatta la riserva di legge pur in presenza di mere pronunce giurisprudenziali pare infatti contraddire le esigenze di prevedibilità poste dalla stessa Corte a fondamento della garanzia. In altri termini, in un assetto ordinamentale retto da un principio di legalità formale sembra lecito attendersi che i consociati identifichino esclusivamente nella legge *stricto sensu* intesa l'unica fonte capace di introdurre limitazioni delle proprie libertà.

Allo stesso modo, in sistemi non vincolati al rispetto del principio dello *stare decisis* non potrebbe essere neppure astrattamente attribuita a mere affermazioni giurisprudenziali – per quanto autorevoli – una stabilità interpretativa tale da fondare l'esistenza di una ragionevole prevedibilità dell'ingerenza».

Quanto al significato da attribuire all'espressione «previste dalla legge» di cui all'art. 52 CDFUE, si ritiene che «essa vada intesa, con riferimento agli ordinamenti nazionali, secondo le regole nell'ambito di questi comunemente adottate per interpretare siffatte riserve a livello di protezione dei diritti fondamentali» (così R. Cisotta, *Brevi note sulla giurisprudenza sull'art. 52, par. 1 della Carta dei diritti fondamentali dell'Ue in materia di limitazioni ai diritti fondamentali ...con uno sguardo in avanti*, in *Osservatorio sulle fonti* 2021, f. 1, 29; conf. F. Ferraro, sub art. 52 CDFUE, in *Carta dei diritti fondamentali dell'Unione europea*, cit., 1064.

⁸⁷ Per la rassegna giurisprudenziale aggiornata, anche sotto questo profilo, v. il documento a cura della stessa C. eur. “*Guide on Article 8 of the European Convention on Human Rights*”, 31.12.2020, spec. 10 ss. (https://www.echr.coe.int/documents/guide_art_8_eng.pdf).

⁸⁸ *Court of Appeal (Civil Division)*, Case No: C1/2019/2670, § 91 s.

Sull'estrema genericità dell'art. 189 Cpp non vi sono dubbi: «dopo aver stabilito il limite della libertà morale e quello idoneità all'accertamento dei fatti», tale disposizione «lascia all'autorità procedente totale libertà nel determinare le modalità con le quali la prova atipica deve essere acquisita, salva la necessità del contraddittorio con le parti, preventivo, quando possibile, ovvero successivo in relazione agli atti a sorpresa»⁸⁹.

Detto altrimenti, lo «scarno telaio dell'art. 189 c.p.p. è ben lontano dal soddisfare» l'aspettativa del singolo di «mantenere il controllo» sugli «ambiti di sviluppo della [propria] vita privata», conoscendone in anticipo il «regime di comprimibilità», «poiché fissa soltanto i limiti esterni della idoneità all'accertamento dei fatti e del divieto di compromettere la libertà morale della persona, lasciando scoperti aspetti normativi essenziali del potere probatorio»⁹⁰.

Quanto al secondo profilo, premesso che le garanzie concernenti «*the quality of the laws allowing for data collection*» «*are closely related to the question of whether the interference [i]s "necessary in a democratic society"*»⁹¹, emerge che l'art. 189 Cpp può al più risultare idoneo a circoscrivere il novero delle limitazioni a quelle «“utili” od “opportune”», mentre il *case-law* convenzionale ha escluso che si possa fare riferimento a concetti dotati di un tale margine di flessibilità⁹².

3.3. I rilievi appena svolti inducono ad accogliere con una certa soddisfazione la proposta di regolamento COM(2021) 206 *final* avanzata dalla Commissione europea nella scorsa primavera «che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione»⁹³ (d'ora in poi “proposta”) nelle cui trame si scorge una notevole sensibilità verso le possibili ricadute negative delle tecniche di riconoscimento facciale automatizzato.

Già solo la collocazione “topografica” delle disposizioni rilevanti in materia appare indicativa dell'approccio seguito: a venire in considerazione è infatti il Titolo II dedicato alle «[p]ratiche di intelligenza artificiale vietate».

Nello specifico, all'art. 5 § 1 lett. *d* della proposta si afferma, in prima battuta, il generale divieto di impiego per finalità di *law enforcement* dei sistemi di identificazione biometrica in tempo reale in luoghi accessibili al pubblico.

⁸⁹ Così C. Conti, *Accertamento del fatto e inutilizzabilità*, cit., 164.

⁹⁰ D. Negri, *op. cit.*, 26; O. Mazza, *op. cit.*, 12.

⁹¹ K. de Vries, *Right to respect for private and family life*, in *Theory and Practice of the European Convention on Human Rights*⁵, a cura di P. Van Dijk, F. Van Hoof, A. Van Rijn e L. Zwaak, Cambridge-Antwerp-Portland 2018, 674.

⁹² C. eur., 22.10.1981, *Dudgeon c. the Regno Unito*, §§ 51-53; cfr. C. Fanuele, *op. cit.*, 40, la quale ritiene che le limitazioni debbano essere «indispensabili».

⁹³ Per un primo commento v. F. C. La Vattiatà, *Brevi note “a caldo” sulla recente Proposta di Regolamento UE in tema di intelligenza artificiale*, in www.dirittopenaleuomo.org, 30.6.2021,

Le eventuali deroghe – ammesse a patto che i *software* superino lo scrutinio preventivo di conformità da parte di un ente certificatore terzo – sono circoscritte *ab origine* alle ipotesi contemplate dalla stessa disposizione in cui sia «strettamente necessario»: «individuare specifiche vittime di reato» (i); prevenire «un'imminente minaccia alla vita o all'incolumità fisica degli individui o [...] un attacco terroristico» (ii); o, infine, «individua[re]», «localizza[re]» o esercitare «l'azione penale» nei confronti dell'«autore» o di «colui che si sospetta sia tale» di uno dei reati riconducibili alle 32 categorie di fattispecie di cui alla decisione quadro 2002/584/CE istitutiva del mandato d'arresto europeo, e a patto che, sulla base della disciplina nazionale, tali reati siano «punibil[i] nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni» (iii)⁹⁴.

Nel successivo § 2, si aggiunge che l'utilizzo dei sistemi *de quibus* dovrà inoltre essere calibrato sulla «natura della situazione» nonché sulle «conseguenze» che possono derivarne «per i diritti e le libertà di tutte le persone interessate», con particolare riguardo, nel primo caso, alla «gravità», alla «probabilità» ed all'«entità del danno causato dal mancato uso del sistema» (a) e, nella seconda ipotesi, alla «gravità», alla «probabilità» ed all'«entità» delle suddette conseguenze (b).

Ancora, viene operato un riferimento esplicito alla necessità di stabilire limitazioni «temporali» e «geografiche», oltreché «personali», che siano «necessarie e proporzionate in relazione all'uso».

L'intento è evidentemente quello di “blindare” la materia, con un primo vaglio di proporzionalità operato in astratto a livello eurounitario, vaglio che spetterà poi ai singoli ordinamenti nazionali declinare con «regole dettagliate che limitino» ulteriormente «l'esercizio di un potere tanto invasivo e impattante su beni giuridici supremi»⁹⁵ nell'ipotesi in cui decidano di ammettere l'utilizzo di *software* di identificazione biometrica in tempo reale in luoghi accessibili al pubblico (§ 4).

Ma vi è di più: alle condizioni appena esaminate, la proposta affianca infatti un altro requisito che suona come una conferma della definitiva presa di coscienza del potenziale afflittivo delle *AFRTs*. Invero, ogni singolo utilizzo delle tecnologie in questione deve essere preceduto dal rilascio di un'apposita autorizzazione da parte di un'autorità giudiziaria o di un'autorità amministrativa indipendente dello Stato membro, emessa a seguito di richiesta motivata e nel rispetto delle suddette regole nazionali dettagliate. Segnatamente, occorre accertare, sulla base di «prove oggettive» o «indicazioni chiare», la necessità e la proporzionalità della misura rispetto ad almeno una delle finalità ammesse. L'unica ipotesi in cui è consentito prescindere dall'autorizzazione riguarda eventuali situazioni di urgenza, salvo comunque l'obbligo

⁹⁴ V., per tutti, M. Chiavario, *Manuale dell'estradizione e del mandato d'arresto europeo*, Torino 2013, 214 ss.

⁹⁵ F. C. La Vattiana, *op. cit.*, 10.

di ottenere la convalida (§ 3).

In conclusione, appare chiaro come la Commissione abbia concepito il riconoscimento facciale automatizzato svolto in tempo reale alla stregua di un'«intrusion[e] significativ[a] nella sfera privata e dei dati personali» tutelati dagli artt. 7 e 8 CDFUE, che, in quanto tale, stando all'orientamento consolidato della Corte di Giustizia, deve non solo essere «regolat[a] da norme di legge, di modo che l'acquisizione per fini di prevenzione o di accertamento processuale sia circoscritta al ricorrere di reati sufficientemente gravi» e «contenuta nella misura strettamente necessaria per conseguire il fine perseguito», ma anche «accompagnata dal controllo preventivo di un giudice o di una entità amministrativa indipendente»⁹⁶.

Ecco che, laddove la proposta fosse effettivamente approvata ed il nostro legislatore – come prevedibile – decidesse di non rinunciare completamente all'impiego delle AFRTs, la normativa interna di adeguamento non potrà prescindere dal tenere in debita considerazione anche il *case-law* del giudice eurounitario rilevante in materia.

Così, ad esempio, nell'individuazione dell'autorità competente a concedere l'autorizzazione, non potranno trascurarsi le ragioni che hanno portato alla recente modifica dell'art. 132 del codice della *privacy* in tema acquisizione dei dati del traffico e di ubicazione e, in particolare, ad escludere che possa bastare un provvedimento del pubblico ministero, essendo viceversa necessario l'intervento preventivo del giudice⁹⁷.

⁹⁶ T. Rafaraci, *Verso una law of evidence dei dati*, in *DPP* 2021, 853, il quale afferma efficacemente che, con riferimento al nostro ordinamento, «i richiamati standard di tutela accreditati dalla giurisprudenza della Corte europea potrebbero utilmente presiedere» «all'istituzione di adeguati presidi nei non pochi casi di tecniche o strumenti di indagine – per lo più qualificati come atipici – che, nonostante la loro invasività, vengono disinvoltamente praticati a prescindere da qualsivoglia garanzia».

⁹⁷ Il riferimento corre in particolare al d.l. 30.10.2021 n. 132 (cfr. A. Malacarne, *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132*, www.sistemapenale.it, 8.10.2021), nel cui preambolo si legge che la finalità del provvedimento è quella di adeguare il nostro ordinamento alla decisione C.G.U.E, 2.3.2021, *H.K.*, Causa C-746/18 (v., oltre al contributo richiamato nella nota precedente, N. E. La Rocca, *Dopo la Corte di Giustizia in materia di tabulati: applicazioni e disapplicazioni interne*, in *Arch. pen. (web)* 2021, f. 2, 1 ss.; M. Aranci, *L'acquisizione dei dati esteriori delle comunicazioni nel processo penale italiano dopo la sentenza H.K.: alcuni spunti di riflessione sulle prime applicazioni giurisprudenziali*, in www.lalegislazionepenale.eu, 19.7.2021; P. Di Stefano, *La Corte di giustizia interviene sull'accesso ai dati di traffico telefonico e telematico e ai dati di ubicazione a fini di prova nel processo penale: solo un obbligo per il legislatore o una nuova regola processuale?*, in *CP* 2021, 2556 ss.; L. Filippi, *Il legislatore deve urgentemente riformare la disciplina dell'acquisizione dei tabulati relativi al traffico e all'ubicazione*, www.ilpenalista.it, 15.3.2021; G. Leo, *Le indagini sulle comunicazioni e sugli spostamenti delle persone: prime riflessioni riguardo alla recente giurisprudenza europea su geolocalizzazione e tabulati telefonici*, in www.sistemapenale.it, 31.5.2021; G. Spangher, *I tabulati: un difficile equilibrio tra esigenze di accertamento e tutela di diritti fondamentali*, in www.giustiziainsieme.it, 3.5.2021).

4. Per riprendere quanto osservato in apertura, la sensazione è che le AFRTs siano nel pieno di uno dei «cosiddetti inverni dell'intelligenza artificiale», ovvero di uno di quei «momenti di depressione» che l'IA ha ciclicamente attraversato dopo l'iniziale «euforia» suscitata dalle potenzialità delle innovazioni⁹⁸.

Alla luce delle riflessioni svolte, emerge che a traghettare il nostro ordinamento verso una “stagione” rispettosa dei diritti fondamentali in gioco non potrà essere l'art. 189 Cpp, bensì un'adeguata valorizzazione del diritto alla riservatezza, che non a caso è stato definito l'odierno «baluardo in grado di proteggere l'individuo contro l'avanzata incontrollata di alcune forme “aggressive” di intelligenza artificiale»⁹⁹.

Tuttavia, occorre fare chiarezza: nemmeno le disposizioni delle Carte dei diritti paiono da sole in grado di assolvere questa funzione. Esse sono «tutt'al più capaci di produrre conseguenze invalidanti in relazione ai risultati delle attività», ma non offrono una tutela preventiva idonea a «scongiorare l'illegittima intrusione nella sfera intima prima che la stessa si verifichi»¹⁰⁰. In aggiunta, per ciò che concerne specificamente i precetti convenzionali, la possibilità di desumerne una «regola di esclusione tale da rispondere ai requisiti di tassatività e precisione postulati dall'art. 191 c.p.p.» è tutt'altro che pacifica¹⁰¹.

Detto altrimenti, si rivela imprescindibile un intervento normativo del tenore di quello prospettato dalla Commissione europea che, attraverso la predeterminazione delle condizioni relative all'*an* e al *quomodo* delle operazioni, nonché alle relative sanzioni, individui il punto di equilibrio tra la tutela del *right to privacy* e le opposte esigenze di *law enforcement*.

Peraltro, l'adozione della proposta eurounitaria si rivelerebbe ancor più indispensabile laddove, nell'ambito delle iniziative da mettere in campo per addivenire al c.d. “*Next generation Prüm*”, fosse effettivamente dato seguito alla prospettazione di ampliare le categorie di dati incluse nel meccanismo di scambio informativo fino a ricomprendervi per l'appunto le immagini facciali, innanzitutto attraverso la creazione di banche dati nazionali, quale preconditione necessaria per il trasferimento e la condivisione di tali informazioni¹⁰²: solo così si può scongiurare che le carenze interne ai singoli ordinamenti finiscano per riverberare i propri effetti negativi anche in altri sistemi.

⁹⁸ G. Sartor, *Introduzione*, in *Rivista di filosofia del diritto* 2020, f. 1, 65.

⁹⁹ L. Lupária Donati, *Privacy, diritti della persona e processo penale*, in *RDPr* 2019, 1449.

¹⁰⁰ F. Nicolichia, *op. cit.*, 55.

¹⁰¹ M. Daniele, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *CP* 2013, 374.

¹⁰² Per l'analisi di tali iniziative, con una particolare attenzione rivolta al riconoscimento facciale, v. L. Scaffardi, *Next Generation Prüm e le scelte strategiche della UE: dall'ampliamento dello scambio dei dati genetici all'introduzione del riconoscimento facciale*, in *federalismi.it* 2021, f. 8, 200 ss.