QUESITI

LUISA SAPONARO

Le nuove frontiere tecnologiche dell'individuazione personale

L'evoluzione tecnologica porta al crescente utilizzo di innovativi strumenti di identificazione personale che, spesso, prendono il posto dei tradizionali metodi di individuazione previsti dal codice di rito. Il Sistema automatico di riconoscimento delle immagini costituisce una novità in tal senso che, se da un lato consente una maggiore possibilità identificativa, dall'altro legittima un'invasione altrettanto pericolosa nella sfera dei diritti individuali.

The new technological frontiers of personal identification

Technological evolution implies the use of new personal recognition tools. These systems have replaced the traditional legal procedures envisaged by the code of criminal procedure. The SARI facial recognition system is a paradigmatic case of these new technologies: this system is a powerful mass surveillance tool but could also legitimize a dangerous violation of individual rights.

1. *Il caso.* La vicenda all'origine del ricorso alla Suprema Corte riguardava la questione della validità del riconoscimento facciale effettuato attraverso il SARI (Sistema automatico di riconoscimento immagini). Questo il caso: il pubblico ministero formula richiesta di custodia cautelare nei confronti di X, sul presupposto che le immagini riprese dalle telecamere del luogo del reato[1] – comparate attraverso il SARI *Enterprise* – hanno individuato in X il soggetto autore del delitto. Il giudice per le indagini preliminari rigetta la richiesta di custodia cautelare, motivandola sulla mancanza della gravità indiziaria. Il Tribunale di Milano, investito dell'appello da parte del pubblico ministero, conferma la decisione del gip e precisa, altresì, che le immagini poste alla base del riconoscimento non sono nitide, dunque, non consentono di distinguere i dettagli relativi al soggetto e non risultano idonee a consentirne l'individuazione.

Tale decisione pone diversi interrogativi riconducibili all'utilizzo dell'intelligenza artificiale nel processo penale, alla liceità giuridica di tale nuovo sistema di riconoscimento facciale attraverso dati biometrici, al suo inquadramento sistematico in assenza di normativa *ad hoc*, nonché ai suoi limiti nell'ottica della tutela dei diritti soggettivi.

[1] Il reato ipotizzato era tentato omicidio e porto di oggetto atto ad offendere.

Il ruolo e l'utilizzo dell'intelligenza artificiale[2] è diventato quasi essenziale nella nostra quotidianità: i sistemi automatizzati, conoscono e studiano le nostre abitudini elaborandole in dati[3], riuscendo così ad anticipare i bisogni dell'uomo. Ed è proprio questa capacità di plasmarsi sulle necessità di ognuno l'elemento che conferisce ai sistemi automatizzati la caratteristica dell'essenzialità. Tutto ciò si traduce nella pratica processuale in quella che viene definita "giustizia predittiva"[4]. Il sistema automatizzato, grazie all'utilizzo di algoritmi, riesce a prevedere l'esito della controversia o la commisurazione della pena, così come attraverso il *match* di varie informazioni riesce a individuare un soggetto.

I metodi di riconoscimento personale, previsti originariamente dall'ordinamento, risultano, così, facilmente superati attraverso il ricorso a nuovi strumenti tecnologici atti all'individuazione soggettiva. Il dettato codici-

---

[2] Cfr. ALGERI, *Intelligenza artificiale e polizia predittiva*, in *Dir. pen. proc.*, 2021, 724; CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, in *www.sistemapenale.it*, 8 gennaio 2021; CICCONI, *Linguaggio giuridico e intelligenza artificiale* in *Diritto e intelligenza artificiale*, a cura di Alpa, Pisa, 2020; CIRONE, *Big data e tutela dei diritti fondamentali: la ricerca di un (difficile) equilibrio nell'ambito delle iniziative europee,* in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, a cura di Dorigo, Pisa, 2020, 143; FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, 1676; PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in *Intelligenza Artificiale, protezione dei dati personali e regolazione*, a cura di Pizzetti, Torino, 2018; QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, 2020; Ead., *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *www.lalegislazionepenale.eu*, 18 dicembre 2018; Ead., *Equo processo penale e sfide della società algoritmica*, in *BioLaw Journal*, 2019, 1, 135 ss.; RICCIO-SCORZA-BELISARIO, *GDPR e normativa privacy*, Milano, 2018; SELLAROLI, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Dir. pen. cont.*, 2019, 6, 47; RICCIO, *Ragionando su intelligenza artificiale e processo penale*, in *questa Rivista*, 2019, 3; RUFFOLO, *Intelligenza Artificiale,* machine learning *e responsabilità da algoritmo*, in *Giur. it.*, 2019, 1689; SANTOSUOSSO, *Intelligenza artificiale e diritto*, Milano, 2020. In tema v. pure *White Paper on* Artificial *Intelligence: a European approach to excellence and trust* COM(2020)65 final, 19.2.2020, in www.*ec.europa.eu*.

[3] In tema di *Big Data v.*: DELLA MORTE, Big data *e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2018, 178 ss.; DE MAURO-GRECO-GRIMALDI, *A Formal definition of Big Data based on its essential features*, in *Library Review*, 2016, 65, 122 ss.; DE GREGORIO-R. TORINO, *Privacy, tutela dei dati personali e Big Data*, in *Privacy Digitale*, a cura di Tosi, Milano, 2019, 447 ss.; NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, in *Law and Media Working Paper Series*, 2017, 6.

[4] Cfr. LOPEZ, *Riconoscimento facciale tramite software e individuazione del sospettato*, in *Preinvestigazioni*, a cura di Scalfati, Torino, 2020, 295. In tema v. *ex multis*: BICHI, *Intelligenza digitale, giurimetria, giustizia predittiva e algoritmo decisorio. Machina sapiens e il controllo sulla giurisdizione*, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, a cura di Ruffolo, cit., 424.

stico diventa un sistema residuale da applicare, solo in forma analogica, ai nuovi metodi captativi. Pertanto, la ricognizione personale *ex* art. 213 c.p.p.[5], l'identificazione effettuata dalla polizia giudiziaria *ex* art. 349 c.p.p.[6] o l'individuazione effettuata dal pubblico ministero *ex* art. 361 c.p.p.[7], quali metodi tradizionalmente utilizzati per il riconoscimento di un soggetto, vengono ora convertiti in strumenti di captazione tecnologicamente avanzati; si pensi al riconoscimento effettuato utilizzando immagini per mezzo di impianti di videosorveglianza o alle individuazioni ottenute semplicemente inserendo un'immagine in un *database* di riconoscimento facciale.

Il dettato normativo resta un passo indietro rispetto all'evoluzione tecnologica, determinando una sorta di indolenza legislativa che, al fine di legittimare l'impiego di tali strumenti di captazione, favorisce il ricorso all'applicazione analogica di alcune norme, quando, invece, per i diritti e gli interessi coinvolti, sarebbe necessaria una disciplina *ad hoc*. Difatti, la scelta di disciplinare in maniera puntuale le tecniche di installazione delle telecamere e l'utilizzo dei dati ottenuti[8], visti i diritti in gioco, fa propendere ancora di più per la assoluta impossibilità di applicazione analogica della normativa relativa alle immagini, spostando l'attenzione su di una disciplina autonoma che attribuisca legittimità, non soltanto ai sistemi, ma anche all'utilizzo in sede processuale dei risultati ottenuti.

---

[5] In argomento, v. BERNASCONI, *La ricognizione di persone nel processo penale*, Torino, 2003; BONZANO, *Attività del pubblico ministero*, in *Indagini preliminari e udienza preliminare*, a cura di Garuti, in *Trattato di procedura penale*, diretto da Spangher, Milano, 2009, 327; CAPITTA, *Ricognizioni e individuazioni di persone nel diritto delle prove penali*, Milano, 2001; CAVINI, *Le ricognizioni e i confronti*, Milano, 2015; CECANESE, *Confronto, ricognizione ed esperimento giudiziale nella logica dei mezzi di prova*, Napoli, 2013; CHELO, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria,* Padova, 2014; MOSCARINI, voce *Ricognizioni (proc. pen.)*, in *Enc. giur.* XXVII, Roma, 1991, 3; PRIORI, *La ricognizione di persone dal modello teorico alla prassi applicativa*, in *Dir. pen. proc.*, 2006, 376; TRIGGIANI, *Ricognizioni mezzo di prova nel nuovo processo penale*, Milano, 1998.

[6] Cfr. BONSIGNORI, *Nuovi profili processuali delle indagini motu proprio della polizia giudiziaria*, in *Le nuove norme sulla tutela della riservatezza dei cittadini*, a cura di Spangher, Milano, 2001, 148; CURTOTTI-SARAVO, *Il volo di Icaro delle investigazioni sulla scena del crimine: il ruolo della polizia giudiziaria*, in *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, a cura di Conti, Milano, 2011, 201 ss.; D'AMBROSIO-VIGNA, *La pratica di polizia giudiziaria*, Padova, 1998.

[7] CECANESE, *Aspetti problematici e snodi interpretativi dell'individuazione di persone e di cose*, in *questa Rivista*, 2018, 1.

[8] Provvedimento del Garante *Privacy* 1712680 del 2010, considerato nei limiti di compatibilità con l'art. 22, comma 4, d.lgs.101/2018 e, in combinato disposto con le Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video.

2. *Nuovi strumenti di identificazione personale: il sistema automatico di riconoscimento delle immagini.* In questo contesto di innovazione tecnologica nell'identificazione personale si inserisce il SARI – acronimo di "Sistema automatico di riconoscimento delle immagini", introdotto nel 2017[9], in forma di supporto alle attività investigative e di sorveglianza della polizia scientifica – che rappresenta la nuova frontiera dell'individuazione personale. Questo sistema di intelligenza artificiale opera attraverso algoritmi di riconoscimento delle sembianze facciali che consentono di comparare l'immagine captata con tutte quelle presenti nella banca dati del sistema, al fine di trovare quella corrispondente o più affine al soggetto ricercato. Il sistema utilizza le c.d. *face-print*, ovvero le caratteristiche precipue di un viso, che sono registrate ed elaborate a monte dal sistema e, attraverso tali peculiarità, elabora e predispone un modello di individuazione (*template*), necessario per la comparazione con altre immagini, al fine di effettuare l'identificazione.
L'assenza di un riferimento normativo da un lato, e la necessità di un inquadramento giuridico dall'altro, portano a far confluire tale nuova tipologia di individuazione personale nella categoria delle pre-investigazioni – quali «atti e attività realizzate quando la *notitia criminis* non si è manifestata in alcuni o tutti i suoi contorni costitutivi»[10] – allorquando la ricerca effettuata attraverso il SARI sia precedente alla formazione definitiva della notizia di reato, e nella categoria delle indagini atipiche,[11] quando tale sistema automatico viene utilizzato per l'individuazione personale, dopo l'iscrizione della notizia di reato, in sostituzione dei "tradizionali" sistemi identificativi previsti dal codice di rito.
I dati personali attraverso cui si effettua il riconoscimento nel SARI, sono rilevati biometricamente[12]: si tratta di dati, idonei ad identificare in modo uni-

[9] Il Ministero dell'Interno ha stipulato un contratto con l'azienda italiana Parsec 3.26, fornitrice del *software*, che collabora con l'ISASI (Istituto di scienze applicate e sistemi intelligenti) del Centro nazionale per le ricerche e lo sviluppo di algoritmi di riconoscimento facciale.
[10] SCALFATI, *Il fermento pre-investigativo*, in *Pre-investigazioni*, a cura di Scalfati, cit., 1.
[11] In tema v. per tutti *Le indagini atipiche*, 2ª ed., a cura di Scalfati, Torino, 2019.
[12] ALESCI, *Il corpo umano fonte di prova,* Milano, 2017, 89; AMATO-CRISTOFARI-RACITI, *Biometria. I codici a barre del corpo*, Torino, 2013, 33; DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della* High Court of Justice *(ma raccoglie le critiche del Garante Privacy d'Oltremanica)*, in *www.sistemapenale.it*; GULOTTA-TUOSTO, *Il volto nell'investigazione e nel processo. Nuova fisiognomica forense*, Milano, 2017, 114; LOPEZ, *La rappresentazione facciale tramite* software, in *Le indagini atipiche*, cit., 239; PREITE, *Il riconoscimento biometrico. Sicurezza* versus *Pri-*

voco un soggetto, che costituiscono una *species* precisa del *genus* "dati personali".
Punto di partenza è sempre il dato personale così come indicato all'art. 4, lett. b) del c.d. Codice della *privacy*-d.lgs. 196/2003, modificato dal d.lgs. 101/2018[13]: è definito dato personale «qualunque informazione relativa ad una persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale»; in questa categoria rientrano, a giusto titolo, le immagini di una persona, in quanto contenenti "informazioni" relative alla stessa. I dati biometrici, in particolare, sono definiti nell'allegato A al provvedimento del Garante *privacy* 12/11/2014, come dati ricavati da «proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili, laddove tali caratteristiche o azioni sono tanto proprie di un certo individuo quanto misurabili»[14] e risultano, pertanto, in grado di identificare in modo abbastanza certo un determinato soggetto. Possono elencarsi, a titolo esemplificativo, tra i dati biometrici: la scansione della retina, l'immagine dell'iride, le caratteristiche vocali, le impronte digitali, il colore della pelle ovvero le caratteristiche comportamentali di un individuo come il modo di muovere le mani, di camminare, ecc. È di tutta evidenza, quindi, che i biometrici siano dati individuali particolarmente sensibili, in grado per un verso di permettere una rapida identificazione del soggetto, per altro verso di costituire una grave lesione del diritto alla *privacy*. Un esempio in tal senso è il riconoscimento facciale: se da un lato si tratta "praticamente" di un sistema non

vacy, Trento, 2007, 37; SACCHETTO, *Face to face: il complesso rapporto tra* automated facial recognition technology *e processo penale*, in *www.lalegislazionepenale.eu*, 16 dicembre 2020, 1.

[13] "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la Direttiva 95/46/CE".

[14] Tale definizione è contenuta nell'allegato A suddetto, ma riporta una definizione data dal gruppo di lavoro art. 29 per la tutela dei dati personali costituito da rappresentanti delle Autorità di protezione dati dei diversi stati membri dell'Unione Europea-*Working Party* art 29 o WP29, in quanto previsto dall'art. 29 della direttiva europea 95/46-, Parere 2/2012 (WP192) sul riconoscimento facciale nei servizi *online* e mobili, 3/2012 (WP193) sugli sviluppi nelle tecnologie biometriche, adottato il 27 aprile 2012, che a sua volta riprende la definizione dello stesso gruppo di lavoro, nel parere 4/2007 (WP136). Il WP29 è stato sostituito dall'*European data protection board* (Comitato europeo per la protezione dei dati) con il nuovo Regolamento europeo generale per la protezione dei dati personali (*General data Protection Regulation* o GDPR) 2016/679.

invasivo, dall'altro può risultare gravemente lesivo dei diritti individuali soggettivi.

Il sistema automatico di riconoscimento delle immagini ripropone, infatti, la sempre attuale questione del reale bilanciamento tra interesse dello Stato alla repressione dei reati e tutela delle libertà del singolo[15]. La conquista di un equilibrio, in tal senso, nel tempo è diventata più precaria, dovendo riconoscere la crescente invasività, nella sfera della libertà personale, da parte dei sistemi di captazioni di immagini strettamente collegati ad un sempre più articolato sviluppo tecnologico-digitale[16].

Il SARI opera in due modalità: *Entrerprise* o *Real time*, la prima rappresenta la forma di automazione di un sistema di riconoscimento da sempre esistente, che non genera particolari lesioni dei diritti individuali, e, in quanto tale, è stato ritenuto utilizzabile dall'Autorità garante della protezione dei dati personali[17]. Con l'identificazione attraverso SARI *Enterprise*, l'operatore inserisce in una banca dati di circa dieci milioni di elementi[18] l'immagine di un soggetto,

---

[15] In tema *ex multis*: BONETTI, *Riservatezza e processo penale*, Milano, 2003; FAMIGLIETTI, *Il diritto alla riservatezza o la riservatezza come diritto*, in *Bio-tecnologie e valori costituzionali*, a cura di D'Aloia, Torino, 2005, 299; S. FIORE, voce *Riservatezza*, in *Enc. giur.*, VIII, Roma, 2000, 6; LUPÀRIA DONATI, *Privacy, diritti della persona e processo penale*, in *Riv. dir. proc.*, 2019, 1448; RODOTÀ, *Intervista su* privacy *e libertà*, Bari, 2005; SCALISI, *Il diritto all'immagine, il diritto al segreto, la tutela dei dati personali, il diritto alle vicende della vita privata, gli strumenti di tutela*, Milano, 2002; UBERTAZZI, *Il diritto alla* privacy. *Natura e funzione giuridiche*, Padova, 2004.

[16] In tema: Cyber forensics *e indagini digitali. Manuale tecnico giuridico e casi pratici*, a cura di Aterno-Cajani-Costabile-Curtotti, Torino, 2021; CONTI-BACCARI, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla* privacy, in *Dir. pen. proc.*, 2021, 6, 711; BACCARI, *Il trattamento anche elettronico dei dati personali per finalità di accertamento dei reati*, in *Cybercrime*, diretto da Cadoppi-Canestrari-Manna-Papa, Milano, 2019, 1599; CURTOTTI, *Indagini* hi-tech*, spazio* cyber*, scambi probatori tra stati e* internet provider service *e "vecchia europa": una normativa che non c'è (ancora)*, in *Dir. pen. proc.*, 2021, 6, 745; IASELLI, *Investigazioni digitali*, Milano, 2020; LUPARIA, *Diritto alla* privacy, in *Diritti della persona e nuove sfide del processo penale*, *Atti XXXII Convegno nazionale dell'Associazione tra gli studiosi del processo penale*, Salerno 25-27 ottobre 2018, Milano, 2019, 97 ss.; TORRE, Privacy *e indagini penali*, Milano, 2020, Id. *Nuove tecnologie e trattamento dei dati personali*, in *Dir. pen. proc.*, 2021, 1042.

[17] Parere Garante della protezione dei dati personali 26 luglio 2018, n. 9040256: «Il trattamento in argomento costituisce, infatti, un mero ausilio all'agire umano, avente lo scopo di velocizzare l'identificazione, da parte dell'operatore di polizia, di un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato».

[18] I dati sono sia impronte digitali, sia immagini di volti con relative caratteristiche biometriche, sia dati anagrafici di soggetti sottoposti a fotosegnalamento, vengono utilizzate diverse piattaforme (A.F.I.S., *Automated finger print identification system*, S.S.A. Sotto sistema anagrafico)

al fine di individuarne l'identità: il sistema si sostituisce all'operatore nella ricerca all'interno delle banche dati, comparando l'immagine del soggetto da ricercare con le altre presenti nell'archivio, in cerca di una possibile corrispondenza. Al termine della ricerca, il sistema propone un elenco di foto segnaletiche somiglianti al soggetto da identificare, tra cui l'operatore dovrà individuare quella più affine al ricercato. L'uso di tale modalità operativa velocizza le operazioni di riconoscimento, limitando l'apporto degli investigatori che non devono più inserire manualmente dati anagrafici o altri dati identificativi del soggetto agevolando l'attività d'indagine, così come accaduto nel caso di specie.

La modalità *Real time*, invece, pone interrogativi più rilevanti in ordine alla lesione dei diritti individuali. Tale sistema di riconoscimento è mobile, può essere installato ovunque e può fungere da sistema di videosorveglianza in quanto prevede la possibilità di registrare le riprese mediante telecamere installate in una determinata area geografica. La procedura consente di analizzare in tempo reale i volti ripresi, in particolare alcuni dati biometrici degli stessi, di confrontarli con altri presenti in una banca dati predefinita, la c.d. *watch list* – che può contenere al massimo diecimila volti – e, qualora attraverso un algoritmo di riconoscimento venga rilevata una corrispondenza tra il volto ripreso e quello presente nella *watch list*, generare un *alert* che consente agli operatori di intervenire. Diversamente, la procedura di identificazione genera una *candidate list*: una lista di soggetti simili a quello da individuare dove, come nel caso precedente, sarà compito dell'operatore trovare il volto più affine al ricercato sulla base di vari parametri. In entrambe le ipotesi sarà un "uomo" e non il sistema ad effettuare l'individuazione, circostanza che, teoricamente, dovrebbe rappresentare una garanzia di tutela dei diritti individuali dei singoli. Il grado di certezza dell'identificabilità di un soggetto varia in base alla qualità dell'immagine – più questa è nitida più semplice sarà il riconoscimento – e alla tipologia di dato biometrico in possesso dell'autorità: laddove il dato biometrico sia costituito da una caratteristica fisica, l'identificazione del soggetto sarà certa; qualora, invece, il dato biometrico sia costituito da una caratteristica comportamentale, il grado di attendibilità del *match* potrà essere al 90%.

Dove individuare il punto di criticità, allora? Lungi dall'essere una semplice videoripresa, il sistema di riconoscimento delle immagini nella modalità *Real time*, crea problemi di invasività nella sfera della *privacy* del singolo, ben più

rilevanti di quelli connessi ai semplici impianti preposti alla sorveglianza[19]. In primo luogo, tale sistema consente di individuare un soggetto sulla base di precise caratteristiche fisiologiche o comportamentali che, in un momento successivo, verranno analizzate in relazione a ciascun individuo presente nel luogo in cui è installato lo strumento captativo, al fine di trovare il soggetto ricercato. Di seguito, qualora il sistema rilevi una corrispondenza, gli agenti provvederanno immediatamente ad un controllo diretto sul soggetto individuato; non è difficile evidenziare quanto la procedura possa risultare utile qualora l'algoritmo di riconoscimento funzioni correttamente, mentre si riveli estremamente lesiva dei diritti personali qualora il sistema generi un falso positivo. Il sistema, infatti, può essere fallace producendo falsi positivi o falsi negativi[20]: se dal punto di vista dei diritti fondamentali sarà preferibile l'ipotesi della mancata identificazione di un "colpevole" piuttosto che l'errata identificazione di un innocente, allorquando si verifichi un falso positivo, il soggetto verrà comunque fermato, interrogato e la propria immagine sarà conservata nel *database*. Malgrado la tendenza politica sia quella di far trapelare poco o nulla di ufficiale, sia in merito alle modalità operative di funzionamento del sistema (numero effettivo dei volti archiviati, banche dati realmente utilizzate), sia sulla reale affidabilità dello stesso[21] (numero di falsi positivi o di falsi negativi generati dai sistemi), l'esperienza, nazionale ed internazionale indica che tali sistemi di riconoscimento risultano spesso fallaci anche perché, essendo le

[19] In tema v.: GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Dir. pen. cont.*, 29 maggio 2019; NIEVA FENOLL, *Intelligenza artificiale e processo*, Torino, 2019; PARODI-SELLAROLI, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Dir. pen. cont.*, 2019, 6, 47; QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, cit.; UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *www.sistemapenale.it*.

[20] Durante la finale di Champions League del 2017 tra Juventus e Real Madrid a Cardiff il sistema utilizzato ha identificato 2470 possibili sospetti sbagliando il riconoscimento in 2297 casi, cioè il 92% delle volte**.** La polizia del Galles ha dichiarato che l'elevato numero di false corrispondenze era dovuto alle immagini di scarsa qualità fornite da Uefa e Interpol, ma la spiegazione non è sufficiente. Percentuali peggiori, 98% di errori, sono stati registrati dalla Metropolitan Police britannica, come ha scoperto il gruppo del Regno Unito per le libertà civili *Big Brother Watch* (BBW) che ha chiesto di dismettere il sistema perché inutile e perché le telecamere di riconoscimento facciale violerebbero l'articolo 8 dello Human Right Act del 1998 in cui si afferma che qualsiasi interferenza nella vita privata debba essere necessaria e proporzionata. Nel caso della partita di Cardiff ad esempio i volti di 2451 persone analizzate sono stati archiviati per 12 mesi come previsto dall'*Investigatory Power Act* 2016: ROMANDINI, *Come (non) funziona il sistema Sari di riconoscimento facciale*, *www.wired.it*.

[21] LOPEZ, *La rappresentazione facciale tramite software*, cit., 246.

tecnologie utilizzate particolarmente sensibili, non sempre riescono a "lavorare" correttamente sul colore della pelle o sulle identità di genere[22].
Un secondo aspetto che merita attenzione riguarda la sorte delle immagini captate dal sistema: mentre l'immagine del soggetto da individuare, indipendentemente dal modo in cui si è concluso il processo identificativo, resta depositata in memoria nell'archivio della banca dati, nulla è dato sapere, sempre per la scelta politica del riserbo sulla questione, sul possibile utilizzo delle altre immagini catturate dal sistema *Real time*: si ignora, ad esempio, se vengano tutte eliminate o comunque salvate dal sistema, pronte a generare altre e nuove connessioni investigative. È legittimo sospettare che alcune immagini possano essere conservate al sol fine di incrementare la banca dati e per costituire un archivio permanente.
Infine, ed è forse l'aspetto più inquietante, la ricerca da parte del sistema consiste, ad esempio, nella comparazione tra la scansione dell'immagine della retina del soggetto da identificare con la scansione biometrica della retina di tutti gli altri soggetti presenti in un determinato luogo, circostanza che rappresenta la vera e propria insidia di questa modalità del sistema. Come si dirà meglio in seguito, questa semplice modalità operativa del sistema *Real time* implica il controllo di tutti i soggetti presenti nel luogo di ricerca, portando alla degenerazione del controllo di massa.

3. *Gli effetti delle operazioni di riconoscimento.* La disciplina relativa al trattamento dei dati biometrici è prevista dal *Regolamento generale sulla protezione dei dati* (RGDP)[23], recepito dalla legislazione italiana nel d.lgs.

[22] In tema ANGIUS-COLUCCINI, *Riconoscimento facciale nel database di Sari quasi 8 schedati su 10 sono stranieri*, in *www.wired.it*, 3 aprile 2019. Joy Buolamwini, ricercatrice MIT, ha verificato varie tipologie di riconoscimenti facciali elaborati da Microsoft, Ibm e Megvii, e ha stabilito che «nel complesso, i soggetti maschili sono classificati più accuratamente di quelli femminili» e che «i soggetti più chiari sono riconosciuti con più precisione rispetto a quelli più scuri», e ha verificato che il sistema ha difficoltà rispetto alle differenze di genere, i suoi studi sono stati utilizzati da Ibm, Microsoft e Google, v. *Gender Shades – MIT Media Lab; Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products – MIT Media Lab.*

[23] Regolamento europeo n. 679 del 2016, cui l'Italia si è adeguata con il d.lgs. 101/2018, che è stato integrato dal DPR 15/2018 "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia" e ha modificato parte del d.lgs. 196/2003 Codice in materia di protezione dei dati personali. Anche l'art. 6 DPR 15/2018 specifica che «i trattamenti dei dati personali che implicano maggiori rischi di un danno alla persona interessata, con particolare riguardo alle banche di

101/2018. Se l'art. 9 comma 1 RGDP stabilisce il divieto di trattamento di dati biometrici tesi ad individuare in modo certo un determinato soggetto, il comma 2 già contiene alcune eccezioni[24]: *in primis,* il necessario consenso dell'interessato, nonché la tutela di un interesse vitale dell'interessato o di un'altra persona fisica; e, infine, la tutela di un interesse pubblico rilevante sulla base del diritto dell'Unione europea o degli Stati membri, anche nel caso in cui tale interesse riguardi la sanità pubblica[25].
In adeguamento, l'art. 7 d.lgs. 51/2018[26] dispone l'assoluta necessità di una disciplina normativa, stabilendo che il trattamento dei dati di cui all'art. 9 RGDP sia autorizzato «solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea e da legge o, nei casi previsti dalla legge da regolamento», laddove «necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato».

---

dati genetici o biometrici, alle tecniche basate su dati relativi all'ubicazione, alle banche dati e ai trattamenti di cui all'articolo 7 basati su particolari tecniche di elaborazione delle informazioni o su particolari tecnologie, sono effettuati nel rispetto delle misure e degli accorgimenti prescritti dal Garante ai sensi dell'articolo 17 del Codice, sulla base di preventiva comunicazione inviata con le modalità indicate nell'articolo 39 del Codice», ma a seguito delle modifiche apportate dal d.lgs. 101/2018 gli artt. 17 e 39 del Codice sulla protezione dei dati personali sono stati abrogati.

[24] A proposito di deroghe alla disciplina prevista per la protezione dei dati personali a fine della tutela della sanità pubblica non è possibile non menzionare l'art. 14 D.L. 9 marzo 2020 n. 14 che opera sino "al termine dello stato di emergenza deliberato dal Consiglio dei ministri in data 31 gennaio 2020" (c.d. emergenza Covid-19), ai fini dell'adozione da parte delle autorità competenti delle misure urgenti di contenimento e gestione dell'emergenza epidemiologica ai sensi dell'art. 3 del D.L. n. 6/2020, convertito con modificazioni dalla L. 13/2020. Tale deroga ha legittimato l'utilizzo di termoscanner in aeroporto o comunque la legittimazione alla misurazione della temperatura in luoghi pubblici o aperti al pubblico.

[25] L'art. 9 RGDP prevede tra le altre possibilità di eccezione: il trattamento utilizzato per assolvere obblighi dell'interessato, diritti specifici del titolare del trattamento in materia di diritto del lavoro, della sicurezza sociale e della protezione sociale; il trattamento di dati resi pubblici dall'interessato; il trattamento di dati di membri o ex membri di un'associazione, fondazione, o altro organismo senza scopo di lucro, nell'ambito delle sue legittime attività; il trattamento è necessario per accertare esercitare o difendere un diritto in sede giudiziaria o allorquando venga esercitata dall'autorità funzione giurisdizionale; il trattamento necessario per finalità di medicina preventiva o di medicina del lavoro; il trattamento ai fini di ricerca scientifica, storica o statistica.

[26] Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

A fronte di una incertezza regolamentare, si richiama quanto stabilito nella *Convenzione sulla protezione degli individui rispetto al trattamento automatizzato di carattere personale*[27] all'art. 6 (Conv. 108+) ove è stabilito che l'utilizzo di dati biometrici, idonei ad identificare in maniera univoca un individuo, può essere consentito solo in presenza di adeguate garanzie sancite dalla legge che integrino gli aspetti normativi previsti dalla Convenzione. Tali garanzie legislative sono approntate per tutelare gli interessi, i diritti e le libertà fondamentali dell'individuo, titolare di tali dati sensibili, soprattutto dal rischio di discriminazione (art. 6, par. 2). Il rischio è che tale sistema diventi un modo per identificare minoranze culturali, etniche o per individuare soggetti appartenenti ad associazioni[28]. Il Comitato Consultivo della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di carattere personale[29] ha adottato, inoltre, in data 28 gennaio 2021, le "*Linee guida sul riconoscimento facciale*" che, oltre ad indicare le regole base per l'uso di tali sistemi di individuazione , in ambito sia pubblico sia privato[30], ribadisce all'art. 1, richiamando l'art. 6 della Convenzione 108+, la necessità di un presupposto di natura giuridica, quale fonte di legittimità dei sistemi di riconoscimento biometrici.

[27] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di carattere personale datata 28 gennaio 1981, tale convenzione è stata aggiornata, attraverso un protocollo di modifica da parte del Consiglio d'Europa il 18 maggio 2018, ratificata dall'Italia con l. 60/2021 al fine di rafforzare la protezione dei dati, si parla attualmente di Convenzione 108+.

[28] Nel 2016 la Commissione Europea ha proposto di utilizzare il riconoscimento facciale per contenere la crisi migratoria, utilizzando l'Eurodac (*European Asylum Dactyloscopy*) un database europeo delle impronte digitali per coloro che richiedono asilo politico e per le persone fermate mentre varcano irregolarmente una frontiera esterna dell'Unione Europea. Oltre alle impronte digitali i dati contenuti indicano lo Stato membro d'origine, il luogo e la data dell'eventuale domanda d'asilo, il sesso, un numero d'identificazione, nonché la data in cui sono state prese le impronte digitali e la data in cui sono stati trasmessi i dati ad Eurodac. La FRA (*European UnionAgency for Fundamental Rights*) nel 2019 ha sottolineato la pericolosità di tale tipologia di controllo.

[29] Istituito ai sensi dell'art. 18 della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di carattere personale.

[30] Tali linee guida distinguono il trattamento in ambito pubblico che opera secondo leggi e regolamenti, ma senza l'espresso consenso di ogni singolo individuo, che deve essere comunque adeguatamente informato, attraverso cartellonistica idonea, e il trattamento in ambito privato dove è necessario il consenso espresso del soggetto.

4. *Il parere del Garante della protezione dei dati personali sul SARI Real time.* Il Ministero dell'Interno, in osservanza dell'art. 23 d.lgs. 51/2018[31] ha redatto e sottoposto al Garante della protezione dei dati personali, quale autorità di controllo, un documento di valutazione formulato sul presupposto che il sistema di riconoscimento facciale «rappresenta un rischio elevato per i diritti e la libertà delle persone fisiche», generando, pertanto, un forte impatto sulla protezione dei dati del sistema SARI *Real time*. L'allegato 1 al provvedimento 467 dell'11 ottobre 2018, che contiene l'elenco di tipologie di trattamenti soggetti a meccanismi di coerenza, da sottoporre a valutazione di impatto, ai punti 7 e 10, prevede i trattamenti effettuati attraverso l'uso di tecnologie innovative, nonché espressamente i dati biometrici *ex* art. 9 RGDP, in quanto incidenti su aspetti particolarmente sensibili della vita delle persone. Premesso che, ai sensi dell'art. 4 RGDP, «il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità», resta l'urgenza di rinvenire una base giuridica legittimante l'invasione nella sfera dei diritti individuali, lesione che deve essere proporzionata al bene sociale da tutelare.
Il Garante *privacy*, pronunciandosi sulla questione, ha dato parere negativo alla richiesta del Ministero dell'Interno, circa l'installazione del SARI *Real time* in spazi pubblici, con provvedimento n. 127 del 25 marzo 2021[32]. L'autorità di controllo, in ossequio a quanto previsto dalle Linee guida del Consiglio d'Europa[33], sottolinea, infatti, l'intrusività del sistema di captazione

[31] «Se il trattamento, per l'uso di nuove tecnologie e per la sua natura, per l'ambito di applicazione, per il contesto e per le finalità, presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima di procedere al trattamento, effettua una valutazione del suo impatto sulla protezione dei dati personali».
[32] L'Autorità garante della protezione dei dati personali aveva già vietato l'installazione del SARI *Real time* nel parco della città di Como (impianto già installato prima della richiesta al Garante) con provvedimento n.9309458 del 26 febbraio 2020, sempre basandosi sulla mancanza del fondamento giuridico di tale sistema di riconoscimento.
[33] Il Comitato Consultivo della Convenzione 108+, istituito presso il Consiglio d'Europa, in data 28 gennaio 2021, ha adottato delle linee guida in materia di riconoscimento facciale, richiamando la necessità di un approccio precauzionale e mostrando preoccupazione circa i rischi di ingerenza sui diritti umani. Lo stesso Comitato ha stabilito che l'uso di tali sistemi di riconoscimento facciale debba essere limitato a situazioni di pericolo imminente e grave alla sicurezza pubblica e debba essere preventivamente sottoposto al parere delle Autorità di protezione dei dati prima dell'utilizzo o della sperimentazione. Tali linee guida prevedono, inoltre, la possibilità per le persone sottoposte a tali sistemi di esercitare il diritto di rettifica e il diritto di non essere sottoposto a decisioni puramente automatizzate senza che la propria

dati sul «diritto alla vita privata e alla dignità delle persone, unitamente al rischio di ripercussioni negative su altri diritti umani e sulle libertà fondamentali», dal momento che tale sistema consente di individuare tutti i soggetti presenti in un determinato luogo.
A sostegno di tale rigetto vi è, innanzitutto, la mancanza di una adeguata base giuridica fornita dal Ministero dell'Interno per l'applicazione del sistema di riconoscimento facciale. Il fondamento normativo addotto non è ritenuto dall'Autorità garante adeguato a giustificare l'invasione nella *privacy* degli individui, soprattutto per la tipologia di dati che interessano tali sistemi. Va tenuto sempre presente che i dati biometrici e tutti quelli idonei a rivelare convinzioni politiche, religiose, sessuali, sindacali necessitano, per essere compressi e compromessi, di una fonte normativa adeguata, che in questo caso manca.
Il Ministero ha addotto, come sostegno legislativo delle videoriprese *de qua*, varie disposizioni normative: oltre al già citato d.lgs. 51/2018, il DPR 15/2018 (protezione dei dati personali relativamente al trattamento dei dati effettuato per finalità di polizia), la l. 121/1981 (sull'ordinamento dell'Amministrazione della pubblica sicurezza), l'art. 1 del Testo unico delle leggi di pubblica sicurezza (T.U.L.P.S.), approvato con regio decreto 18 giugno 1931, n. 773; il decreto del Ministro dell'Interno del 24 maggio 2017 (Individuazione dei trattamenti di dati personali 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, effettuati con strumenti elettronici e i relativi titolari), nonché, e certo non da ultime, disposizioni del codice di procedura penale. Tra queste ultime ricordiamo le modalità di documentazione in forma audiovisiva (art. 134, comma 4, c.p.p.), la prova documentale (art. 234 c.p.p.), i limiti alle intercettazioni (art. 266 c.p.p.), l'attività di polizia giudiziaria: generica (art. 55 c.p.p.), diretta ad assicurare le fonti di prova (art. 348 c.p.p.), relativa agli accertamen-

opinione sia "adeguatamente considerata". Il Comitato precisa, inoltre, che i sistemi di riconoscimento facciale non debbano essere utilizzati «nelle procedure di assunzione del personale, nell'accesso ai servizi assicurativi e all'istruzione», né per determinare il colore della pelle di una persona, o le convinzioni religiose, gli orientamenti sessuali, le condizioni sociali o di salute. Le linee guida sono consultabili al *link 1680a134f3 (coe.int).*

ti urgenti su luoghi, cose e persone (art. 354 c.p.p.) e attività diretta e delegata dal pubblico ministero (art. 370 c.p.p.).
Sulla scorta di tali indicazioni, il Garante riconosce che il SARI *Real time* possa rientrare nell'ambito di applicazione del d.lgs. 51/2018, ma precisa che, ai sensi del combinato disposto di cui agli artt. 1 comma 2 e 5 del d.lgs. 51/2018, il trattamento dei dati personali è da considerarsi lecito quando lo stesso derivi da disposizioni di legge, o se previsto, da regolamenti e sia necessario per l'esecuzione di un compito dell'autorità competente per le finalità di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, inclusa la salvaguardia e la prevenzione di minacce alla sicurezza pubblica. Tale restrizione è in linea con l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, laddove è stabilito il rispetto e la tutela della vita privata e familiare di ogni individuo, senza alcuna ingerenza dell'autorità in tali libertà fondamentali, salvo che sia giustificata dalla legge per la tutela di interessi nazionali di rango pari, se non superiori, al bene giuridico da salvaguardare (pubblica sicurezza, sicurezza nazionale, protezione dei diritti e delle libertà di altri individui, tutela della salute, ecc.). È opportuno, inoltre, precisare che la necessità di una previsione legislativa che legittimi e sostenga l'ingerenza nella vita privata e nei dati personali di un individuo è altresì disciplinata nell'art. 52 della Carta dei diritti fondamentali dell'Unione Europea, nonché nella nostra Carta costituzionale agli artt. 13, 14 e 15, pur non espressamente richiamati dal Garante nel parere *de quo*.
L'Autorità di controllo ritiene che tra le norme addotte a sostegno dell'installazione del sistema di riconoscimento biometrico non ci sia alcuna disposizione che consenta tale tipo di trattamento. I riferimenti codicistici richiamati dal Ministero, a sostegno della legittimità del SARI, risultano troppo labili per consentire il sistema di riconoscimento biometrico facciale, né può effettuarsi un'applicazione analogica della disciplina utilizzata in tema di videoriprese. Non è sostenibile neppure che la fonte si possa rinvenire nel d.lgs. 51/2018, perché questo è deputato a disciplinare le condizioni che consentono l'effettuazione del trattamento, indicando come necessaria un'altra fonte normativa europea o nazionale a sostegno dell'installazione dello stesso. Parimenti, non può trovarsi un appiglio normativo nel DPR 15/2018 che, pur prevedendo e disciplinando il trattamento dei dati, per finalità di polizia, recepiti da sistemi di audio e videosorveglianza, non legittima l'applicazione

analogica della disciplina ai sistemi biometrici di riconoscimento che sono «ontologicamente diversi» dai primi. A ben vedere, neanche l'art. 1 del T.U.L.P.S. contiene una norma specifica sull'argomento, ma disciplina genericamente le attività dell'Autorità di pubblica sicurezza.

5. La tecnologia nel rispetto delle disposizioni del c.p.p. Quanto alle norme del codice di rito, richiamate, è necessario distinguere tra quelle relative alle funzioni della polizia giudiziaria e quelle utilizzate per legittimare l'uso delle videoriprese nel processo penale. Gli artt. 55, 348, 354 e 370 c.p.p. disciplinano, infatti, le funzioni della polizia giudiziaria, l'assicurazione delle fonti di prova, gli accertamenti urgenti su luoghi, cose e persone e gli atti delegati svolti su richiesta del pubblico ministero; nessuna di queste norme, a parere del Garante ed a giusta ragione, è in grado di costituire la fonte normativa richiesta dall'art. 7 d.lgs. 51/2018, in quanto effettivamente in nessuna di esse vi è il minimo riferimento a dati personali sensibili di questo tipo. Ne consegue, pertanto, l'impossibilità di applicare l'art. 55 c.p.p., quale norma generale sulle funzioni della polizia giudiziaria, come appiglio normativo per legittimare il ricorso da parte della polizia a tali sistemi di videosorveglianza: se, per un verso, è innegabile che l'identificazione biometrica costituisca un eccellente sistema per ricercare gli autori dei reati e rappresenti anche un modo per raccogliere fonti di prova, così come disposto all'art. 55, comma 1, c.p.p.; per altro verso, è ugualmente indubbio che i dati personali, oggetto di individuazione attraverso il SARI *Real time*, rappresentino dati talmente sensibili da non poterne legittimare l'acquisizione per applicazione analogica di una norma generale.
Analogo discorso investe le norme che si utilizzano per legittimare l'ingresso delle immagini nel processo penale: la prova documentale e le intercettazioni richiamate dal Ministero a sostegno della legittimità del SARI *Real time*. Il nostro codice di rito non prevede alcuna disciplina circa l'utilizzo delle immagini all'interno del procedimento penale, così il *modus* di ingresso e di valutazione delle stesse nella dinamica processuale è stato costruito nel tempo attraverso concordi pronunce giurisprudenziali che, utilizzando norme codicistiche affini, hanno legittimato l'uso dello strumento investigativo attribuendogli, in alcuni casi, anche valore probatorio. Il giurista, di fronte all'innegabile apporto conoscitivo dato da un'immagine nella ricostruzione del *thema probandum* o nell'identificazione del "presunto colpevole" nella fase prodromica

al processo, ha scelto di legittimare l'ingresso delle immagini, siano esse fotografie o videoriprese, utilizzando la disciplina della prova documentale o quella delle intercettazioni o, ancora, quella della prova atipica. Attraverso le diverse pronunce giurisprudenziali, si è giunti ad elaborare alcune regole base, al fine di consentire l'ingresso delle immagini nel processo penale.

Innanzitutto, è necessario distinguere le immagini riprese in luogo pubblico da quelle captate in luogo privato: l'utilizzabilità delle prime è ammessa in ragione della natura stessa del luogo – nei limiti del rispetto del diritto all'immagine[34] – attraverso il ricorso alla categoria delle prove atipiche *ex* art. 189 c.p.p., nella cui specie, secondo autorevole giurisprudenza[35], rientrerebbero anche i c.d. mezzi di ricerca della prova atipici. In merito alle immagini riprese in un luogo privato, si è giunti ad un'ulteriore distinzione: immagini aventi contenuto comunicativo e altre prive di contenuto comunicativo. Le riprese visive con contenuto comunicativo sono assimilate alle intercettazioni, pertanto soggiacciono alla disciplina degli artt. 266 ss., e possono essere utilizzate quali mezzi di ricerca della prova; diversamente la mancanza di contenuto comunicativo rappresenta causa di inammissibilità al procedimento nel quale l'immagine è stata assunta, ma non in un procedimento diverso. Infatti, le videoriprese prive di contenuto comunicativo possono essere utilizzate nel processo penale come prova documentale *ex* art. 234 c.p.p., per il richiamo ivi previsto a documenti acquisiti mediante fotografia, cinematografia o qualsiasi altro mezzo, allorquando siano formate fuori dal procedimento in oggetto.

Il giurista si è trovato a dover sopperire al silenzio legislativo per garantire l'ammissione della prova visiva quale strumento di portata dimostrativa dirompente; ma tale disciplina di creazione puramente giurisprudenziale è, già di per sé, frutto di una forzatura normativa che non può ulteriormente estendersi ad altre fattispecie ancora più invasive della "semplice" videoripresa. Si

---

[34] CIONTI, *La nascita del diritto sull'immagine*, Milano, 2000; SANTORO, *Diritto all'immagine come diritto costituzionale inviolabile: tutela risarcitoria patrimoniale e non patrimoniale*, in *Nuova giur. civ. comm.*, 2008, 1404.

[35] Cass. Sez. Un., 28 marzo 2006, n. 26795, Prisco, in *Dir giust.*, 2006, 34, 40, con nota di BELTRANI, *Le videoriprese? Sono una prova atipica. Ma le Sezioni Unite non sciolgono il nodo*; in *Dir. pen. proc.*, 2006, 1213 con nota di CONTI, *Le video-riprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati"*; in *Cass. pen.*, 2006, 3937, con nota di DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni Unite*. In tema TRIGGIANI, *Le videoriprese investigative e l'uso dei droni*, in *Le indagini atipiche*, cit., 161 ss.

ritiene, quindi, che le immagini contenenti dati biometrici, in quanto idonee ad identificare in maniera certa un individuo, meritino una disciplina *ad hoc* e non l'applicazione estensiva di un'interpretazione giurisprudenziale per legittimarne l'uso.
Allorquando si argomenta sulle videoriprese, è opportuno applicare la disciplina relativa all'installazione di un impianto di videosorveglianza, non richiamata dal Ministero dell'Interno a sostegno della propria tesi sulla legittimità dell'utilizzo del sistema di captazione SARI *Real time*, nonostante le modifiche intervenute con il nuovo regolamento del 2018, il GDPR *General Data Protection Regulation*, che ha limitato e definito maggiormente il *modus* di utilizzo dei dati personali.

6. *Il rischio reale di una sorveglianza di massa.* Come anticipato, l'ulteriore e più allarmante motivazione espressa nel parere negativo del Garante, riguarda l'utilizzo del sistema di riconoscimento facciale che, senza un'adeguata disciplina normativa, porterebbe ad un'identificazione di massa di tutti i soggetti presenti nel luogo monitorato, determinando, di fatto, il passaggio «dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale», con evidente pregiudizio per i diritti di libertà dei singoli. Se la motivazione formale del diniego all'installazione del SARI *Real Time,* da parte dell'Autorità di controllo, è la mancanza di un valido fondamento normativo, la motivazione reale riposa nel fondato timore che un uso indiscriminato, e non limitato da una previsione normativa *ad hoc*, possa trasformare questo sistema di captazione di immagini in uno strumento di sorveglianza di massa.
Legittimare il Sistema di riconoscimento facciale in tempo reale, senza alcun vincolo legislativo, ribalterebbe completamente il delicato rapporto tra individuo e autorità: se nella videosorveglianza "comune" l'obiettivo è quello di controllare un luogo ed eventualmente, in un momento successivo, qualora si verifichino dei reati, cercare di individuare il colpevole; nella sorveglianza "di massa" l'obiettivo non è più controllare un luogo, ma controllare le persone presenti in quel luogo, con l'effetto che i dati dei soggetti presenti potranno essere analizzati e utilizzati per valutazioni diverse quali, ad esempio, la partecipazione ad un comizio politico, ad una cerimonia religiosa, o ad un incontro sessuale. con una palese, quanto inaccettabile, lesione dei diritti individuali di libertà.

La videosorveglianza a fini repressivi e preventivi si trasformerebbe in una forma di sorveglianza di massa, potendo verificare in tempo reale l'identità di tutti i soggetti captati e non solo la condotta di alcuni[36]. I pericoli sottesi all'utilizzo di tali sistemi di riconoscimento sono evidenti: lesione dei diritti individuali dei singoli, globalmente intesi quale diritto all'immagine, alla riservatezza, alla espressione di pensiero, di opinione politica. In sintesi: l'offesa alla libertà di azione. Lo spettro del costante controllo, inoltre, può generare anche un possibile effetto dissuasivo sul legittimo esercizio di tali diritti, il c.d. *chilling effect*: il timore della sorveglianza che limita la libertà di azione degli individui.

Ecco perché tale forma di controllo non è ammissibile al di fuori di un'adeguata e puntuale normativa, soprattutto in uno Stato che, sia a livello nazionale sia a livello comunitario, riconosce i diritti individuali dei singoli[37].

La possibilità che un sistema di controllo, in un futuro non troppo lontano, possa identificare biometricamente e scansionare i volti di tutti i soggetti presenti negli spazi attraversati dall'individuo da identificare è un'ipotesi che si potrebbe giustificare solo, e soltanto, per gravi ragioni di sicurezza nazionale. Altrimenti, la raccolta indiscriminata di dati biometrici costituirebbe una gravissima invasione e limitazione della sfera della libertà personale.

L'applicazione del SARI *Real time* in tutti i luoghi collettivi o di massa non è giustificabile, perché verrebbe meno la proporzionalità tra pericolo per la collettività e tutela dei diritti individuali e non solo: legittimare un ricorso indi-

---

[36] Sul tema della sorveglianza e del controllo: LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, 2003; ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019.

[37] In Cina sono installate circa 200 milioni di telecamere in tutto il Paese, i cittadini sono sorvegliati ovunque. A Shangai alcune telecamere sono posizionate in prossimità di passaggi pedonali, per cui il cittadino che attraversa con il semaforo rosso viene individuato, la sua immagine mostrata su videoschermi adiacenti, come metodo di censura, e deve pagare una multa (*New York Times*). Il riconoscimento facciale viene utilizzato in Cina non solo a fini di sorveglianza, ma anche per altre attività quali i pagamenti *on line*, l'ingresso in università o condomini, a scuola per valutare l'attenzione degli alunni e si prevede la possibilità. Inoltre, c'è l'intenzione di creare un sistema, già sperimentato in alcune zone, di "credito sociale" che valutando le azioni degli individui distribuirà crediti o sanzioni in base al comportamento. Un'azienda cinese *Hanwang Technology* è riuscita ad elaborare un modo per consentire il riconoscimento facciale anche con la mascherina.

Negli Stati Uniti il ricorso al sistema di riconoscimento facciale biometrico è molto frequente, un *software* dell'Università di Stanford è riuscito ad individuare l'orientamento sessuale degli individui. In Inghilterra il sistema di riconoscimento facciale viene notoriamente utilizzato durante il Carnevale di Notting Hill a fini preventivi.

scriminato a tali forme di individuazione permetterebbe un'ingerenza inammissibile nella vita privata delle persone che si sentirebbero costantemente sorvegliate, vivendo nella finzione della libertà e nella certezza di essere esposti ad un continuo controllo.
Il possibile passaggio dalla sorveglianza al controllo universale è troppo rischioso: la logica della tutela della collettività non deve, in alcun modo, costituire la legittimazione per il controllo della collettività stessa.
L'EDRi, *European Digital Rights*, un gruppo di difesa dei diritti digitali a livello europeo costituito da 35 ONG, esperti e sostenitori, ha chiesto ed ottenuto dalla Commissione europea la registrazione dell'iniziativa *Reclaim your face* per il divieto di utilizzo dei dati biometrici, come forma di sorveglianza di massa. A seguito di tale registrazione è partita una raccolta firme a sostegno dell'iniziativa che, se raggiungerà un milione di firme entro un anno, in almeno sette paesi dell'Unione Europea, chiederà l'impegno della Commissione europea a prendere una posizione precisa sulla questione. L'EDRi sostiene, legittimamente, che l'esercizio della sorveglianza biometrica di massa sia causa di violazione delle norme dell'Unione Europea di protezione dei dati limitando, indebitamente, i diritti delle persone: in particolare, il diritto alla riservatezza, alla non discriminazione, alla libertà di espressione, nonché il diritto di manifestare il proprio pensiero.
Lo stesso Garante europeo della protezione dei dati (GEPD) ha espresso preoccupazione riguardo l'uso di tecnologie che utilizzano dati biometrici, chiedendo di interrompere il ricorso a tali forme di riconoscimento automatico, negli spazi pubblici.
La Commissione europea il 21 aprile 2021 ha presentato una bozza della proposta legislativa per la regolamentazione dei sistemi dotati di intelligenza artificiale, che ha lo scopo di introdurre regole in materia, direttamente applicabili dagli Stati membri, esattamente come accaduto con il GDPR. Il regolamento proposto dalla Commissione europea deve essere vagliato dal Parlamento e dal Consiglio europeo, per cui, molto probabilmente, prima dell'approvazione definitiva, passerà ancora del tempo. Ad ogni modo è importante sottolineare i punti focali del nuovo regolamento: *in primis,* il divieto d'uso dell'identificazione biometrica remota in tempo reale negli spazi pubblici, quindi il divieto dell'uso SARI *Real time*, che, da quanto analizzato, comporta rischi per i diritti fondamentali dell'individuo. Tale divieto prevede delle eccezioni che la Commissione delinea come «rigorosamente definite,

limitate e regolamentate», tra cui l'uso «ai fini di attività di contrasto per la ricerca mirata di potenziali vittime specifiche di reato, compresi minori scomparsi, la risposta a una minaccia imminente di attacco terroristico o l'individuazione e l'identificazione degli autori di reati gravi». Le sanzioni per il mancato rispetto delle prescrizioni imposte potrebbero arrivare fino a 30 milioni di euro o al 6% del fatturato complessivo di un'azienda[38].
Sono proprio le previste eccezioni che destano perplessità sul ricorso a strumenti tecnologici di tale portata, dal momento che, dalla previsione di queste "ipotesi speciali", potrebbe derivare una pericolosa applicazione analogica ad altre fattispecie.

[38] La Vicepresidente della Commissione Margrethe Vestager sostiene che «non c'è posto per la sorveglianza di massa. Per l'intelligenza artificiale, la fiducia non è facoltativa, è indispensabile. Queste regole rappresentano una svolta che consentirà all'UE di guidare lo sviluppo di nuove norme globali per garantire che l'AI possa essere considerata affidabile».