RICONOSCIMENTO FACCIALE E RISCHI PER I DIRITTI FONDAMENTALI ALLA LUCE DELLE DINAMICHE DI RELAZIONE TRA POTERI PUBBLICI, IMPRESE E CITTADINI (*)

di Marco Colacurci

Il contributo ambisce ad approfondire da un'angolazione penalistica alcune delle problematiche relative all'utilizzo, da parte di attori pubblici e privati, delle tecnologie di riconoscimento facciale, come tali in grado di registrare e processare i dati biometrici di un numero indefinito di individui. L'obiettivo è mettere in evidenza i rischi derivanti dall'utilizzo di tali strumenti da un punto di vista dei rapporti tra Stato e cittadini, anche alla luce del ruolo centrale svolto dalle imprese che sviluppano simili tecnologie, in assenza, ad oggi, di discipline organiche sul tema. Pertanto, dopo aver inquadrato lo sviluppo delle TRF come fenomeno coerente con le teorizzazioni in materia di società del controllo e capitalismo della sorveglianza, e dopo averne brevemente illustrato il funzionamento, sono passati in rassegna alcuni esempi problematici nel contesto cinese e in quello statunitense. In seguito, l'attenzione si focalizza sull'ambito interno, in particolare su alcune pronunce del Garante per la protezione dei dati personali intervenute sul tema, nonché sulla Proposta di Regolamento della Commissione Europea in materia di IA. L'analisi della proposta è utile a evidenziare, in chiave conclusiva, la necessità di un dibattito pubblico partecipato e consapevole, capace di far risaltare rischi e benefici delle TRF e dunque utile a orientare le scelte del legislatore.

(*) Il testo è stato elaborato nell'ambito del progetto di ricerca interdipartimentale su "*The use of AI neural networks in the fight against corporate crimes*" realizzato presso l'Università della Campania "Luigi Vanvitelli" sotto la coordinazione scientifica della Dott.ssa De Simone

1. Introduzione: i rischi della diffusione delle tecnologie di riconoscimento facciale da un'angolazione penalistica.

Nel marzo del 2022, con l'invasione dell'Ucraina da parte della Russia già in corso da alcune settimane, sui giornali è stata diffusa la notizia dell'arresto di un'attivista russa all'uscita dalla metropolitana di Mosca, qualche settimana dopo aver rilanciato su *Twitter* una manifestazione contro la guerra organizzata in piazza Pushkinskaya. L'attivista sarebbe stata identificata grazie al sistema di riconoscimento facciale *Sphere*, installato sui mezzi pubblici della capitale russa[1].

Quasi negli stessi giorni, ancora più risalto è stato dato alla notizia che la società *Clearview AI* si sia offerta di aiutare il governo ucraino mettendo a disposizione i propri servizi per individuare infiltrati russi, riunire i rifugiati con le proprie famiglie e identificare le persone morte durante la guerra[2]. *Clearview AI* è una *startup* newyorchese che vende a imprese e agenzie di controllo pubbliche servizi di riconoscimento facciale basati su algoritmi allenati al riconoscimento a partire da un *database* di oltre dieci miliardi di immagini raccolte dai *social network* senza consenso delle persone interessate[3]. Le modalità di raccolta delle immagini e i servizi connessi, che sembrano permettere una profilazione e sorveglianza delle persone, hanno portato alcuni Stati a ritenere l'attività di *Clearview AI* contraria alla legge. Tra questi, come si avrà modo di vedere, c'è anche l'Italia[4].

Pochi mesi prima di questi eventi, *Apple* ha annunciato di aver migliorato il sistema di riconoscimento facciale installato sui modelli più recenti di *iphone*, permettendo di sbloccare il telefono con il proprio volto anche nel momento in cui si indossi una mascherina, a condizione che gli occhi siano ben visibili[5].

I tre esempi qui brevemente riportati consentono già di intuire in cosa consistano le tecnologie di riconoscimento facciale (TRF) e quali applicazione possano ricevere: si tratta di sistemi in grado di identificare o autenticare una persona a partire dalle caratteristiche del volto[6]. Si è quindi nel campo della raccolta di dati biometrici, che

---

[1] L. CARRER, *La Russia usa il riconoscimento facciale su chi manifesta contro la guerra*, 16 marzo 2022, in *www.wired.it*.

[2] K. CARBONI, *La più controversa startup di riconoscimento facciale sta collaborando con l'Ucraina*, 14 marzo 2022, in *www.wired.it*.

[3] L. ZORLONI, *Ho scoperto che la più discussa società di riconoscimento facciale al mondo ha le mie foto*, 23 marzo 2021, in *www.wired.it*.

[4] V. per ora il comunicato stampa del GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale: il Garante privacy sanziona Clearview AI per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani*, 9 marzo 2022, in *www.garanteprivacy.it*. Più ampiamente, *infra*, par. 5.

[5] *Ora è possibile sbloccare gli iPhone anche indossando la mascherina*, 15 marzo 2022, in *www.ilpost.it*.

[6] Nella dottrina giuridica interna, un lavoro monografico dedicato al tema è quello di G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, Napoli, 2021; v. anche, da un'angolazione processual-penalistica, E. SACCHETTO, Face to face*: il complesso rapporto tra* automated facial recognition technology *e processo penale*, in *www.lalegislazionepenale.it*, 16 ottobre 2020. Per una ricognizione della materia da una prospettiva penalistica, con specifico riguardo al contesto statunitense, cfr. New York City Bar, *Power, Pervasiness and Potential: the Brave New World of Facial Recognition Through a Criminal Law Lens (and beyond)*, agosto 2020, in

permettono di distinguere le persone in base a particolari attributi del corpo quali, ad esempio, le impronte digitali, la forma dell'iride o il DNA[7]. Nel caso delle TRF, tuttavia, il dato da ottenere e analizzare è particolarmente visibile e piuttosto facile da "raccogliere", sia nello spazio fisico sia in quello digitale[8].

Se, dal primo punto di vista, la messa a punto di tecnologie sempre più sofisticate punta a riconoscere un volto anche laddove sia parzialmente travisato, ad esempio con una mascherina, è nello spazio *online* che è possibile rinvenire, in maniera estremamente semplice, milioni quando non miliardi di immagini che ritraggono volti. Si pensi appunto ai *social network*, dove sono gli stessi utenti a caricare, volontariamente, le proprie foto, il più delle volte provvedendo anche a *taggarle* ossia a indicare a chi corrisponda un determinato volto, così contribuendo all'identificazione delle persone raffigurate.

Le TRF si presentano, dunque, come uno strumento dalle potenzialità applicative particolarmente ampie, sia dal punto di vista della diffusione potenzialmente capillare di strumenti di videosorveglianza diretti a "catturare" il volto delle persone sia delle numerose finalità a cui le stesse possono essere indirizzate, tanto di gestione della pubblica sicurezza quanto di natura prettamente commerciale[9]. Esse determinano un salto evolutivo significativo nella raccolta e gestione del dato biometrico, che lo rende suscettibile di molteplici utilizzi, come già risulta dagli esempi prima riportati, e che spaziano dall'impiego da parte della pubblica autorità per fini di controllo e sorveglianza oppure in contesti financo bellici alla messa in atto di strategie commerciali per aumentare la vendita di prodotti.

La natura anfibia di questi strumenti costituisce, dunque, un primo elemento degno di riflessione, che permette di illuminare il ruolo centrale giocato dalle imprese private nello sviluppo di tali tecnologie e nella vendita successiva alle amministrazioni governative e agenzie di controllo.

Infatti, si registra un apparente disallineamento tra la crescente diffusione delle TRF nell'ambito commerciale e qualche battuta d'arresto rintracciabile nel campo della gestione della sicurezza pubblica, dove, negli ultimi tempi, alcune tra le più grandi *tech company* hanno in parte smesso di fornire i propri prodotti alle forze dell'ordine per scopi di gestione dell'ordine pubblico. Questi comportamenti, visibili soprattutto nel contesto

---

http://documents.nycbar.org.s3.amazonaws.com/files/2020662-BiometricsWhitePaper.pdf.

[7] L'art. 4, n. 14) del Regolamento Generale sulla Protezione dei dati (GDPR) definisce i dati biometrici come «*i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*». Essi rientrano, dunque, nell'elenco delle particolari categorie di dati di cui all'art. 9 del medesimo Regolamento, il cui trattamento è pertanto sottoposto a un regime di maggior tutela, con la possibilità, espressamente prevista dal medesimo art. 9, per ciascuno Stato di prevedere ulteriori restrizioni a simili trattamenti proprio allorquando si tratti di dati biometrici.

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

[9] Per una ricognizione delle distinte finalità per cui possono essere utilizzate le TRF, v. T. HUANG - Z. XIONG - Z. ZHANGE, *Face Recognition Applications*, in S.Z. LI - A.K. JAIN (a cura di), *The Handbook of Face Recognition*, Springer, Cham, 2005, p. 617 ss.

statunitense, non derivano da un'intervenuta disciplina di settore volta a restringerne il campo applicativo, ma sono conseguenza di precise scelte di *business*, motivate dalla volontà d'impresa di dissociarsi da pratiche oggetto di forti critiche da parte dell'opinione pubblica. Non a caso, si tratta di un *trend* che riguarda principalmente gli attori più importanti attivi sul mercato, ma che non sembra coinvolgere, invece, le imprese più piccole[10]. Ad ogni modo, si è in presenza di un fenomeno che fornisce un punto di vista parzialmente inedito nell'analisi dei rapporti tra impresa e Stato, con la prima a richiedere al secondo un intervento legislativo in un settore caratterizzato da uno squilibrio delle conoscenze in tutto favore dei soggetti privati[11].

Al contempo, il tema delle TFR sollecita un approfondimento dal punto di vista penalistico, non soltanto in relazione ai rischi di violazione del diritto alla *privacy* e al corretto trattamento dei dati personali, ma anche, e soprattutto, in ragione della possibilità di attuare, dietro ragioni di tutela della pubblica sicurezza, forme di sorveglianza[12] di massa e di profilazione[13] delle persone, con una severa compressione dei diritti fondamentali e costituzionalmente garantiti della personalità nonché di riunione, associazione e libera manifestazione del pensiero[14]. A tal riguardo, da più parti si è messo in luce come l'installazione di TRF in spazi pubblici possa esplicare effetti di auto-censura da parte della popolazione, scoraggiata dall'esercitare tali fondamentali diritti (*chilling effect*)[15].

Dunque, l'idea di un potere pubblico in grado di esercitare un controllo pervasivo e costante delle persone, che consenta di tenere traccia del comportamento di ciascuno a partire dalle riprese effettuate dai sempre più diffusi sistemi di videosorveglianza, non sembra rappresentare la concretizzazione di un immaginario distopico o riconducibile alla sola realtà di Stati autoritari. Certamente, in ordinamenti in cui vi è un minore rispetto delle libertà personali, alcuni usi delle TRF spingono verso l'ulteriore compressione di diritti fondamentali: oltre all'esempio già fatto della Russia, si vedrà

---

[10] *Infra*, par. 4.

[11] Su come lo squilibrio di conoscenze in settori a elevata complessità tecnologica favorisca il diffondersi di fenomeni auto-normazione (più o meno regolata) d'impresa cfr. soprattutto G. FORTI, *Principio di precauzione e diritto penale*, in *Criminalia*, 2006, p. 196 ss., nonché C. PIERGALLINI, *Danno da prodotto e responsabilità penale. Profili dommatici e politico-criminali*, Giuffrè, Milano, 2004, p. 301 ss. Sul fenomeno dell'autonormazione, all'interno di una vasta bibliografia, v. da ultimo D. BIANCHI, *Autonormazione e diritto penale. Intersezioni, potenzialità, criticità*, Giappichelli, Torino, 2021.

[12] Da intendersi come la «*raccolta ed elaborazione di dati personali, identificabili o meno, allo scopo di influenzare o controllare coloro ai quali essi appartengono*»: così, D. LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002, p. 2. V. anche G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, Milano, 2015.

[13] Ai sensi dell'art. 4 del GPDR, per profilazione s'intende «*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*».

[14] G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 57 ss.

[15] Sul c.d. *chilling effect*, tra i contributi più recenti, v. F. VIGANÒ, *La proporzionalità della pena. Profili di diritto penale e costituzionale*, Torino, 2021, p. 277 ss.; N. RECCHIA, *Il principio di proporzionalità nel diritto penale*, Torino, 2020, 252 ss.

come in Cina il riconoscimento facciale contribuisca a perpetrare quello che è stato definito come il genocidio culturale della popolazione degli Uiguri, minoranza musulmana e turcofona che vive nel nord-ovest del paese[16].

Nondimeno, è opportuno inquadrare i rischi ingenerati dall'uso (e abuso) di simili tecnologie anche alle nostre latitudini, dove, ad esempio, le forze di polizia dispongono di un sistema di riconoscimento facciale la cui funzione "*real time*" – fino ad oggi non ancora utilizzata – è stata di recente ritenuta illegittima dal Garante per la protezione dei dati personali perché priva di un'adeguata base legale. Al riguardo, il Garante ha appunto stigmatizzato i rischi derivanti da una simile tecnologia, capace di attuare delle vere e proprie forme di sorveglianza di massa[17]. Non a caso, nelle più recenti proposte di regolamentazione della materia elaborate a livello di Unione Europea, le TFR sono incluse tra i sistemi di intelligenza artificiale ad alto rischio, il cui utilizzo va adeguatamente limitato o, in alcuni casi, addirittura bandito[18].

La particolare cautela con cui affrontare il tema deriva dalla capacità di queste tecnologie di ridisegnare il rapporto tra potere statuale e cittadini, tra autorità e libertà: un mutamento che passa anche da una nuova e diversa concezione dello spazio pubblico, inteso come luogo in cui ognuno è visibile e di conseguenza tracciabile. Spazio pubblico "fisico" che funge, a ben vedere, da specchio rovesciato del mondo *online*, dove è ancora più facile divenire oggetti di uno stretto monitoraggio, così rinsaldando il legame che avvince dimensione pubblica e privata dell'utilizzo delle TFR.

In quest'ottica, prima di procedere a un'analisi ravvicinata del fenomeno, appare opportuno compiere un passo indietro, per tentare di inquadrare la diffusione del riconoscimento facciale all'interno della società contemporanea.

2. Le TRF espressione del capitalismo della sorveglianza e della società del controllo.

Profilazione, controllo e sorveglianza costituiscono elementi caratteristici delle società attuali, rispetto alle quali la proliferazione delle TFR, supportata dal comportamento aggressivo di imprese dai fatturati paragonabili o superiori a quelli degli Stati più evoluti, sembra porsi in maniera perfettamente coerente. Come illustrato nel lavoro già classico di Shoshana Zuboff, l'ultima evoluzione del modello socio-politico del capitalismo avrebbe riconfigurato l'attività d'impresa in un senso "estrattivo" ossia rivolto in via prioritaria ad acquisire dati sul comportamento delle persone, per poi utilizzarli per scopi commerciali[19]. Non si tratta soltanto della possibilità di fare previsioni su gusti e comportamenti di un certo *target*, ma anche di sfruttare i dati

---

[16] V., ad es., M. CLARKE, *Framing the Xinjiang emergency: colonialism and settler colonialism as pathways to cultural genocide?*, in ID. (a cura di), *The Xinjiang emergency Exploring the causes and consequences of China's mass detention of Uyghurs*, p. 10 ss. Più ampiamente, *infra* par. 4.

[17] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema SARI real time*, 25 marzo 2021. Più in dettaglio, *infra*, par. 5.

[18] *Infra*, par. 6.

[19] Cfr. S. ZUBOFF, *The age of surveillance capitalism. The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York, 2019.

a disposizione per incidere, mediante meccanismi di condizionamento, sul comportamento effettivo delle persone, da orientare nel senso ritenuto più vantaggioso da un punto di vista economico[20].

La possibilità per le imprese di attingere a una mole vastissima di dati deriva dalla crescente digitalizzazione delle attività umane, favorita dalla diffusione di sistemi, a partire dagli *smartphone*, che consentono di individuare una "traccia" di ciò che si è compiuto. D'altronde, in letteratura si è efficacemente proposto di definire con il termine *onlife* la dimensione soltanto all'apparenza scissa che l'uomo contemporaneo vive, diviso tra la vita *online* e quella *offline*, che appunto si ritiene non possano più continuare a essere considerate in maniera separata[21].

Ebbene, gli effetti del capitalismo della sorveglianza non s'impongono soltanto nella strutturazione delle attività economiche, ma incidono in profondità anche nell'assetto delle relazioni sociali. Le potenzialità del controllo pervasivo a cui chiunque può essere sottoposto determinano, infatti, un mutamento nei comportamenti quotidiani, all'interno di quello che viene definito come un nuovo *panopticon* digitale, un sistema di controllo che opererebbe come una sorta di super-io collettivo in grado di condizionare "da remoto" i comportamenti individuali e indirizzarli in vista di una loro monetizzazione[22].

D'altronde, in letteratura si è segnalato come le metafore prese in prestito dall'immaginario distopico da "Grande fratello", solitamente adoperate per descrivere società connotate da una massiccia sorveglianza dei cittadini, risultino inadeguate a descrivere quella che, in altre e precedenti teorizzazioni, è stata inquadrata come società del controllo[23], quale forma che avrebbe sostituito le precedenti società disciplinari, entrate irrimediabilmente in crisi nel corso del Novecento[24].

Queste ultime erano caratterizzate dalla presenza di istituzioni per così dire "rigide", all'interno delle quali l'individuo era anzitutto contenuto fisicamente e quindi disciplinato, lungo un arco temporale potenzialmente capace di coprire una vita intera (famiglia scuola caserma fabbrica ospedale)[25]. Nella società del controllo si assiste,

---

[20] ID., spec. p. 65 ss.

[21] La felice espressione è stata coniata da L. FLORIDI, *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Springer, Cham, 2015.

[22] S. ZUBOFF, *The age of surveillance capitalism*, cit., p. 438, dove l'A. descrive la nuova realtà in cui gli individui sono immersi: «*a new phenomenon to live continuously in the milieu of the gaze of others, to be followed by hundreds or thousands of eyes, augmented by Big Other's devices, sensors, beams, and waves rendering, recording, analyzing, and actuating*».

[23] G. DELEUZE, *Les sociétés de contrôle* (1990), ora disponibile in *EcoRev'*, 1, 2018, p. 5 ss.

[24] Così, D. LYON, *La cultura della sorveglianza. Perché la società del controllo ci ha reso tutti controllori*, Luiss University Press, Roma, 2020, p. 19 ss. V. anche G. BALBI – P. DI SALVO, *Introduzione all'edizione italiana. La sorveglianza: un tema "classico" per capire il contemporaneo*, ivi, p. 9 ss.

[25] Sulle società disciplinari, imprescindibile il riferimento a M. FOCAULT, *Sorvegliare e punire. Nascita della prigione* (1975), Einaudi, Torino, 2014. Nella letteratura interna, altrettanto obbligatorio il rimando a M. PAVARINI - D. MELOSSI, *Carcere e fabbrica. Alle origini del sistema penitenziario* (1977), Il Mulino, Bologna, 2018. Sulla (successiva) perdita di centralità dell'istituzione carceraria e sull'esercizio di un controllo latamente penale all'interno e da parte dell'intera collettività, altrettanto doveroso è il riferimento a D. GARLAND, *La cultura del controllo. Crimine e ordine sociale nel mondo contemporaneo* (2001), Il Saggiatore, Milano, 2004.

invece, a una rarefazione e contestuale moltiplicazione degli strumenti – appunto – di controllo: «*i controlli sono una modulazione, come una modellatura auto-deformante, che si modifica continuamente, da un istante all'altro, o come un setaccio le cui maglie cambiano da un punto all'altro*»[26]. In un tale contesto, a occupare il campo non è più la fabbrica, ma l'impresa, che gestisce salari, premi e promozioni mediante meccanismi che stimolano la competitività tra le persone[27].

Proprio la constatazione del carattere maggiormente orizzontale del controllo, differente dalla "verticalità" con cui è esercitato il potere disciplinare, è valorizzata da chi pone in relazione l'affermarsi della società del controllo con il diffondersi di una cultura della sorveglianza generata dagli stessi utenti[28]. Al riguardo, sia sufficiente riprendere l'esempio dei *social network*, e della mole di informazioni che da essi possono essere ricavate, semplicemente "seguendo" una persona nella sua vita *online*[29].

Si ribalta, dunque, l'idea che concepisce un sorvegliante munito di poteri particolarmente penetranti e una moltitudine di sorvegliati: in un contesto iper-connesso, sono le stesse persone suscettibili di controllo a rendersi, a loro volta, solerti controllori. Da questa angolazione, la collettività è immersa all'interno di una vera e propria cultura della sorveglianza. Accanto a quella tradizionale, messa in campo, in maniera più o meno legittima, da agenzie di *intelligence*, governi e poteri digitali, si pone il comportamento dei singoli cittadini, che erige una simile attività a pratica quotidiana.

I concetti di capitalismo della sorveglianza, società del controllo e cultura della sorveglianza, ancorché diretti a inquadrare da angolazioni parzialmente diverse l'evoluzione degli assetti socio-economici delle società contemporanee, convergono, quindi, nel delineare uno scenario in cui la costante tracciabilità delle vite umane consente l'immagazzinamento di dati e al contempo diffonde forme di sorveglianza orizzontali[30]. La possibilità di ricorrere a tecnologie di riconoscimento facciale, che come tali consentono di identificare e tracciare le persone a partire dal proprio volto, si inserisce in maniera perfettamente congruente in un simile scenario, imprimendo una particolare curvatura alle pratiche estrattive tipiche del capitalismo della sorveglianza[31]. In questo campo, infatti, persino il volto umano è ridotto a un insieme di dati, da disaggregare e utilizzare per le finalità più disparate.

Per comprendere meglio questo elemento, è dunque opportuno esaminare con maggior grado di dettaglio il funzionamento di tali tecnologie.

---

[26] G. DELEUZE, *Les sociétés de contrôle*, cit., p. 7.

[27] *Ibidem*.

[28] D. LYON, *La cultura della sorveglianza*, cit., p. 25 ss.

[29] Per un catalogo delle «*pratiche della sorveglianza*», ivi, p. 59 ss.

[30] V. le considerazioni sviluppate ivi, p. 50 ss.

[31] Diversi esempi connessi all'utilizzo delle TRF sono illustrati già da S. ZUBOFF, *The age of surveillance capitalism*, cit., spec. p. 230 ss., all'interno del paragrafo dedicato all'estrapolazione dei dati direttamente dal corpo (*body rendition*).

3. Il funzionamento delle TRF: datificazione e classificazione degli individui.

In via di prima approssimazione, le TRF compiono un trattamento in modo automatizzato di immagini digitali che contengono il volto di una persona: ricorrendo a tecniche biometriche, ne sono ricavati i caratteri identificativi, riportati in forma di codici alfanumerici ed eventualmente arricchiti da indici ulteriori (*hashing*)[32].

Tale processo può essere utilizzato per finalità di autenticazione/verifica della persona, mediante l'abbinamento del volto dal vivo alla foto (ad esempio) presente su un documento di identità; di identificazione, tramite l'individuazione di una corrispondenza (*match*) tra la fotografia e quelle già raccolte e contenute in un *database*; infine, di rilevazione ossia di individuazione dei volti, come può accadere utilizzando i filmati realizzati da telecamere a circuito chiuso, da confrontare con le foto presenti in un *database* alla ricerca di una corrispondenza.

Le TRF permettono che la ricerca del *match*, indicato per il tramite di un indice percentuale, avvenga in maniera particolarmente rapida e in relazione a centinaia di migliaia di foto. Questa potrà essere realizzata sia in modalità "da remoto" sia "in tempo reale": nel primo caso, si tratta appunto di ricercare una corrispondenza tra l'immagine acquisita e quelle già presenti nel *database*; nel secondo, le TRF permetteranno di operare un confronto tra una moltitudine di volti, catturati in tempo reale, e quelli già presenti a catalogo. Uno degli esempi più classici è rappresentato dalla ricerca di un soggetto ritenuto pericoloso all'interno di una folla facendo ricorso a videocamere di sorveglianza puntate su aree pubbliche.

È tale ultima modalità a destare le maggiori perplessità, in quanto comporta, in linea potenziale, una sorveglianza di massa, in assenza di qualunque forma di consenso da parte delle persone oggetto del trattamento. Nel prosieguo si vedrà come le proposte di regolamentazione mirino a limitare fortemente la possibilità di ricorrere a tali forme di riconoscimento facciale, privilegiandosi quelle che operano *ex post*[33].

Ad ogni modo, in tutti i casi è operata una categorizzazione delle persone, a prescindere dall'identità delle stesse, semplicemente isolando le caratteristiche tipiche del volto del soggetto ritratto[34]. Tale operazione è realizzata grazie al ricorso a strumenti di apprendimento automatico, tipici di sistemi che vengono definiti di intelligenza artificiale. Il riconoscimento facciale pertiene, quindi, a un sotto-campo dell'IA, quello della visione artificiale, che si occupa appunto di insegnare alle macchine a rilevare e interpretare le immagini. Come segnalato in letteratura, si tratta di un ambito particolarmente problematico, stante la natura relazionale e spesso inafferrabile delle immagini[35].

---

[32] Illustra in dettaglio il funzionamento delle TFR, G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 32 ss. V. anche J. BUOLAMWINI – V. ORDÓÑEZ – J. MORGENSTERN – E. LEARNED-MILLER, *Facial recognition technologies: a primer*, Algorithmic Justice League, 29 maggio 2020, disponibile in *https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf*.

[33] *Infra*, parr. 5 e 6.

[34] La c.d. «*indifferenza formale*» verso gli utenti caratterizza, a ben vedere, il capitalismo della sorveglianza in sé e le pratiche che gli sono tipiche: cfr. S. ZUBOFF, *The age of surveillance capitalism*, cit., p. 353 ss.

[35] K. CRAWFORD, *Né intelligente né artificiale. Il lato oscuro dell'IA*, Il Mulino, Bologna, 2021, p. 119 ss.

Pertanto, al fine di istruire la macchina alla comprensione di ciò che "vede", si parte dalla raccolta di un campione quanto più esteso possibile di immagini, opportunamente catalogate ed etichettate. Come noto, nel vasto settore del c.d. *deep learning*, il processo di apprendimento e miglioramento continuo delle macchine avviene mediante delle tecniche di correlazione induttiva e inferenza probabilistica basate sulla frequenza statistica con cui si replicano determinati schemi nel campione. Non vi è, dunque, un'effettiva comprensione degli stessi, quanto, appunto, un progressivo raffinamento delle capacità di individuare correlazioni interne a ciò che viene processato[36].

Così, nel campo delle TRF, una volta che alla macchina sono state presentate le immagini entra in gioco un algoritmo (*learner*) che guida l'apprendimento a partire dai dati etichettati e che, a sua volta, informa un ulteriore algoritmo (*classifier*) sulle modalità con cui individuare le relazioni tra i nuovi *input* e gli *output* attesi. Il miglioramento costante di un simile sistema è dunque strettamente dipendente dalla mole dei dati analizzati e dal grado di precisione con cui sono stati etichettati. Una volta messi a punto *set* di dati stabilizzati per lo sviluppo della visione artificiale, questi fungono da base di partenza per il perfezionamento dei diversi sistemi, a seconda degli obiettivi di volta in volta prefissati[37].

I sistemi di riconoscimento facciale necessitano, allora, di poter attingere a un catalogo quanto più ampio e variegato possibile di immagini, capace di alimentare e istruire macchine voraci e all'apparenza insaziabili. Da ciò ne discende, da un canto, la raccolta "selvaggia" del materiale disponibile in rete, compiuta nell'assenza sostanziale del consenso da parte delle persone coinvolte, e, dall'altro, il ricorso a *database* già esistenti e concepiti per altri utilizzi, come ad esempio accaduto con le raccolte di foto segnaletiche a disposizione delle autorità di pubblica sicurezza. Ne discendono problematiche connesse non soltanto al rispetto del diritto alla *privacy* delle persone le cui foto sono state utilizzate per allenare i sistemi di riconoscimento facciale, ma anche in termini di affidabilità dei sistemi, dipendenti dalla varietà dei dati e dalla correttezza dell'etichettamento[38].

A tal riguardo, da più parti si sono evidenziati i *racial bias* dei sistemi di riconoscimento facciale, meno allenati a riconoscere persone di determinati generi o colori della pelle[39], e, di volta in volta, le aziende coinvolte hanno cercato di rimediare ampliando la tipologia di dati a cui fanno ricorso[40]. Nondimeno, in letteratura si è

---

[36] V. ad es. S. QUINTARELLI (a cura di), *Intelligenza artificiale. Cos'è davvero, come funziona, che effetti avrà*, Bollati Boringhieri, Milano, 2020; M. CHIRIATTI, *Incoscienza artificiale. Come fanno le macchine a prevedere per noi*, Luiss University Press, Roma, 2021.

[37] K. CRAWFORD, *Né intelligente né artificiale*, cit., p. 111 ss.

[38] Ivi, spec. p. 141 ss.

[39] Cfr., ad es., I. IVANOVA, *Why face-recognition technology has a bias problem*, in *www.cbsnews.com*, 12 giugno 2020; A. NAJIBI, *Racial Discrimination in Face Recognition Technology*, in *https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/*, 24 ottobre 2020. V. anche *Coded Bias*, documentario del 2020 che indaga, appunto, i pregiudizi e le discriminazioni realizzate dagli algoritmi, in particolar modo nei sistemi di riconoscimento facciale.

[40] V., ad es., J. ROACH, *Microsoft improves facial recognition technology to perform well across all skin tones, genders*,

criticato questo *modus operandi*, diretto a correggere problematiche ritenute al contrario insite nei sistemi di intelligenza artificiale e discendenti in maniera diretta dall'attività di classificazione che è alla base del processo di apprendimento delle macchine: «*Le pratiche di classificazione danno forma al modo in cui l'intelligenza artificiale viene classificata e prodotta* (…) *tutto ciò che esiste al mondo viene convertito in dati attraverso l'estrazione, la misurazione, l'etichettatura e l'ordinamento, e questo diventa, intenzionalmente o meno, una scivolosa evidenza empirica per i sistemi tecnologici addestrati su questi dati*»[41].

Ne risulta che le TFR sembrano realizzare al massimo grado il processo di "datificazione" dell'individuo, ridotto a mero dato numerico; al medesimo tempo, si contribuisce alla costruzione di generi e razze in base alle quali distinguere artificialmente il genere umano. In letteratura si sollecita dunque a interrogarsi su chi compia una siffatta catalogazione e su quali basi[42]: una questione che diviene ancor più pressante allorché si pretenda di classificare le persone a partire dalle caratteristiche del proprio volto e che chiama in causa le imprese private impegnate nello sviluppo dei sistemi di intelligenza artificiale.

4. I rapporti tra Stato e imprese nell'utilizzo delle TRF. L'esempio cinese: il ruolo ausiliario nella persecuzione della popolazione degli Uiguri.

Una volta osservata la non neutralità alla base del funzionamento delle TRF, e più in generale dei sistemi di IA, strettamente dipendente dalle modalità di classificazione dei dati a partire dai quali le macchine "imparano", ai fini delle presenti riflessioni appare opportuno concentrarsi, altresì, sul ruolo – anfibio e ambiguo – occupato dall'impresa nella diffusione di tali strumenti presso le forze di pubblica sicurezza[43].

Un ruolo che muta, evidentemente, al variare del contesto osservato, a seconda della natura più meno autoritaria dello Stato di riferimento, ma che in ogni caso conferma come le *big tech* di fatto forniscano la tecnologia necessaria a forme di sorveglianza di massa, quando non sono esse stesse a promuovere il ricorso a simili strumenti, soprattutto laddove si muovano in ambiti scarsamente disciplinati e al riparo dall'attenzione mediatica. Al contrario, qualora esigenze reputazionali lo suggeriscano, sono le medesime imprese a prendere le distanze dagli utilizzi controversi delle TRF, in alcuni casi anche mediante l'interruzione dei rapporti commerciali con Stati e agenzie federali.

La Cina sembra offrire un chiaro esempio di brutale utilizzo dell'IA e delle TFR per scopi di sorveglianza e profilazione di massa. Se l'ambizione a divenire *leader*

---

26 giugno 2018, articolo apparso sul sito della società *Microsoft*, nonché R. PURI, *Mitigating Bias in AI Models*, 6 febbraio 2018, articolo apparso sul sito della società *IBM*.

[41] K. CRAWFORD, *Né intelligente né artificiale*, cit., p. 144.

[42] Ivi, p. 164 ss.

[43] Così D. LYON, *La cultura della sorveglianza*, p. 50: «*La sorveglianza è anche una grande industria. Le* corporation *globali vi prendono parte e spesso hanno stretti legami con il governo*».

mondiale nel settore ha determinato una diffusione di queste tecnologie all'interno di città sempre più connesse e "*smart*", nella regione dello Xinjiang, dove risiede la popolazione degli Uiguri, sembra si stia compiendo un vero e proprio esperimento totalitario[44].

Agli strumenti tradizionali di controllo sociale si affiancano, infatti, quelli più tecnologici, al fine di ottenere una sorveglianza a tappeto e permanente di tale minoranza etnico-religiosa, giustificata dal governo cinese per ragioni di contrasto al terrorismo. La raccolta dei dati degli Uiguri è associata all'elaborazione di modelli predittivi – rischio criminale compreso – rivelando in maniera plastica come l'installazione di telecamere e la diffusione di *app* di controllo sociale si presti a declinazioni liberticide nei rapporti tra autorità e cittadini. Le nuove tecnologie, incluse quelle di riconoscimento facciale, sono utilizzate nell'ambito di una politica di "rieducazione" promossa dal partito comunista e che comprende anche forme di detenzione di massa[45].

I tentativi di portare all'attenzione della Corte Penale Internazionale tali pratiche, così da avviare un'indagine, non sono andati a buon fine: nel dicembre 2021, l'Ufficio del Procuratore ha ritenuto che non vi fossero le basi giuridiche per procedere per genocidio e crimini di guerra, in quanto i fatti sarebbero avvenuti prevalentemente nel territorio della Repubblica popolare cinese, che non ha mai aderito allo Statuto di Roma[46].

Invece, si è assistito al proliferare di sanzioni di natura economica, promosse in primo luogo dagli Stati Uniti e indirizzate anche verso le imprese multinazionali cinesi accusate di contribuire alle pratiche di individuazione e confinamento della popolazione uigura. In particolare, i primi *ban* sono stati emanati durante il mandato presidenziale di Donald Trump, inserendosi all'interno di una più generale politica di accesa competizione commerciale con la Cina[47]. Nondimeno, anche nel corso della presidenza di Joe Biden si è proseguito lungo la medesima direttrice, e lo scorso dicembre è stato approvato il c.d. *Uyghur Forced Labor Prevention Act*, che prevede, tra le altre cose, il divieto di importazione dei prodotti dalla regione dello Xinjiang, a meno che le imprese

---

[44] Cfr. S. PIERANNI, *Red Mirror. Il nostri futuro si scrive in Cina*, Laterza, Roma, 2020, p. 52 ss. Ma v. anche le risoluzioni del Parlamento europeo del 17 dicembre 2020 sul lavoro forzato e la situazione degli uiguri nella regione autonoma uigura dello Xinjiang, del 19 dicembre 2019 sulla situazione degli uiguri in Cina ("*China Cables*"), del 18 aprile 2019 sulla Cina, in particolare la situazione delle minoranze religiose ed etniche, e del 4 ottobre 2018 sulla detenzione di massa arbitraria di uiguri e kazaki nella regione autonoma uigura dello Xinjiang.

[45] Si legga il recente *report* di HUMAN RIGHTS WATCH, *"Break Their Lineage, Break Their Roots". China's Crimes against Humanity Targeting Uyghurs and Other Turkic Muslims*, 19 aprile 2021, disponibile in *www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots/chinas-crimes-against-humanity-targeting#_ftn109*.

[46] G. PANE, *Il popolo abbandonato degli Uiguri: il Prosecutor della CPI chiude le indagini contro la Cina*, in *www.iusinitinere.it*, 28 settembre 2021. Per il comunicato della Corte, v. THE OFFICE OF THE PROSECUTOR - INTERNATIONAL CRIMINAL COURT, *Report on Preliminary Examination Activities 2020*, 14 dicembre 2020, par. 70 ss., in *www.icc-cpi.int/sites/default/files/itemsDocuments/2020-PE/2020-pe-report-eng.pdf*.

[47] Cfr. A. NISSEN, *Import Bans on Products from Forced Labor in the Trump Era*, in *Un. Bologna L. Rev.*, 2020, p. 367 ss.

non dimostrino, in maniera "chiara" e "convincente" di essere estranee a pratiche di sfruttamento del lavoro[48].

Inoltre, sempre nel dicembre 2021, alcune imprese cinesi, accusate di contribuire alla sorveglianza biometrica e al tracciamento della popolazione uigura, sono state inserite in una delle *blacklist* messe a punto dell'*Office of Foreign Assets Control* (OFAC) presso il Dipartimento del Tesoro statunitense. La competenza di tale ufficio si radica a partire dalla valuta usata nelle transazioni, il dollaro, e ad essa di riconnette il potere di vietare rapporti commerciali in dollari con Stati, individui e gruppi di persone ritenuti una minaccia alla sicurezza, alla politica estera o all'economia nazionale[49].

Anche l'Unione Europa ha reagito: sulla base della Decisione 2020/1999 del Consiglio del 7 dicembre 2020, sono state applicate misure restrittive a quattro alti ufficiali cinesi nella regione dello Xinjiang per le violazioni dei diritti umani sulla minoranza musulmana degli uiguri[50].

Oltre alle sanzioni economiche, è opportuno prendere in considerazione anche l'effetto reputazionale delle accuse mosse alle imprese di essere coinvolte in tali pratiche: una vasta eco mediatica hanno avuto le notizie che riguardavano società cinesi come *Alibaba* e *Huawei*, "giganti" del settore: la prima, tra le più importanti multinazionali nel campo dell'*e-commerce*, è stata accusata di aver messo a punto un *software* in grado, a partire da filmati o fotografie caricati dagli utenti, di individuare e segnalare persone appartenenti alla minoranza uigura[51]. La seconda, attiva nel settore delle telecomunicazioni e già destinataria di una serie di *ban* dovuti ad accuse di spionaggio, si ritiene fornisca alla polizia cinese un sistema di *scan* facciale capace di individuare una persona di etnia uigura e, eventualmente, di inviare un *alert*[52]. In entrambi i casi, le aziende si sono difese dichiarando che si tratta di sistemi soltanto testati in via di prova e non destinati ad utilizzi che possano contribuire a pratiche discriminatorie e dannose per i diritti umani[53].

---

[48] Per una ricognizione a prima lettura, v., ad es., GIBSON DUNN, *The Uyghur Forced Labor Prevention Act Goes Into Effect in the United States*, 14 gennaio 2022, in *www.gibsondunn.com/the-uyghur-forced-labor-prevention-act-goes-into-effect-in-the-united-states/*.

[49] Dal sito dell'OFAC: *https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20211216*. Sul tema, v., ad es., V. ORTBLAD, *Criminal Prosecution in Sheep's Clothing: The Punitive Effects of OFAC Freezing Sanctions*, in 98 *J. Crim. L. and Criminology*, 2008, p. 1439 ss. Nella letteratura interna, particolare attenzione all'attività dell'OFAC, anche in relazione alle regole di *compliance* d'impresa, è prestata da S. MANACORDA, *The "Dilemma" of Criminal Compliance for Multinational Enterprises in a Fragmented Legal World*, in S. MANACORDA – F. CENTONZE (a cura di), *Corporate Compliance on a Global Scale. Legitimacy and Effectiveness*, Springer, Cham, 2022, p. 67 ss.

[50] Cfr. *Council implementing Regulation (EU) 2021/478 of 22 March 2021 implementing Regulation (EU) 2020/1998 concerning restrictive measures against serious human rights violations and abuses*, disponibile in *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2021:099I:FULL&from=EN*.

[51] H. DAVIDSON, *Alibaba offered clients facial recognition to identify Uighur people, report reveals*, 20 dicembre 2020, in *www.theguardian.com*.

[52] V. NI, *Documents link Huawei to Uyghur surveillance projects, report claims*, 15 dicembre 2021, in *www.theguardian.com*.

[53] V. *Statement from Alibaba Group Regarding Recent Reports of the Company's Facial Recognition Technology*, 16 dicembre 2020, in *www.alizila.com/statement-from-alibaba-group-regarding-recent-reports-of-the-companys-facial-recognition-technology/*; le dichiarazioni da parte di Huawei sono riportate da E. DOU, *Documents link Huawei*

In un contesto autoritario come quello cinese, dunque, sembrano trovare attuazione particolari modelli di sorveglianza totale, con le imprese attive nel settore che rivestono un ruolo ausiliare, consistente nella messa a disposizione di tecnologie idonee alla realizzazione di simili politiche. Al medesimo tempo, l'utilizzo di tali tecnologie su scala così vasta ne contribuisce al miglioramento, atteso che, come già osservato, quanto maggiore è la mole di dati processati dai sistemi di IA tanto più rapida e precisa ne sarà l'evoluzione[54].

5. L'esempio statunitense: il ruolo "attivo" delle big tech e l'accusa di contribuire al razzismo endemico della polizia locale.

Nel volgere lo sguardo, invece, a una democrazia liberale come quella statunitense, il ruolo delle imprese nel contribuire alla diffusione di strumenti di controllo e sorveglianza presso le forze di polizia appare maggiormente riconducibile all'incontro tra gli interessi commerciali delle prime e gli obiettivi di gestione dell'ordine pubblico delle seconde. In altre parole, nel vuoto normativo che caratterizza il settore, l'utilizzo o meno di simili strumenti sembra rimesso, in buona parte, alle scelte dei singoli uffici e alle eventuali sinergie che vengono a instaurarsi con le *corporation* che li producono.

Così, *Rekognition*, il sistema di riconoscimento facciale messo a punto da *Amazon*, è stato al centro di progetti-pilota sviluppati in alcune città, tra cui, ad esempio, Orlando[55]. In questo caso, il progetto è terminato in virtù del fatto che la città non disponesse della tecnologia adeguata al funzionamento del sistema in modalità *real time*[56]. Già prima dell'interruzione della sperimentazione, però, numerose associazioni di attivisti, ma anche impiegati e *shareholder* di *Amazon*, avevano protestato contro i rischi derivanti dal suo utilizzo, proteste rimaste tuttavia inascoltate dall'impresa[57].

Soltanto qualche tempo dopo, invece, la società ha deciso di vietare, prima per un anno e poi anche per quello successivo, la vendita di *Rekognition* alle forze di polizia, anticipando di qualche mese le società *IBM* e *Microsoft*. Il deciso cambio di rotta da parte di *Amazon* e di altre tra le più importanti *tech company* al mondo è da ascriversi al moto di reazioni e proteste che in tutti gli Stati Uniti sono seguite alla morte di George Floyd, uomo nero di 46 anni morto a causa della tecnica di immobilizzazione c.d. *knee on neck* alla quale è stato sottoposto nel corso di un arresto da parte di Dereck Chauvin, ufficiale

---

to China's surveillance programs, 14 dicembre 2021, in *www.washingtonpost.com*.

[54] Lo sottolinea S. PIERANNI, *Red Mirror*, cit., p. 55.

[55] D. ALBA, *With No Laws To Guide It, Here's How Orlando Is Using Amazon's Facial Recognition Technology*, 30 ottobre 2018, in *www.buzzfeed.com*.

[56] N. STATT, *Orlando police once again ditch Amazon's facial recognition software*, 18 luglio 2019, in *www.theverge.com*.

[57] J. VINCENT, *AI researchers tell Amazon to stop selling 'flawed' facial recognition to the police*, 3 aprile 2019, in *www.theverge.com*; ID., *Amazon employees protest sale of facial recognition software to police*, 22 giugno 2018, ivi; C. LECHER, *Shareholders are pushing Amazon to stop selling its facial recognition tool*, 17 gennaio 2019, ivi.

di polizia bianco[58].

Nell'ambito delle critiche al razzismo strutturale che caratterizza la società statunitense e che si rifletterebbe in maniera vistosa nelle attività degli apparati di polizia[59], alle *big tech* si è contestato di fornire strumenti di controllo e sorveglianza massiva, a loro volta viziati da *racial* (e *gender*) *bias*, con le TFR più allenate a identificare uomini bianchi. La necessità di prendere le distanze dalle attività della polizia ha dunque portato le multinazionali in questione a rivedere le proprie politiche aziendali in materia e a interrompere i contratti in essere, in attesa di una disciplina legislativa sul tema.

La soluzione più radicale è quella adottata da *IBM*: nel giugno 2020, il CEO ha dichiarato che la società non avrebbe più sviluppato, compiuto ricerche e venduto TRF per scopi di *law enforcement*. Al medesimo tempo, con una lettera indirizzata al Congresso degli Stati Uniti, ha sollecitato a disciplinare la materia, ponendo in risalto l'estrema opacità alla base dei rapporti tra le agenzie di controllo e le imprese impegnate nella vendita di tali tecnologie nonché, soprattutto, i rischi di «*mass surveillance, racial profiling, violations of basic human rights and freedoms*»[60]. *Microsoft*, invece, analogamente ad *Amazon*, ha temporaneamente interrotto le sue attività nei confronti degli organi dello Stato, in attesa di un'espressa disciplina del settore[61].

Le scelte delle *corporation* di interrompere la fornitura di sistemi di riconoscimento facciale appaiono quindi dettate, almeno in primo luogo, da esigenze reputazionali[62]. In una fase storica connotata da profonde tensioni e divisioni in senso alla società statunitense, i rischi per i colossi tecnologici di essere percepiti dai consumatori come fornitori di sistemi in grado di perpetuare forme di discriminazione e razzismo da parte degli agenti di polizia è stato considerato evidentemente troppo alto. In tal senso, il comune richiamo a una regolamentazione pubblica della materia è espressione evidente della necessità di poter aderire a un insieme codificato di regole a cui attenersi, di modo da poter agire nella legalità e, soprattutto, di poter dichiarare di farlo. Sebbene già fossero noti i pericoli discendenti dall'utilizzo delle TRF, è stata l'esplosione della questione razziale a rivelarsi determinante nello spingere le imprese a rimeditare le proprie scelte di *business*.

Negli Stati Uniti, all'iniziale opacità nella diffusione del riconoscimento facciale

---

[58] R. CORNELLI, *Note sulla* Police brutality *a partire dai fatti di Minneapolis*, *in Riv. trim. dir. pen. cont.*, n. 2/2020, p. 1 ss.

[59] Esalta il fattore razziale nelle pratiche violente della polizia statunitense, R. CORNELLI, *La forza di polizia. Uno studio criminologico sulla violenza*, Giappichelli, Torino, 2020, p. 25 ss. Mette in luce la natura sistematica dell'addestramento alla violenza a cui sono formati gli agenti di polizia negli Stati Uniti, E. GRANDE, *La condanna di Derek Chauvin per la morte di George Floyd: giustizia è fatta?*, 14 maggio 2021, in *www.questionegiustizia.it*.

[60] Il testo della lettera è disponibile in: *www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/*.

[61] A. LEVY, *Microsoft says it won't sell facial recognition software to police until there's a national law 'grounded in human rights'*, 11 giugno 2020, in *www.cnbc.com*; K. WEISE – N. SINGER, *Amazon Pauses Police Use of Its Facial Recognition Software*, 10 giugno 2020, in *www.nytimes.com*.

[62] Sull'importanza della dimensione reputazionale nell'esercizio dell'attività d'impresa, e sui costi derivanti da una "*bad reputation*", v. il numero speciale della rivista *Buss.&Soc.*, num. 6, 2019, intitolato appunto *Corporate Reputation: Being Good and Looking Good*, e in particolare D. BREITINGER-J.P. BONARDI, *Firms, Breach of Norms, and Reputation Damage*, p. 1143 ss.

tra forze di polizia è quindi seguita una fase di sovraesposizione mediatica che ha inquadrato criticamente la questione, spingendo i *competitor* più in vista a uscire dal mercato. Tutto ciò, comunque, non ha ancora portato a una regolamentazione a livello federale. Così, permane il rischio che, a fronte della scelta delle maggiori società di dissociarsi da pratiche commerciali malviste dai consumatori, siano aziende più piccole ad occupare il campo e soddisfare la domanda[63].

6. Uno sguardo all'Italia: le pronunce del Garante per la privacy nei casi SARI e Clearview AI.

Nel contesto italiano, o meglio europeo, sebbene allo stato non via sia ancora una regolamentazione in materia di riconoscimento facciale, deve registrarsi un crescente interesse per la questione. Ne è significativo testimone la Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'uso dell'IA nel diritto penale, in cui, tra le altre cose, si chiede alla Commissione «*una moratoria sulla diffusione dei sistemi di riconoscimento facciale per le attività di contrasto con funzione di identificazione*»[64], almeno finché non vi sia la garanzia che tali tecnologie siano conformi ai diritti fondamentali e immuni da pregiudizi discriminatori, e sussista un quadro giuridico tale da evitarne un uso distorto e improprio. Nel medesimo testo si esprime, inoltre, profonda preoccupazione «*per l'utilizzo di database privati di riconoscimento facciale da parte delle autorità di contrasto e dei servizi di intelligence, come* Clearview AI*, una banca dati di oltre tre miliardi di immagini raccolte illegalmente dai social network e da altre fonti Internet*»[65].

A seguito di tale Risoluzione, l'Italia ha effettivamente approvato una moratoria dei sistemi biometrici di riconoscimento facciale in luoghi pubblici o aperti al pubblico fino alla fine del 2023, ad eccezione, tuttavia, dei trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati, o anche di esecuzione di sanzioni penali ai sensi del d.lgs. 51/2018. Una soluzione temporanea, in attesa dell'approvazione del Regolamento sulla c.d. legge sull'intelligenza artificiale[66].

Si delinea, quindi, uno scenario in rapido mutamento, in cui la recente attenzione di legislatore e opinione pubblica costituisce un elemento di novità. A differenza degli Stati Uniti, infatti, dove l'assenza di leggi federali favorisce l'attività di imprese multinazionali nell'incidere e direzionare le scelte dell'autorità nelle modalità di gestione di ordine e sicurezza pubblici, grazie anche a dei programmi pilota con cui testare e migliorare tali strumenti, nello scenario europeo si registra una maggiore volontà di regolamentare la materia. Ciononostante, vi sono casi significativi di utilizzo delle TRF tutt'altro che scevri da problematiche.

Guardando all'Italia, sin dal 2017 il Ministero dell'Interno dispone del *Sistema*

---

[63] J. HOROWITZ, *Tech companies are still helping police scan your face*, 3 luglio 2020, in *www.edition.cnn.com*.

[64] *Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI))*, par. 27.

[65] Ivi, par. 28.

[66] V. artt. a 9 a 12, lg. n. 3374/2021, di conversione del d.l. n. 139/2021.

Automatico di Riconoscimento Immagini (SARI). Quest'ultimo, ad oggi, è utilizzato nella sola funzione da remoto, denominata *Enterprise*, che consente l'identificazione di un soggetto ignoto a partire da un'immagine fotografica. In particolare, mediante «*una ricerca computerizzata nella banca dati AFIS, e grazie a due algoritmi di riconoscimento facciale,* [SARI Enterprise] *è in grado di fornire un elenco di immagini ordinato secondo un grado di similarità*»[67]. A sua volta, la banca dati AFIS (*Automated Fingerprint Identification System*) rappresenta il sistema automatizzato di acquisizione delle impronte digitali, di cui fa parte il *Sotto Sistema Anagrafico* (Ssa), che contiene, invece, le foto segnaletiche presenti nei *database* della polizia, insieme alle informazioni fisiche delle persone ritratte.

SARI *Enterprise* è venuto alla pubblica ribalta nel settembre 2018, quando il suo utilizzo ha consentito l'identificazione e l'arresto di due persone di origine georgiana accusate di aver compiuto un furto in un'abitazione qualche mese prima: grazie alle immagini riprese dalle videocamere di sorveglianza, il sistema ha potuto individuare una corrispondenza tra i milioni di immagini presenti nel *database*[68]. In tale occasione, la Polizia di Stato ha comunicato che la fase di sperimentazione era terminata e che SARI rappresentava un importante ausilio nel contrasto alla criminalità[69].

Se, dunque, in precedenza era necessario immettere manualmente i tratti caratterizzanti il volto della persona ricercata per sperare di ottenere dal sistema qualche corrispondenza, con SARI questa operazione è automatizzata. Proprio perché rappresenta una semplice sofisticazione nel trattamento delle immagini, appena qualche mese prima dell'identificazione delle persone accusate di furto in abitazione il Garante per la protezione dei dati personali aveva dato il via libera a SARI *Enterprise*. Nel relativo provvedimento si era osservato, infatti, che tale funzione rappresenta «*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*»[70].

Diametralmente opposta è stata, invece, la decisione del medesimo Garante sulla modalità *real time* di SARI, intervenuta soltanto di recente, a causa, come svelato da un'inchiesta giornalistica, delle resistenze opposte dal Ministero dell'Interno alla richiesta di fornire una valutazione d'impatto sulla *privacy* dei cittadini (DPIA), come noto necessaria allorché il trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone interessate[71]. L'istruttoria, aperta nel 2017, è arrivata soltanto nel 2021 a conclusione. Nel frattempo, il Ministero dell'Interno aveva pubblicato un bando

---

[67] Così si può leggere sul sito del Ministero dell'Interno, *www.interno.gov.it*. Sul tema, in letteratura, v. R. LOPEZ, *La rappresentazione facciale tramite* software, in A. SCALFATI (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2019, 239 ss.

[68] V., ad es., *Brescia: ladri d'appartamento identificati con il riconoscimento facciale*, 7 settembre 2018, in *www.repubblica.it*.

[69] *Ecco Sari, il nuovo software di riconoscimento facciale della polizia*, 7 settembre 2018, in *www.skytg24.it*.

[70] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell'identità di un volto*, provvedimento n. 440 del 26 luglio 2018.

[71] R. COLUCCINI, *Lo scontro Viminale-Garante sul riconoscimento facciale*, in *IRPImedia*, 13 gennaio 2020, disponibile in *https://drive.google.com/file/d/1oGPsVzM-TH6JQu0hNX7F8VsLBAIN-7bE/view*.

per potenziare ulteriormente la funzione *real time* di SARI, in modo da utilizzarlo come «*sistema tattico per monitorare le operazioni di sbarco e tutte le varie tipologie di attività illegali correlate, video riprenderle ed identificare i soggetti coinvolti*»[72]: nuovamente, il riconoscimento facciale sembra indirizzarsi a detrimento di particolari fasce deboli della popolazione, in questo caso le persone migranti[73].

Come accennato, tuttavia, nel marzo 2021 il Garante ha espresso parere non favorevole all'utilizzo di SARI *real time*, in quanto non sussiste una base legale adeguata per tale attività. La pronuncia in questione illustra chiaramente i rischi derivanti dal ricorso a forme di riconoscimento facciale in tempo reale, che «*realizza un trattamento automatizzato su larga scala che può riguardare, tra l'altro, anche coloro che siano presenti a manifestazioni politiche e sociali, che non sono oggetto di "attenzione" da parte delle forze di Polizia*»[74], potendo determinare «*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*»[75].

A fondamento della propria decisione, il Garante pone la constatazione che quelli oggetto di trattamento rappresentano categorie particolari di dati ai sensi dell'art. 9 RGPD, in quanto «*dati biometrici intesi a identificare in modo univoco una persona fisica*»[76], nonché, in virtù del potenziale utilizzo nell'ambito di manifestazioni pubbliche, di dati idonei a rivelare le opinioni politiche o l'appartenenza sindacale. Pertanto, il loro trattamento è sottoposto alle condizioni più stringenti dettate dall'art. 7 d.lgs. n. 51/2018, tra cui quella di dovere essere «*specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento*»[77].

Al riguardo, è interessante sottolineare come il Garante non consideri una base legale adeguata il decreto di attuazione del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per finalità di polizia, da organi, uffici e comandi di polizia. Sebbene sia qui prevista una specifica disciplina per il trattamento dei dati raccolti mediante sistemi di videosorveglianza e di ripresa fotografica, audio e video, a parere del Garante si tratta di «*sistemi ontologicamente diversi da quelli dei dati biometrici*»[78].

Infine, come accennato in apertura di lavoro, il Garante per la protezione dei dati personali si è anche occupato di *Clearview AI*, società che offre alle autorità pubbliche un

---

[72] Ivi, p. 2.

[73] V. il report di HERMES – CENTRO PER LA TRASPARENZA E I DIRITTI UMANI DIGITALI, *Tecnologie per il controllo delle frontiere in Italia. Identificazione, riconoscimento facciale e finanziamenti europei*, 2020, disponibile in *https://s3.documentcloud.org/documents/21128523/tecnologie-per-il-controllo-delle-frontiere-in-italia-identificazione-riconoscimento-facciale-e-finanziamenti-europei.pdf*.

[74] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, provvedimento n. 127 del 25 marzo 202.

[75] *Ibidem*. Per un commento ai provvedimenti del Garante, cfr. anche G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 240 ss.

[76] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, cit., par. 2) delle osservazioni.

[77] *Ibidem*.

[78] *Ibidem*.

servizio di ricerca e trattamento mediante TRF delle immagini sul *web* liberamente accessibili. Il procedimento, nato a seguito di notizie stampa che denunciavano le criticità nella gestione dei dati da parte di *Clearview AI*, e a quattro reclami di persone che avevano scoperto che la società deteneva diverse immagini che le raffiguravano senza che avessero prestato consenso, ha fatto chiarezza sull'attività svolta, ritenendola in contrasto con le disposizioni del GDPR relative ai principi che devono caratterizzare il trattamento dei dati (di correttezza e trasparenza, di limitazione delle finalità e di limitazione della conservazione), alle condizioni di liceità del trattamento in generale e a quelle previste per particolari tipologie di dati sensibili, nonché con riguardo al rispetto dei diritti dell'interessato. Pertanto, è stata ordinata l'applicazione della sanzione amministrativa pecuniaria nel limite edittale massimo di venti milioni di euro[79].

La decisione del Garante si rivela di particolare interesse perché illustra in modo plastico le pratiche di sorveglianza e profilazione permesse dalle TRF a partire dal materiale accessibile *online*. Mediante tecniche di *web scraping* – normalmente vietate dai gestori dei siti, in particolare di *social network* – la società raccoglie foto pubblicamente accessibili da siti o video disponibili in rete, per poi elaborarle con tecniche biometriche. Una volta indicizzate, queste possono essere arricchite con i metadati disponibili associati all'immagine (ad es. la pagina *web* da cui è stata presa, la data di nascita della persona ritratta, la nazionalità, la lingua parlata ecc.), che saranno trasmesse una volta trovata la corrispondenza.

Da tutto ciò il Garante ne ricava che l'attività svolta non consiste, come dichiarato dalla società *Clearview*, nella mera classificazione di individui sulla base di caratteristiche note, ma nella gestione di dati biometrici che consente un tracciamento nel tempo delle persone ad essi associate[80].

7. Prime indicazioni dalla Proposta di Regolamento della Commissione Europea e qualche considerazione conclusiva.

La ricognizione compiuta sinora ha mostrato come il campo delle TRF sia stato interessato, nel corso degli ultimi anni, da un dibattito sempre più ampio, dove stanno trovando spazio e riconoscimento le voci più critiche e preoccupate circa la diffusione di tali strumenti per finalità di gestione della pubblica sicurezza, specialmente in assenza di una disciplina che regoli chiaramente la materia.

Nel caso specifico dell'Italia, le pronunce del Garante per la protezione dei dati

---

[79] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di* Clearview AI, provvedimento n. 50 del 10 febbraio 2022.

[80] *Ibidem*: «*Le informazioni in questione formano oggetto di archiviazione nel database di* Clearview *e vengono arricchite nel tempo con altre estratte da nuovi* template *idonei a riflettere anche i cambiamenti fisici avuti dallo stesso soggetto, come emerge dall'esame di alcuni dei reclami proposti all'Autorità* (…). *Ne discende che* Clearview *non offre come risultato della ricerca una semplice corrispondenza, ma anche un archivio di risorse che si snoda attraverso il tempo. La valutazione di tale circostanza, unitamente alla finalità comparativa sopra evidenziata, è idonea ad integrare, come richiesto nel Considerando 24, un'attività assimilabile al controllo del comportamento dell'interessato in quanto posta in essere tramite il tracciamento in internet e la successiva profilazione*».

personali hanno censurato alcune forme di utilizzo delle TRF capaci di aprire la strada a forme di sorveglianza di massa e profilazione nel tempo delle persone, ribadendo con forza la necessità di una legge sul tema. Il Parlamento italiano ha approvato una moratoria sulla possibilità di usare sistemi di videosorveglianza dotati di riconoscimento facciale in luoghi pubblici – sebbene con l'eccezione, tra le altre, dell'ipotesi in cui il trattamento sia effettuato dalle autorità competenti a fini di prevenzione e repressione dei reati – in ciò allineandosi all'indicazione contenuta nella Risoluzione del Parlamento europeo sulla richiesta alla Commissione di bandire tali tecnologie, quantomeno in attesa di un intervento legislativo che ne assicuri l'uso in maniera compatibile al rispetto dei diritti fondamentali.

Al riguardo, sono rinvenibili diversi esempi di linee guida, ove le condizioni per l'utilizzo del riconoscimento facciale sono più o meno stringenti anche a seconda dell'organismo che le ha elaborate[81]. Al contempo, alcune iniziative promosse da associazioni a tutela dei diritti digitali e fondamentali delle persone mirano a sensibilizzare l'opinione pubblica affinché siffatte tecnologie vengano messe al bando[82]. Le motivazioni sono molteplici e spaziano dall'inaffidabilità alla circostanza per cui i costi, in termini di compressione dei diritti e di mutamento nella relazione tra autorità e libertà, sono di gran lunga maggiore dei benefici.

In un tale scenario, la proposta di Regolamento in materia di intelligenza artificiale[83], il primo tentativo compiuto nel contesto europeo di disciplinare in maniera organica l'IA, costituisce un parametro di riferimento particolarmente importante, anche alla luce dell'intensa attività preparatoria che lo ha preceduto, condensata in numerosi atti di impulso e strumenti di *soft law*[84]. Nell'ambizione di disciplinare l'utilizzo dell'IA

---

[81] Ad es., se nel documento elaborato dal UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS, *Report. The right to privacy in the digital age*, 13 settembre 2021, par. 45, si condivide la proposta già avanzata dal Parlamento Europeo di una moratoria sull'uso di quei sistemi in grado di compromettere diritti fondamentali, come accade con il riconoscimento facciale, almeno fino a quando non sia provato che tali rischi siano stati neutralizzati, il recente *white paper* intitolato *A Policy Framework for Responsible Limits on Facial Recognitio Use Case: Law Enforcement Investigations* e messo a punto nell'ambito del *World Economic Forum* con la partecipazione di Interpol e UNICRI, contiene significative aperture all'utilizzo delle TRF. Particolarmente rilevanti, altresì, sono le linee guida elaborate dal COMITATO CONSULTIVO 108 istituito presso il Consiglio d'Europa, dal titolo *Guidelines on Facial Recognition*, del 28 gennaio 2021.

[82] V. soprattutto la campagna "*Reclaim your face*", un'Iniziativa dei Cittadini Europei (ECI) – strumento di partecipazione diretta che consente di proporre alla Commissione europea l'approvazione di nuove leggi – con cui si chiede «*di vietare, nel diritto e nella pratica, gli usi indiscriminati o tendenziosi della biometria che possono sconfinare in attività di sorveglianza di massa illecita*». In Italia, la campagna è promossa dal Centro Hermes per la Trasparenza e i Diritti umani digitali.

[83] *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale*, 21 aprile 2021.

[84] V. ad es. le due risoluzioni del Parlamento europeo sui principi etici dell'IA, della robotica e della tecnologia correlata, nonché sul regime di responsabilità civile per l'IA, entrambi del 20 ottobre 2020,e la risoluzione sull'uso dell'IA del 20 gennaio 2021, nonché il Libro Bianco sull'Intelligenza artificiale della Commissione, del 19 febbraio 2020. In dottrina, cfr. L. PARONA, *Prospettive europee e internazionali di regolazione dell'intelligenza artificiale tra principi etici,* soft law *e* self regulation, in *Riv. regolaz. mercati*, n. 1/2020, p. 70 ss.

mediante un «*approccio equilibrato*»[85], che sia consapevole che «*gli stessi elementi e le stesse tecniche che alimentano i benefici socio-economici dell'IA possono altresì comportare nuovi rischi o conseguenze negative per le persone fisiche o la società*»[86], la proposta di Regolamento qualifica alcuni usi dell'IA come vietati o ad alto rischio, in questo secondo caso prevedendo delle particolari condizioni di utilizzo che siano in grado di attenuarlo[87].

Ebbene, il tema dell'identificazione biometrica riceve ampia considerazione, proprio in virtù dei potenziali rischi per i diritti fondamentali che ne possono discendere. Coerentemente alle modalità con cui tali sistemi possono operare, si distingue tra l'identificazione biometrica in tempo reale e da remoto: la prima, in spazi pubblici e per attività di contrasto, è vietata in quanto ritenuta particolarmente invasiva dei diritti e delle libertà delle persone interessate «*nella misura in cui potrebbe avere ripercussioni sulla vita privata di un'ampia fetta della popolazione, farla sentire costantemente sotto sorveglianza e scoraggiare in maniera indiretta l'esercizio della libertà di riunione e di altri diritti fondamentali*»[88].

Nondimeno, si prevedono delle significative eccezioni a una simile messa al bando, allorché questi sistemi si rendano necessari per la ricerca di potenziali vittime di reato, compresi i minori scomparsi, la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone o di un attacco terroristico, nonché il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o di una persona sospettata di un reato per cui può essere spiccato un mandato d'arresto europeo, allorché tale reato sia punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni[89].

Anche qualora si versi in una delle descritte situazioni, ai fini del trattamento dei dati dovrà tenersi conto della natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno causato dal mancato uso del sistema, e le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze. L'uso dovrà essere subordinato a un provvedimento motivato dell'autorità giudiziaria o amministrativa dello Stato membro, ad eccezione dei casi in cui ragioni di urgenza non autorizzino a procedere immediatamente, rimandando la richiesta di autorizzazione a una fase successiva[90].

---

[85] *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale*, cit., Relazione, cap. 1, Contesto della proposta.

[86] *Ibidem*.

[87] Per una ricognizione del contenuto della proposta, cfr. C. CASONATO – B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw J.*, n. 1/2021, p. 1 ss.

[88] *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale*, cit., considerando n. 18). La disciplina è contenuta al Titolo II – Pratiche di Intelligenza Artificiale vietate, art. 5.

[89] *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale*, cit., Titolo II, art. 5, lett. d).

[90] *Ibidem*.

Invece, per quel che concerne i sistemi di identificazione biometrica da remoto, questi sono inquadrati tra i sistemi di IA ad alto rischio[91]. Concordemente, il loro utilizzo deve rispettare una serie di condizioni, tra cui l'attuazione, per tutto il ciclo di vita del sistema, di un meccanismo di *risk-management* volto a individuare e minimizzare i rischi prevedibili prima della messa in commercio o emersi durante l'utilizzo, a cui si accompagnano contestuali obblighi di informazione al pubblico e di *testing* costante dei sistemi, nonché il rispetto di standard qualitativi dei dati che fungono da base per l'addestramento dei sistemi ad alto rischio al fine di contenere errori e discriminazioni. Un aspetto, quest'ultimo, particolarmente rilevante in relazione alle tecnologie di riconoscimento facciale, come visto sovente affette da pregiudizi di genere o legati al colore della pelle delle persone[92]. Inoltre, si richiede che il sistema sia «*sufficientemente trasparente*», così da permettere di comprendere come funzioni il meccanismo di apprendimento della macchina, e che assicuri un'efficace supervisione umana. Infine, tali sistemi dovranno sottostare a una procedura di verifica di conformità a standard e regole stabilite dall'Unione, che potrà essere effettuata dal produttore stesso o da un organismo certificatore terzo[93].

Come si evince da questa pur rapida ricognizione della proposta di Regolamento, il tema del riconoscimento facciale, e più in generale dell'identificazione biometrica, è inquadrato in termini problematici, alla luce delle potenziali ricadute negative sui diritti fondamentali. Se nella modalità da remoto si prevede una serie di condizioni che consente di vigilare sul concreto utilizzo delle TFR e, di riflesso, sulle sue finalità, la consapevolezza circa la possibilità di realizzare forme di sorveglianza di massa attraverso la modalità in tempo reale spinge verso la scelta, ben più radicale, del divieto.

Nondimeno, è facile accorgersi come le eccezioni a siffatto divieto siano suscettibili di ricevere un'applicazione estensiva. Non solo l'elenco eterogeneo dei reati per i quali è prevista la possibilità di ricorrere a un mandato d'arresto europeo, ma il riferimento a situazioni di emergenza o di attacchi terroristici, da un canto, e alle attività di ricerca di vittime, compresi minori scomparsi, dall'altro, sembra inquadrare scenari emergenziali rispetto ai quali appare lecito ricorrere anche ai mezzi più controversi per conseguire lo scopo prefissato.

Visti da un'angolazione penalistica, le condizioni dettate dalla proposta per derogare al divieto riguardano ambiti e obiettivi politico-criminali – il contrasto al terrorismo specialmente, ma anche, in parte, la tutela delle vittime – che hanno legittimato profonde trasformazioni del diritto penale[94]. Nel caso delle TRF, il richiamo

---

[91] Ivi, Allegato III - Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2.

[92] *Supra*, par. 3.

[93] Ivi, Titolo III - Sistemi di IA ad alto rischio, artt. 8 ss. Per un commento delle condizioni richieste dalla Proposta per i sistemi di IA ad alto rischio, v. C. CASONATO – B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, cit., p. 13 ss.

[94] Si tratta di una bibliografia vastissima: v., ad es., M. DONINI, *Diritto penale di lotta vs. diritto penale del nemico*, in A. GAMBERINI - R. ORLANDI (a cura di), *Delitto politico e diritto penale del nemico*, Monduzzi, Bologna, 2007, 131 ss.; invece, sugli aspetti in chiaroscuro sul sistema di garanzie penalistiche discendenti dalla diffusione del c.d. paradigma vittimario, cfr. tra i tanti C. ELIACHEFF – S. LARIVIÈRE, *Il tempo delle vittime. Come le vittime sono diventate i nuovi eroi della società democratica contemporanea* (2007), Ponte alle grazie, Firenze, 2008, nonché,

a scenari emergenziali per giustificarne l'uso anche in *real time* ripropone nuovamente uno schema collaudato di rinuncia parziale a determinate garanzie per finalità di pubblica sicurezza[95].

Tuttavia, come si è osservato nel corso della presente trattazione, la diffusione di tali tecnologie in siffatte modalità rischia di trasformare in maniera irreversibile il rapporto tra potere e cittadini. Le ulteriori condizioni dettate dalla proposta, inerenti alla verifica della gravità della situazione e alla previa autorizzazione dell'autorità (nel caso in cui ragioni d'urgenza non consentano di richiederla in seguito) non sembrano poter contenere il rischio di città puntellate di telecamere di videosorveglianza munite di TRF, che seppure "silenti" – in quanto utilizzabili solo al verificarsi di un'emergenza – molto probabilmente eserciterebbero un effetto dissuasivo nell'esercizio di diritti fondamentali dei cittadini.

Come già accennato, alcune associazioni attive nel campo della tutela dei diritti fondamentali e dei diritti digitali si battono perché il riconoscimento facciale venga messo al bando, senza eccezioni. In questo senso va la recente proposta di emendamenti al Regolamento, presentata il 31 marzo 2022, che prevede, tra le altre cose, il divieto assoluto di ricorrere alle tecniche di identificazione biometrica in tempo reale[96].

In ogni caso, anche laddove il Regolamento sia approvato nell'attuale conformazione, ciascuno Stato membro sarà libero di limitare ulteriormente l'uso delle TRF[97]. A quel punto, sarà necessario un dibattito pubblico partecipato e consapevole, che metta in chiara luce rischi e benefici derivanti da tali tecnologie, e che sia dunque capace di orientare le scelte del legislatore.

---

per un lavoro di taglio monografico, M. VENTUROLI, *La vittima nel sistema penale. Dall'oblio al protagonismo?*, Jovene, Napoli, 2015.

[95] V. il sempre attuale lavoro di S. MOCCIA, *La perenne emergenza. Tendenze autoritarie nel sistema penale*, II[a] ed., ESI, Napoli, 2000.

[96] La proposta di emendamenti è disponibile in: *www.europarl.europa.eu/doceo/document/ITRE-AM-719802_IT.pdf*.

[97] *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale*, cit., art. 5, par. 4.