La regolamentazione delle tecnologie di riconoscimento facciale nell'UE e negli USA: *alea IActa est*?

di Alberto Orlando

Abstract: *The regulation of facial recognition technologies in the EU and the USA*: alea IActa est? - This paper compares the first regulatory approaches of the European Union and the United States regarding facial recognition technologies. The European Union is adding a new regulation to the regulation coming from the GDPR and the Law Enforcement Directive with the introduction of the AI Act, which, among other things, also deals with "biometric identification". In the United States, regulation at the federal level continues to be lacking, while regulatory attempts at the state level are increasing. The contribution reflects on the consequences of this regulatory divergence by examining the different uses of facial recognition technologies in the public and private sectors.

Keywords: Facial recognition; Biometric identification; AI Act; AI policy; GDPR

1. Utilizzi e peculiarità delle TRF: "cosa" regolare

Le tecnologie di riconoscimento facciale (di seguito, TRF) sono tra le applicazioni tecnologiche in più rapida diffusione, con utilizzi molto diversi per obiettivi, intensità, incidenza e rischi connessi [1]. La riflessione sulla loro regolamentazione presenta profili problematici che sono comuni alla regolamentazione delle nuove tecnologie e, in particolare, alla regolamentazione tanto discussa della Intelligenza artificiale (di seguito, IA)[2]. Il presente lavoro, più che indagare sul corretto bilanciamento di diritti

[1] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021; D. Lyon, *La cultura della sorveglianza. Come la società del controllo ci ha reso tutti controllori*, Roma, 2020; S.Z. Li, A.K. Jain (a cura di), *The Handbook of Face Recognition*, New York, 2011; K.A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*, New York, 2011; M. Mann, M. Smith, *Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight*, in *University of New South Wales Law Journal*, 40, 1, 2017, 121 ss.

[2] Esse pongono il regolatore di fronte al c.d. dilemma di Colingridge, ossia alla impossibilità di prevedere le conseguenze derivanti dallo sviluppo delle tecnologie, e al c.d. *pacing problem*, ossia all'incapacità del diritto di tenere il passo dello sviluppo tecnologico. Cfr. A. Genus, A. Stirling, *Collingridge and the dilemma of control: Towards responsible and accountable innovation*, in *Research policy*, 47, 1, 2018, 61-69; G.E. Marchant, *Addressing the pacing problem*, in Id., B.R. Allenby, J.R. Herkert (a cura di), *The growing gap between emerging technologies and legal-ethical oversight: The pacing problem*, New York, 2011, 199-205; F. De Vanna, *Diritto e nuove tecnologie: il nodo (controverso) della regolazione giuridica*, in *Lo Stato*, 11, 2018, 387 ss; M.D. Fenwick, W.A.

DPCE online
ISSN: 2037-6677

e interessi in gioco, mira ad approfondire i primi approcci con cui le istituzioni dell'UE e statunitensi stanno scegliendo di affrontare queste nuove sfide.

Con riferimento alle TRF, in primo luogo, il regolatore si trova a dover chiarire "cosa" regolare, almeno in un duplice senso: da una parte, occorre definire chiaramente la categoria; dall'altra, bisogna interrogarsi sulla necessità di distinguere, all'interno della categoria stessa, differenti discipline a seconda delle tipologie e degli utilizzi.

In linea generale, le TRF si basano su complessi procedimenti algoritmici automatizzati che consentono di identificare una persona a partire dall'immagine del suo volto, incrociando l'immagine ripresa in fotografia o in video con altre immagini, presenti in database, con le quali la stessa persona era stata identificata precedentemente[3]. Si tratta di una particolare applicazione della più ampia categoria delle tecnologie biometriche, le quali consentono di identificare una persona sulla base di caratteristiche fisiche uniche, come ad es. le impronte digitali. Un primo dubbio a fini regolatori riguarda quindi la scelta che porta o meno a distinguere tra TRF e altre tecnologie biometriche, per quanto le prime risultino evidentemente peculiari per una serie di aspetti, come la più semplice acquisizione (anche a causa della difficoltà di nascondere il volto), il più basso costo e la minore invasività rispetto ad altre tecnologie biometriche (si pensi alle impronte digitali), condizione – quest'ultima – che astrattamente consente la raccolta dell'immagine all'insaputa del soggetto.

È innegabile che l'utilizzo di TRF si sostanzi in un trattamento di dati personali. A questo riguardo, il regolatore si confronta con un quadro normativo che, per quanto bisognoso di costante aggiornamento, è comunque già esistente e consolidato, almeno nelle esperienze oggetto di questo lavoro[4]. Pertanto, anche in questo caso occorrerà verificare se possano essere trovate soluzioni accettabili già *de iure condito* o, se invece, si renda necessario un aggiornamento della disciplina[5].

D'altro canto, TRF e IA condividono un quadro problematico non soltanto "simile" ma anche "sovrapponibile", nella misura in cui la maggior parte delle TRF si basa sull'applicazione di *software* che possiamo ricondurre a quelle "tecniche e approcci" che l'UE considera propri dell'IA[6]. Ancora, il regolatore dovrà operare una scelta: se disciplinare interamente le TRF "per mezzo" di una eventuale regolamentazione dell'IA, se "ritagliare" uno spazio

Kaal, E.P. Vermeulen, *Regulation Tomorrow: What Happens When Technology is Faster Than the Law?*, in *Amer. Univ. Bus. Law Rev.*, 6, 3, 2017, 591 ss.

[3] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., 11.

[4] Cfr. A. Di Martino, *Profili costituzionali della privacy in Europa e negli Stati Uniti*, Napoli, 2017. Per gli USA, cfr. L. Determann, *Adequacy of data protection in the USA: myths and facts*, in *International Data Privacy Law*, 6, 3, 2016, 245 ss.

[5] Cfr. I.S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, in *International Data Privacy Law*, 3, 2, 2013, 74 ss.; - I. Berle, *Face Recognition Technology. Compulsory Visibility and its Impact on Privacy and the Confidentiality of Personal Identifiable Images*, Cham, 2020.

[6] Cfr. Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione (di seguito, *AI Act*), 21 aprile 2021, COM(2021) 206 final, allegato 1.

specifico alle TRF nell'ambito di questa regolamentazione o se considerare i fenomeni distintamente, optando per forme e modalità regolatorie (o, se del caso, non regolatorie) differenti[7].

Infine, dovendo immaginare una disciplina delle TRF, non si può certamente trascurare la varietà di impieghi in settori e per finalità profondamente diversi. Senza pretesa di esaustività e con l'obiettivo di fornire delle coordinate utili, possiamo valorizzare la distinzione tra impieghi in ambito pubblico e in ambito privato. In ambito pubblico, le TRF sono spesso sfruttate dalle forze dell'ordine, ad esempio, a fini di prevenzione e repressione dei reati attraverso l'identificazione di sospetti e persone scomparse, oppure per garantire la sicurezza in zone sensibili come frontiere e aeroporti o durante eventi con grande affluenza di pubblico, ma altri utilizzi nel settore medico o dell'istruzione sono in rapida crescita[8]. Quanto più si osservano esperienze maggiormente lontane dai valori delle liberaldemocrazie, si incontrano iniziative politiche che utilizzano apertamente le TRF per l'erogazione di sussidi, benefici e sovvenzioni[9], per la profilazione delle persone e per l'assegnazione di un "punteggio"[10], o addirittura per l'identificazione di oppositori politici o appartenenti a minoranze etniche o religiose[11].

D'altro canto, le TRF sono in rapida diffusione anche nel contesto privato, dove vengono utilizzate sia a scopi di sicurezza, sia a scopi commerciali e di monitoraggio della performance lavorativa, sia ancora per rendere più "smart" procedure e ambienti[12].

Pertanto, il regolatore pubblico che reputi di dover disciplinare le TRF dovrebbe interrogarsi? sul giusto peso da riconoscere al settore di impiego e allo specifico utilizzo delle TRF, tenendo presente che a questi fattori non può che essere legata una differente valutazione del rapporto tra rischi e benefici.

2. Il "pacchetto protezione dati" dell'UE alla prova delle TRF

In ambito UE non esiste una normativa specifica per le TRF. Tuttavia, è innegabile come molti dei profili relativi all'utilizzo di queste tecnologie possano trovare una regolamentazione nel vigente quadro normativo europeo, nel quale intanto trova esplicito riconoscimento il diritto alla protezione dei dati personali (art. 8 Carta dei diritti fondamentali dell'UE e

[7] Cfr. G. Mobilio, *L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica*, in *BioLaw Journal*, 2, 2020, 401-424.
[8] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., 17.
[9] Sul caso dell'*Aadhaar project* in India, cfr. G. Formici, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in *DPCE online*, 2, 2019, 1113 ss.
[10] Sul noto caso del *social scoring* cinese, cfr. G. Sciascia, *Reputazione e potere. Il social scoring tra distopia e realtà*, in *Giorn. dir. amm.*, 3, 2021, 317-325.
[11] Cfr., sempre in relazione alla Cina, Human Rights Council, *Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, David Kaye, A/HRC/41/35, 28 maggio 2019.
[12] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., 18-19.

DPCE online
ISSN: 2037-6677

art. 16 TFUE) e dal 2016 opera il c.d. "pacchetto protezione dati", che ricomprende il GDPR[13] e la Direttiva *Law Enforcement* (di seguito, LED)[14].

Con riferimento al nostro tema, il GDPR ha il merito di fornire una definizione di "dati biometrici", intesi come "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"[15]. Questi dati sono assoggettati all'intera disciplina sui dati personali, basata, come noto, sui principi di liceità e trasparenza del trattamento, limitazione delle finalità, minimizzazione ed esattezza dei dati, limitazione della conservazione[16].

Ma soprattutto, i dati biometrici rientrano nella categoria dei "dati sensibili" di cui all'art. 9 GDPR, il cui trattamento risulta vietato a meno che non ricorrano alcune condizioni alternative, tra cui, *inter alia*, il consenso esplicito dell'interessato, il carattere "manifestamente pubblico" dei dati o motivi di interesse pubblico rilevanti sulla base del diritto dell'UE o degli Stati membri[17]. Ai sensi del paragrafo 4, questi ultimi possono poi prevedere ulteriori condizioni per il trattamento dei dati biometrici.

Con riferimento alla LED e al suo ambito di applicazione, è confermata la definizione di "dati biometrici"[18] e anche il loro inquadramento nelle "categorie particolari di dati personali"[19], il cui trattamento è autorizzato, "solo se strettamente necessario" e purché "soggetto a garanzie adeguate per i diritti e le libertà dell'interessato" in casi espressamente stabiliti: se consentito dal diritto dell'UE o degli Stati membri, se necessario per la salvaguardia di un interesse vitale di persona fisica, se riguardante dati manifestamente pubblici. A differenza del GDPR, nella LED il consenso non costituisce la base per il trattamento[20].

Su quest'ultimo profilo, in realtà, occorre notare che, con riferimento alle TRF – ma il discorso può essere esteso a molti impieghi dell'IA – esistono argomenti per contestare la validità del consenso come strumento

[13] Regolamento (UE) 2016/679, "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE". Cfr. L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017.

[14] Direttiva (UE) 2016/680 del 27 aprile 2016, "relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati". In dottrina, cfr. M.M. Caruana, *The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement*, in *Int. Rev. Law, Comp. & Techn.*, *33*, *3*, 2017, 249 ss.

[15] GDPR, art. 4, n. 14.

[16] GDPR, art. 5.

[17] Cfr. G. Druetta, *9. Trattamento di categorie particolari di dati personali*, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2018, 93 ss.

[18] LED, art. 3, n. 13.

[19] LED, art. 10.

[20] Cfr. LED, Considerando 35 e 37.

a salvaguardia dei diritti dell'interessato[21]. Innanzitutto, è dubbio che il consenso esplicito dell'interessato attesti la consapevole accettazione dei rischi correlati al trattamento, poiché, dato il carattere ubiquitario e pervasivo delle TRF, il rilascio del consenso potrebbe regredire a livello di automatismo. Tale problema si pone in misura maggiore per le TRF "passive" (come l'ingresso in una zona videosorvegliata), in cui la raccolta dei dati in qualche modo prescinde dalla percezione dell'interessato, ma riguarda anche le TRF "interattive", in cui comunque la complessità dell'informativa o la specificità della situazione possono svuotare di significato il meccanismo del *notice and consent*. In particolare, una informativa dalla quale l'interessato possa evincere chiaramente finalità e modalità di trattamento appare sempre più improbabile davanti a sistemi basati su tecniche di *machine learning* altamente sofisticate: in questi casi, infatti, il problema della *explainability* potrebbe riguardare non solo l'interessato, ma qualsiasi soggetto, compresi i più "qualificati", come creatori/programmatori/addestratori[22].

Per quanto si compiano sforzi importanti per garantire la *explainability* dei sistemi di IA[23], i dubbi sulla effettività del consenso non risultano del tutto fugati[24]. D'altro canto, pur ammettendo la consapevolezza dell'interessato, il meccanismo del consenso per l'utilizzo di TRF in alcuni ambienti rischia di porlo in una posizione di debolezza, dalla quale questi può uscire solo acconsentendo al trattamento: si pensi al lavoratore subordinato cui venga domandato di acconsentire all'utilizzo di TRF nei suoi confronti per finalità che possono variare dalla più accettabile tutela della sicurezza negli ambienti lavorativi, fino alla registrazione dell'orario di lavoro e più in generale alla valutazione della performance[25].

Inoltre, occorre interrogarsi sulla corretta interpretazione della norma che sia nel GDPR che nella LED consente il trattamento di dati sensibili – compresi quelli biometrici – nel caso in cui questi siano "manifestamente pubblici". Se è acclarato – anche a livello giurisprudenziale[26] – che questa disposizione debba essere intesa nel senso che "l'interessato abbia volontariamente rinunciato alla protezione speciale per i dati sensibili rendendoli disponibili al pubblico, autorità comprese"[27], permangono

[21] Cfr. C. Casonato, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Dir. pub. comp. eur.*, Speciale, 2019, 106-108.
[22] Cfr., *ex multis*, F. Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge (MA), 2015. Sui profili tecnologici dell'IA, cfr. M.C. Carrozza et al., *AI: profili tecnologici. Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'Intelligenza Artificiale*, in *BioLaw Journal*, 3, 2019, 237 ss.
[23] Cfr. A. Barriedo Arrieta e al., *Explainable artificial intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI*, in *arxiv.org*, 2019, 1-72.
[24] Cfr. E. Spiller, *Il diritto di comprendere, il dovere di spiegare.* Explainability *e intelligenza artificiale costituzionalmente orientate*, in *BioLaw Journal*, 2, 2021, 419-432.
[25] Con riferimento ad un caso che ha riguardato l'utilizzo di TRF in ambiente scolastico, cfr. F. Paolucci, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *Medialaws*, 1, 2021, 215.
[26] Corte EDU, *P.G. and J.H. v. the United Kingdom*, 25 settembre 2001, par. 56; Corte EDU, *Peck v. The United Kingdom*, 28 gennaio 2003, par. 59.
[27] Gruppo Di Lavoro "Articolo 29", *Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, WP 258, 29 novembre 2017, 10.

DPCE online
ISSN: 2037-6677

comunque dubbi applicativi: da una parte, trovarsi in un luogo pubblico – ad es. passeggiare per strada – non può legittimare di per sé la raccolta e il trattamento dei dati; dall'altra, però, anche i dati "resi pubblici" dallo stesso interessato sui *social network*, o in generale sul *web*, dovrebbero godere di adeguata protezione e potrebbero essere considerati "manifestamente pubblici" – quindi, oggetto di trattamento – solo nel caso in cui si riuscisse a dedurre, dall'aver reso pubblici determinati dati, una rinuncia alla protezione[28].

Una sicura rilevanza in materia deve poi essere riconosciuta alle disposizioni sul trattamento automatizzato dei dati personali: per quanto plausibile che le TRF richiedano sempre un intervento umano, il ruolo della sorveglianza umana merita di essere analizzato alla luce del dettato normativo di cui all'art. 22 GDPR, il quale, come noto, introduce il c.d. principio di non esclusività dei trattamenti automatizzati[29]. Tuttavia, tale diritto può essere sacrificato quando l'interessato esprime consenso esplicito o se il trattamento è autorizzato dal diritto dell'UE o nazionale[30]. Nel caso di rilascio del consenso, il compito di assicurare l'adeguatezza del trattamento spetta al titolare dello stesso, il quale deve garantire all'interessato "almeno" un ulteriore diritto, ossia quello "di ottenere l'intervento umano"[31]. Come si può notare le disposizioni non solo non escludono del tutto il trattamento interamente automatizzato, ma lasciano aperti alcuni profili problematici.

Innanzitutto, occorre capire quali decisioni possano essere ricomprese tra quelle incidenti "significativamente" sulla persona dell'interessato. In secondo luogo, le eccezioni previste ricoprono un'area vastissima: in particolare, agli Stati membri è concesso di prevedere ipotesi di legittimità del trattamento unicamente automatizzato senza che sia necessario garantire il diritto all'intervento umano. In terzo luogo, si può discutere sul significato da accordare all'avverbio "unicamente": un'interpretazione restrittiva porterebbe infatti ad escludere l'applicabilità dell'art. 22 in tutte le situazioni in cui possa ravvisarsi un minimo intervento umano, anche se sul punto sembra prevalere l'orientamento per cui l'intervento umano dovrebbe comunque assumere contorni significativi[32]. Pur non potendo approfondire in questa sede la riflessione sulla portata dell'art. 22 GDPR, il riconoscimento di un *right to explanation* astrattamente applicabile anche alle TRF appare quantomeno dubbio[33].

[28] Cfr. A.G. Masotti, *Il caso Facebook e la tutela dei dati personali: una partita ancora aperta*, in *DPCE online*, 1, 2024, 605 ss.
[29] Art. 22 GDPR: "L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona".
[30] Art. 22, par. 2, GDPR.
[31] Art. 22, par. 3, GDPR.
[32] Cfr. Gruppo di Lavoro "Articolo 29", *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 6 febbraio 2018, 23.
[33] Tale convinzione trovava sicuramente maggiore forza nelle precedenti versioni del GDPR, mai approvate, in cui si statuiva che la profilazione – intorno a cui, come *species* più rilevante in materia di trattamento automatizzato, la norma era costruita – non poteva basarsi "unicamente o in modo predominante" sul trattamento automatizzato e

In definitiva, il quadro normativo attualmente vigente a livello UE, pur non riferito direttamente alle TRF, fissa principi di base che orientano l'impiego di queste tecnologie verso un utilizzo "responsabile". Tuttavia, alcune difficoltà applicative appaiono decisamente non trascurabili: anche per questo motivo, le stesse Istituzioni dell'UE hanno presto cominciato a ragionare su una regolamentazione specifica del fenomeno, quantomeno nell'ambito della generale riflessione sulla regolamentazione dell'IA.

3. Il "rinforzo" dell'AI Act

Non è infatti un caso che fin dalle prime fasi del percorso unionale[34] che dovrebbe portare, ormai a breve, all'adozione di un Regolamento sull'IA (*AI Act*)[35] le Istituzioni europee abbiano considerato la "identificazione biometrica" – cui evidentemente sono preordinate le TRF – come un'area di applicazione dell'IA bisognosa di specifico intervento.

Così, nel 2019, il Gruppo di esperti sull'IA individuava alcune applicazioni di sistemi intelligenti da relegare a forme di "utilizzo eccezionale", ad esempio per finalità legate alla sicurezza nazionale, nel rispetto dei diritti fondamentali e dei principi di necessità e proporzionalità[36]. In particolare, invocava una futura regolamentazione – adeguando, se del caso, il quadro normativo vigente – con specifico riguardo al tracciamento o

soprattutto doveva essere riconosciuto all'interessato il diritto ad una "valutazione umana, compresa una spiegazione della decisione conseguita dopo tale valutazione". Non soltanto il progetto di regolamento prevedeva disposizioni di ben altro tenore rispetto a quelle poi approvate, ma nello stesso testo vigente permane ancora il considerando n. 71, che si esprime in termini abbastanza diversi rispetto all'articolato, nella misura in cui indica tra le garanzie che dovrebbero essere apprestate a tutela dell'interessato, oltre alle specifiche informazioni dovute e al diritto di ottenere l'intervento umano, anche il diritto "di ottenere una spiegazione della decisione conseguita".
Il dibattito sul tema è acceso. In senso fra loro opposto, cfr. S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to Explanation of Atutomated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 7, 2, 2017, 76 ss.; G. Malgieri, G. Comandè, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 7, 4, 243 ss. Cfr. anche B. Goodman, S. Flaxman, *European Union Regulations on algorithmic decision-making and a "Right to Explanation"*, in *AI Magazine*, 38, 3, 2017.

[34] Cfr. A. Adinolfi, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, 13 ss.; A. Amidei, *La governance dell'intelligenza artificiale: profili e prospettive di diritto dell'Unione europea*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 571-588.

[35] Al momento in cui si scrive, la Proposta di regolamento nota come *AI Act* (v. *supra*, nota 6) è stata approvata in prima lettura dal Parlamento europeo in data 13 marzo 2024 e, secondo la procedura legislativa ordinaria, deve ora ottenere l'approvazione del Consiglio. Cfr. per un primo commento della disciplina B. Marchetti, C. Casonato, *Prime osservazioni sulla proposta di Regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal*, 3, 2021, 415-437; G. Finocchiaro, *The regulation of artificial intelligence*, in *AI & Society*, 3 aprile 2023.

[36] AI HLEG, *Policy and Investment Recommendations for trustworthy AI*, Bruxelles, 26 giugno 2019, punto 28.1.

DPCE online
ISSN: 2037-6677

all'identificazione personale, fisica o mentale degli individui e alla profilazione attraverso metodi di riconoscimento biometrico.

Tuttavia, già nel Libro bianco sull'IA dell'anno successivo, le preoccupazioni generali subivano un ridimensionamento, laddove, pur riconoscendo la varietà di utilizzi e finalità di questo genere di tecnologie, si accordava ampia fiducia alla disciplina in materia di protezione dei dati stabilita dal GDPR. Soltanto per l'identificazione biometrica remota – "ad esempio mediante la diffusione di sistemi di riconoscimento facciale in luoghi pubblici" – si suggeriva l'avvio di un ampio dibattito in seno alla Commissione europea "per affrontare eventuali preoccupazioni sociali relative all'uso dell'IA per tali fini in luoghi pubblici e per evitare la frammentazione del mercato interno"[37].

Al contrario, pochi mesi dopo la presentazione dell'*AI Act* – su cui si tornerà tra poco – il Parlamento europeo, con una Risoluzione relativa all'utilizzo dell'IA in campo penale, manifestava serie preoccupazioni sulle TRF e chiedeva "una moratoria sulla diffusione dei sistemi di riconoscimento facciale per le attività di contrasto con funzione di identificazione, a meno che non siano usate strettamente ai fini dell'identificazione delle vittime di reati, finché le norme tecniche non possano essere considerate pienamente conformi con i diritti fondamentali, i risultati ottenuti siano privi di distorsioni e non discriminatori, il quadro giuridico fornisca salvaguardie rigorose contro l'utilizzo improprio e un attento controllo democratico e adeguata vigilanza, e vi sia la prova empirica della necessità e proporzionalità della diffusione di tali tecnologie"[38].

In Italia, la richiesta del Parlamento europeo veniva recepita con il d.l. 8 ottobre 2021, n. 139 (c.d. Decreto Capienze), il cui art. 9, comma 9, sospendeva fino al 21 dicembre 2023 "l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici […] in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati". Tuttavia, tale moratoria risultava particolarmente attenuata alla luce del comma 12 dello stesso articolo, ai sensi del quale la sospensione non era applicabile "ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali […], in presenza […] di parere favorevole del Garante […]". La moratoria è stata recentemente prorogata – non senza dibattito – fino al 31 dicembre 2025.

Recependo solo in parte le indicazioni del Libro bianco, la proposta di Regolamento (*AI Act*), a partire dalla prima versione presentata nel 2021, contiene una disciplina particolarmente dettagliata sui sistemi di identificazione biometrica remota in tempo reale, ammissibili solo a certe condizioni. Definiti come sistemi "in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi"[39], questi sono consentiti in spazi accessibili al pubblico solo laddove il loro impiego

[37] Commissione europea, *Libro bianco sull'intelligenza artificiale*, Bruxelles, 19 febbraio 2020, COM(2020) 65 final, 24.
[38] Parlamento europeo, *Risoluzione sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale*, 6 ottobre 2021, 2020/2016(INI).
[39] *AI Act* (versione 21.4.2021), art. 3, n. 37.

risulti strettamente necessario per la ricerca di potenziali vittime di reato, la prevenzione di attacchi terroristici o minacce specifiche, sostanziali ed imminenti per la vita e l'incolumità fisica, la localizzazione e l'identificazione di un sospettato di reato di una certa gravità[40]. Tuttavia, anche in questo caso, la messa in atto di tali pratiche deve "tenere conto" della probabilità e della gravità del danno potenziale e delle conseguenze per i diritti e le libertà delle persone interessate[41]. In aggiunta, l'applicazione deve essere autorizzata preventivamente da un'autorità giudiziaria o amministrativa indipendente dello Stato membro, anche se in casi urgenti si consente di richiedere e ottenere detta autorizzazione in un secondo momento[42]. La realizzazione dello schema è demandata agli Stati membri, i cui legislatori non solo dovranno disciplinare le procedure per la richiesta e il rilascio delle autorizzazioni, ma più in generale potranno decidere di consentire "in tutto o in parte" all'uso di questi sistemi secondo le condizioni e i limiti dettati dalla proposta di regolamento[43]. Tale impostazione espone ovviamente al rischio di vedere introdotte discipline nazionali differenti all'interno dell'UE, in una materia che pare necessitare particolarmente di armonizzazione e cooperazione tra le autorità statali, se non altro per il perseguimento di quei crimini connotati da transnazionalità e per i quali vige la disciplina del mandato di arresto europeo.

Tuttavia, la disciplina sulla identificazione biometrica ha costituito uno dei punti nevralgici di discussione della proposta, tanto che nel testo licenziato dal Coreper a inizio 2024[44] si è intervenuti su alcuni aspetti essenziali. Il nuovo art. 5 conferma il divieto di cui sopra, ma modifica leggermente le eccezioni: intanto, è chiarito che è consentito l'utilizzo per la ricerca di vittime di specifici reati – sequestro di persona, traffico di essere umani e sfruttamento sessuale – o di persone scomparse, mentre nella precedente versione questo elenco era assente; inoltre, la localizzazione e l'identificazione devono riguardare persone sospettate di aver commesso i reati indicati in uno specifico allegato al Regolamento – in luogo della Decisione quadro relativo al mandato di arresto europeo, cui rinviava la proposta del 2021 – che siano punibili negli Stati membri interessati con una pena detentiva non inferiore nel massimo a quattro anni (rispetto ai tre anni della versione 2021)[45]. Rispetto all'elenco di reati cui si rimandava nel 2021, il nuovo testo si differenzia sia perché considera un minore numero di illeciti sia, soprattutto, perché evita di operare rinvii ad altri atti, concepiti ad altri fini, e mantiene maggiore "controllo" sulla disciplina. Probabilmente superflua, ma a suo modo interessante perché consente di mettere a fuoco i rapporti tra *AI Act* e GDPR, la precisazione con cui nel nuovo testo si ricorda

[40] *AI Act* (versione 21.4.2021), art. 5.1, lett. d).
[41] *AI Act* (versione 21.4.2021), art. 5.2.
[42] *AI Act* (versione 21.4.2021), art. 5.3.
[43] *AI Act* (versione 21.4.2021), art. 5.4.
[44] Consiglio UE, 2021/0106(COD), 5662/24, 26 gennaio 2024. Il successivo testo approvato dal Parlamento europeo il 13 marzo 2024, con riguardo al tema di nostro interesse, conferma interamente il testo di gennaio, al netto di qualche aggiustamento di carattere meramente formale.
[45] v. *AI Act*, all. II, nel cui elenco si ritrovano una serie di reati molto gravi, tra cui terrorismo, sfruttamento di minori, omicidio, stupro, rapimento, crimini sotto la giurisdizione della Corte penale internazionale, ecc.

DPCE online
ISSN: 2037-6677

che queste disposizioni non pregiudicano in alcun modo l'applicazione dell'art. 9 GDPR sul trattamento di dati biometrici per scopi diversi dal *law enforcement*[46].

Altra importante novità contenuta nel testo del 2024 attiene a due ulteriori divieti esplicitamente menzionati: in primo luogo, il divieto di utilizzare l'IA per creare o espandere database di riconoscimento facciale mediante lo *scraping* incondizionato di immagini facciali da internet o da videocamere a circuito chiuso; inoltre, il divieto di utilizzare l'IA – con evidente riferimento implicito alle TRF – per desumere le emozioni di una persona fisica sul luogo di lavoro o educativo, a meno che non si tratti di ragioni mediche o di sicurezza[47].

Sul piano procedurale, è confermato l'impianto generale della proposta del 2021, con qualche specificazione non banale. Innanzitutto, è esplicitato con chiarezza che l'identificazione biometrica in tempo reale deve essere sfruttata solo per confermare l'identità della persona specificamente individuata[48]. In aggiunta, l'autorità di *law enforcement* deve aver completato una valutazione di impatto sui diritti fondamentali (*fundamental rights impact assessment*) secondo quanto previsto per i sistemi di IA ad alto rischio (art. 27 *AI Act*) e deve aver registrato il sistema nel database di cui all'art. 49 *AI Act*. Ancora, il nuovo testo impone che le discipline nazionali prevedano un termine massimo di ventiquattro ore per la convalida degli utilizzi messi in atto in caso di urgenza[49]. Infine, sono richiesti alcuni adempimenti volti a rendere effettivo il controllo delle Istituzioni europee sulle discipline nazionali: la normativa degli Stati membri deve essere notificata alla Commissione entro trenta giorni dalla sua adozione; le autorità garanti del mercato e della protezione dei dati personali sono obbligate a presentare alla Commissione report annuali sull'utilizzo di questi sistemi ai fini anzidetti; sulla base di questi report, la stessa Commissione pubblicherà report annuali relativi ad ogni Stato membro[50].

Ai fini del presente lavoro, deve essere segnalato un altro notevole passo in avanti compiuto nella nuova versione dell'*AI Act*. Rispetto al testo del 2021, che si limitava a includere tra i sistemi di IA ad alto rischio quelli utilizzati per l'identificazione biometrica reale delle persone fisiche, sia in tempo reale (se consentiti ai sensi dell'art. 5) sia "a posteriori"[51], si è intervenuti interviene opportunamente su questa disciplina. Infatti, si individuano con maggiore chiarezza gli specifici utilizzi ad alto rischio all'interno del settore della identificazione biometrica, sempre nei limiti in cui essa è consentita dalla normativa dell'UE e degli Stati membri: in primo luogo, l'identificazione biometrica remota, ad esclusione di quei sistemi per la "verifica biometrica" aventi il solo scopo di confermare l'identità di una

[46] *AI Act* (versione 13.3.2024), art. 5.1, ultimo periodo.
[47] *AI Act* (versione 13.3.2024), art. 5.1, lett. e) e f). Sull'opportunità di discplinare la pratica nota come "*scraping*", cfr. F. Campbell, *Data Scraping - What Are the Privacy Implications*, in *Privacy & Data Protection*, 20, 1, 2019, 3 ss.
[48] *AI Act* (versione 13.3.2024), art. 5.2.
[49] *AI Act* (versione 13.3.2024), art. 5.3.
[50] *AI Act* (versione 13.3.2024), art. 5, parr. da 4 a 7.
[51] *AI Act* (versione 2021), allegato III, p. 1.

persona; inoltre, i sistemi di IA utilizzati per la "categorizzazione biometrica" e quelli deputati al riconoscimento delle emozioni[52].

Rimandando alle conclusioni altre considerazioni, basti qui notare che la nuova disciplina dell'*AI Act* avrà evidentemente effetti sia sugli impieghi in ambito pubblico sia in ambito privato: nel primo caso, accanto agli obblighi previsti per i sistemi di alto rischio, opera una disciplina più restrittiva relativa all'utilizzo della sola identificazione biometrica in tempo reale da parte delle forze dell'ordine; nel secondo caso, invece, si limita a qualificare ad alto rischio, in attesa di possibili aggiunte del legislatore nazionale, soltanto pochi utilizzi delle TRF, lasciando tutti gli altri utilizzi alla disciplina prevista per i sistemi a basso rischio (sempreché le TRF siano riconducibili all'IA) o alla comunque impregiudicata disciplina sulla protezione dei dati personali di cui al GDPR.

4. Esperienze regolatorie negli USA

Negli USA, sebbene l'attenzione della dottrina e delle istituzioni in materia di dati biometrici e TRF possa dirsi ormai datata[53], non esiste una normativa federale che si occupi di disciplinare il fenomeno. Questo approccio è perfettamente in linea con quanto accade nell'ambito della protezione dei dati personali, laddove, a differenza del modello europeo oggi basato sul GDPR, la relativa disciplina non è contenuta in un "testo unico" ma si ritrova in leggi o regolamenti federali riferiti alle singole materie[54]. Tuttavia, a livello statale esistono in alcuni casi atti legislativi ideati come veri e propri codici della privacy, vicini all'idea del GDPR, in cui sono riportati i principi della disciplina applicabile evidentemente soltanto all'interno del relativo Stato[55].

Con riguardo alle TRF la situazione è abbastanza simile. A fronte di una assenza di normativa federale, si registrano iniziative degli Stati membri – ma, come si accennerà, anche di enti più piccoli – che puntano a regolare il fenomeno concentrandosi su profili non sempre coincidenti.

In realtà, sarebbe quantomeno ingeneroso sottovalutare il dibattito esistente a livello federale. Ad esempio, la *Federal Trade Commission* (FTC) già nel 2012, dopo un'inchiesta relativa all'utilizzo delle TRF da parte di *Facebook*, ha adottato il documento "*Facing facts: Best practices for common uses of facial recognition*"[56]; il *National Institute of Standards and Technology* (NIST),

[52] *AI Act* (versione 13.3.2014), allegato III, p. 1.
[53] Limitandosi alle sole istituzioni, cfr. Congressional Research Service, *Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations*, R46541, Settembre 2020; U.S. Government Accountability Office (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522, 11 agosto 2020.
[54] Cfr. A. Di Martino, *Profili costituzionali della privacy in Europa e negli Stati Uniti*, cit.; U. Pagallo, *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Milano, 2008.
[55] Ad oggi, il numero di Stati americani che hanno introdotto una disciplina organica sulla privacy dei consumatori appare in rapida crescita: tra questi, California, Nevada, Maine, Vermont, Illinois, Texas, Washington, New York, Massachussets, New Mexico.
[56] Federal Trade Commission (FTC), *Facing facts: Best practices for common uses of facial recognition*, ottobre 2012.

DPCE online
ISSN: 2037-6677

agenzia facente parte del Dipartimento del commercio, ormai da molti anni conduce test sugli algoritmi di riconoscimento facciale sottoposti volontariamente ad esame da parte delle aziende private[57]. Infine, non mancano proposte di legge o di moratoria in materia, perlopiù provenienti dall'area del Partito democratico, per quanto il Congresso abbia finora evitato la prosecuzione dei lavori.

Sul punto, merita un rapido cenno il "*Facial Recognition and Biometric Technology Moratorium Act*", presentato al Congresso nel 2021 e poi nuovamente nel 2023[58], relativo appunto alle TRF nello specifico, intese come categoria speciale di sorveglianza biometrica bisognosa di autonoma disciplina. Il testo è dedicato soltanto all'utilizzo "pubblico" delle TRF da parte del Governo federale e delle amministrazioni statali e locali. Dopo aver fornito una definizione di "riconoscimento facciale"[59], la proposta immagina un divieto generalizzato di utilizzo di sistemi di sorveglianza biometrica, ad eccezioni di ipotesi che il Congresso è chiamato a stabilire con successivo atto. In aggiunta, si impone agli Stati membri di uniformare la disciplina statale a quella federale, salvo possibilità di istituire regimi ulteriormente restrittivi[60].

Sempre con riguardo al *law enforcement*, un'altra proposta di legge più articolata – denominata "*Facial Recognition Act of 2022*"[61] – opta come regola generale per un regime autorizzatorio: sarà l'autorità giudiziaria a consentire per non più di sette giorni l'utilizzo del sistema alle forze dell'ordine, le quali nella richiesta dovranno indicare o descrivere la persona che intendono identificare e motivare sulla probabilità che il sospettato abbia commesso un "*serious violent felony*"[62]. Non sarebbe richiesta invece autorizzazione per l'identificazione (*rectius*: per "assistere" l'identificazione[63]) di vittime di reato o per i soggetti legalmente arrestati, né laddove il *prosecutor* valuti sussistente una emergenza, salvo convalida da parte dell'autorità giudiziaria entro dodici ore. Al di fuori di questo regime, restano espressamente vietati utilizzi volti ad agevolare l'applicazione della normativa sulla immigrazione, così come l'utilizzo di *body cameras* e droni e qualsiasi forma di *face*

[57] Il NIST, come agenzia facente parte dell'U.S. Department of Commerce, conduce, a partire dall'inizio degli anni 2000, test degli algoritmi di riconoscimento facciale che vengono ad essa sottoposti volontariamente dalle aziende private: la documentazione è reperibile su https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt.

[58] Congresso USA, *Facial Recognition and Biometric Technology Moratorium Act of 2023*, S. 681.

[59] *Ivi*, sec. 2(3): "The term «facial recognition» means an automated or semi-automated process that— (A) assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating surveillance information about an individual based on the physical characteristics of the individual's face; or (B) logs characteristics of an individual's face, head, or body to infer emotion, associations, activities, or the location of an individual".

[60] *Ivi*, sec. 3 e sec. 4.

[61] Congresso USA, *Facial Recognition Act of 2022*, H.R. 9061.

[62] Il rinvio è ai crimini di cui allo U.S. Code, tit. 18, sec. 3559(c)(2)(F).

[63] Nel testo questa opportuna precisazione è costante: il sistema comunque non "identifica", ma "assiste l'identificazione" da parte delle forze dell'ordine.

surveillance. Infine, il riconoscimento facciale non può costituire la sola base per la ricerca di un sospettato, l'arresto o altro atto di *law enforcement*[64].

Come accennato, queste proposte, comunque limitate agli utilizzi in ambito pubblico, sono state finora ignorate dal Congresso.

D'altro canto, a livello statale la regolamentazione del fenomeno sta assumendo contorni sempre più significativi: fioriscono, infatti, discipline relative sia agli utilizzi in ambito pubblico che in ambito privato, contenute in atti normativi volti a disciplinare, in alcuni casi, in generale la protezione dei dati personali, mentre in altri l'identificazione biometrica se non specificamente le TRF[65].

Tra le normative a livello statale, una delle più complete è quella dell'*Illinois Information Privacy Act* (BIPA) in vigore dal 2008, che regola, tra le altre cose, la raccolta, l'uso e la condivisione di informazioni biometriche da parte di enti privati che svolgono attività commerciale, intendendo per informazioni biometriche qualsiasi informazione che, indipendentemente dal metodo di acquisizione, si basi su identificatori biometrici, come le scansioni facciali o oculari[66]. Il BIPA, in particolare, richiede alle imprese di ottenere il consenso informato degli individui prima della scansione delle informazioni biometriche[67]. Addirittura, è garantito agli individui il diritto di azione in relazione alle informazioni biometriche raccolte o utilizzate in violazione della legge, indipendentemente dal fatto che siano stati causati loro dei danni[68].

In California, il *California Consumer Privacy Act* (CCPA) in vigore dal 2020 e modificato nel 2023 dal *California Privacy Rights Act* (CPRA), pur non operando alcun espresso riferimento alle TRF, considera le informazioni biometriche – definite in maniera molto ampia[69] – come dati personali protetti dalla legge, in relazione ai quali devono essere garantite all'interessato una serie di tutele, quali ad es. il diritto di accesso, cancellazione e opposizione al trasferimento. L'impresa che operi senza aver previsto un programma di sicurezza per il rispetto di questa normativa può incorrere in sanzioni pecuniarie da calcolarsi su ogni violazione e da moltiplicarsi per il numero di consumatori coinvolti. Tuttavia, una considerevole attenuazione della portata del CCPA/CPRA è dovuta al fatto che esso si applica solo nei confronti delle grandi imprese, ossia quelle con fatturato annuo superiore a venticinque milioni o che raccolgano dati su almeno cinquantamila o le cui entrate derivino per la maggior parte dalla vendita di informazioni personali[70]. Se il CCPA/CPRA riguarda soltanto

[64] Tutte queste disposizioni sono contenute in *Facial Recognition Act of 2022*, cit., tit. 1, sec. 101.
[65] J. Spivack, C. Garvie, *A taxonomy of legislative approaches to face recognition in the United States*, in A. Kak (a cura di), *Regulating biometrics: Global approaches and urgent questions*, AI Now Institute, New York, 2020, 86-95.
[66] Illinois Biometric Information Privacy Act (BIPA) of 2008, 740 ILCS 14, sec. 10. In dottrina, cfr. R.J. Yew, A. Xiang, *Regulating facial processing technologies: Tensions between legal and technical considerations in the application of Illinois BIPA*, Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency, 2022.
[67] BIPA, cit., sec. 15(b)(3).
[68] BIPA, cit., sec. 20.
[69] CCPA, sec. 1798.140, lett. c).
[70] CCPA, sec. 1798.140, lett. d).

DPCE online
ISSN: 2037-6677

l'ambito privato di utilizzo delle TRF, nella stessa California il dibattito è molto acceso anche con riguardo agli utilizzi per finalità di *law enforcement*. Tra il 2019 e il 2022 ha infatti operato una moratoria con cui si proibiva l'utilizzo della sorveglianza biometrica da parte delle forze dell'ordine – peraltro limitatamente alle riprese con videocamera, come le *body-worn cameras*[71]: alla sua scadenza, avvenuta il 1° gennaio 2023, nonostante insistenti richieste di proroga, non è stata più rinnovata.

In Texas, dal 2009 è in vigore il *Capture or Use of Biometric Identifier* (CUBI), inserito nel *Business and Commerce Code*, ai sensi del quale è vietata l'identificazione biometrica per scopi commerciali a meno che non vi sia consenso dell'interessato[72]. Inoltre, la *disclosure*, intesa anche come cessione dei dati, è illegittima a meno che l'interessato vi abbia consentito in caso di sua futura morte o scomparsa e in altri casi tassativi[73]. I dati devono comunque essere distrutti entro un anno dall'esaurimento del fine per cui sono stati raccolti, mentre eventuali violazioni della normativa possono portare a sanzioni civili pecuniarie del valore massimo di venticinquemila dollari per ogni violazione[74].

Se non mancano normative statali riferite o riferibili all'utilizzo delle TRF in ambito privato[75], negli ultimi anni sono stati introdotti, a fronte del silenzio sul piano federale, limitazioni importanti con riguardo alle TRF impiegate dalle forze dell'ordine a fini di contrasto e repressione dei reati. Soprassedendo sui divieti che sono stati imposti a livello cittadino[76], gli esempi più rilevanti sono due.

[71] State of California, Assembly Bill n. 1215, cap. 579, 8 ottobre 2019.
[72] Texas Business and Commerce Code, tit. 11(A), sec. 503.001(b)(2).
[73] Texas Business and Commerce Code, tit. 11(A), sec. 503.001(c).
[74] Texas Business and Commerce Code, tit. 11(A), sec. 503.001(c)(3).
[75] Sempre con riferimento agli utilizzi nel settore privato, proposte di legge in materia sono al centro del dibattito anche nello Stato di New York e di Washington.
Nel primo caso (New York State, *Biometric Privacy Act*, A00027, 6 gennaio 2021), si tratterebbe di un intervento normativo specificamente pensato per le TRF, ai sensi del quale l'interessato dovrebbe firmare una liberatoria scritta (*written release*) per accettare il trattamento e le finalità, sarebbe vietato il profitto dalle pratiche di scambio di dati raccolti mediante TRF e la *disclosure* sarebbe consentita solo alle condizioni appena viste con riferimento alla disciplina texana. Non sarebbero previste specifiche sanzioni in caso di violazioni, fatto salvo il risarcimento danni – o altri rimedi ammessi dall'ordinamento statale – che la stessa normativa si sforza di quantificare e distinguere per gravità a seconda che sia imputabile a colpa o a dolo. Si tratterebbe quindi di prevedere un regime di gestione di questi dati assimilato a quello previsto per i dati sensibili e confidenziali, mentre tale proposta di legge non fisserebbe alcuna preclusione per l'utilizzo delle TRF nel settore pubblico.
Nello Stato di Washington, il progetto di legge per l'introduzione del Washington Privacy Act del 2020 (SSB-6281 2019-2020) punterebbe ad una specifica regolamentazione del riconoscimento facciale (sec. 14), che prevederebbe la necessità del consenso dei consumatori prima di implementare servizi di riconoscimento facciale e una significativa sorveglianza umana in qualsiasi tipo di processo di profilazione.
[76] In alcune città, come San Francisco, Boston, Somerville, Portland, è stata discussa l'opportunità o è stato già proibito l'impiego delle TRF da parte delle forze di polizia e altre autorità pubbliche. A San Francisco il divieto è stato introdotto nel 2019. Cfr. A. Chen, *Why San Francisco's ban on face recognition is only the start of a long fight*, in *MIT Review*, 16 Maggio 2019.

Nello Stato di Washington, a partire da luglio 2021, è in vigore una disciplina relativa al riconoscimento facciale considerata tra le più restrittive degli Stati Uniti[77]. Ai sensi di questa normativa, le agenzie governative sono obbligate a notificare l'uso delle TRF in anticipo alla autorità legislativa, a condurre un'analisi di impatto sulla privacy e i diritti fondamentali e a informare il pubblico dell'uso previsto della tecnologia. Prima di impiegare il sistema, qualora questo sia preordinato a prendere decisioni che producono effetti legali su persone fisiche o altri effetti significativi, bisogna innanzitutto garantire che tali decisioni siano soggette ad una "significativa revisione umana" e inoltre occorre che il servizio sia previamente testato in condizioni operative. Con specifico riferimento all'utilizzo da parte delle forze dell'ordine per la prevenzione e repressione dei reati, è l'autorità giurisdizionale a dover rilasciare apposito mandato, a meno che non vi sia urgenza di procedere. Inoltre, l'utilizzo della TRF deve essere comunicato all'imputato prima del processo e, in ogni caso, l'incriminazione non può basarsi soltanto sul riconoscimento facciale.

Nello Stato del Maine dall'ottobre 2021 vige una disciplina in materia di "*facial surveillance*" da parte delle forze dell'ordine che impone un divieto generalizzato di utilizzo delle TRF a meno di eccezioni puntualmente previste, tra le quali le indagini inerenti a reati gravi solo qualora sia probabile la colpevolezza dell'individuo da identificare[78]. Di nuovo, i risultati del sistema di sorveglianza facciale non sono sufficienti da soli per incriminare un individuo. A differenza della disciplina dello Stato di Washington, nel Maine non è necessaria una autorizzazione o un mandato da parte dell'autorità giudiziaria, ma la ricerca nei sistemi di sorveglianza facciale deve essere richiesta, a seconda dei sistemi da utilizzare, al *Bureau of Motor Vehicles* oppure alla Polizia statale, i quali hanno l'obbligo di mantenere i registri delle richieste. Nel caso in cui i dati siano raccolti in violazione della normativa, essi devono essere cancellati immediatamente e non sono utilizzabili ad alcun fine.

Il quadro normativo che va delineandosi negli USA appare fortemente asimmetrico, non soltanto perché gli Stati membri riempiono il "vuoto" federale, ma perché lo fanno in maniera particolarmente differente, dato che la regolamentazione riguarda in alcuni casi l'ambito privato, in altri quelli pubblico e, in linea generale, oggetto e contenuto della disciplina coincidono solo in parte. D'altronde, mentre in ambito privato, a fronte del silenzio del legislatore federale, le normative statali sono quasi sempre incentrate sui dati biometrici spesso all'interno del quadro regolatorio sui dati personali, in ambito pubblico sembra propendersi, anche nelle ancora embrionali intenzioni del legislatore federale, per una regolamentazione specificamente incentrata sulle TRF come categoria peculiare di tecnologia biometrica.

5. Le soluzioni normative a confronto e la "scommessa" europea

La regolamentazione delle TRF nell'UE e negli USA, allo stato attuale, riflette il differente approccio seguito anche con riferimento alla

[77] State of Washington, Revised Code of Washington, sec. 43.386.
[78] Maine Revised Statutes, tit. 25, sec. 6001.

DPCE online
ISSN: 2037-6677

regolamentazione dell'IA[79]. Tuttavia, se nel dibattito la spinta ad una regolamentazione "forte" dell'IA è frenata dalla possibilità/opportunità di ricorrere ad atti di *soft law* o a forme di *co-regulation* e *self-regulation*[80], sembra invece che tale freno operi con meno forza con riferimento alle TRF. Si può infatti notare che nell'UE le preoccupazioni per la "identificazione biometrica", specialmente "in tempo reale", hanno segnato le riflessioni delle istituzioni fin dalle prime fasi del processo di regolamentazione dell'IA, tanto che il tema ha costituito uno dei punti di maggiore discussione nell'attuale testo dell'*AI Act*, in cui gli utilizzi di tecnologie biometriche sono considerati spesso ad alto rischio se non addirittura vietati.

D'altro canto, anche negli USA l'esigenza di regolamentare il fenomeno, a volte incluso nella disciplina sui dati biometrici, appare ormai forte a livello statale, dove l'introduzione di normative in materia comincia a crescere, ma non trascurabile neanche a livello federale, dove, al di là delle proposte di legge, l'esigenza di stabilire delle regole sulle TRF sembra anche più sentita rispetto all'IA in generale. Questo orientamento appare più marcato con riferimento agli utilizzi in ambito pubblico (specialmente da parte delle forze dell'ordine), ma comunque in generale riguarda la maggior parte degli impieghi delle TRF a causa della elevatissima pervasività di queste tecnologie.

Il dado è tratto: sia nell'UE che negli USA si ragiona ormai sempre più spesso su forme di regolamentazione delle TRF con atti di *hard law*, che impongono ai regolatori di stabilire un bilanciamento a priori tra rischi e benefici.

Stabilito questo punto, occorre notare come la regolamentazione degli utilizzi in ambito privato e pubblico segua logiche differenti.

Con riguardo agli impieghi di TRF per scopi privati, l'UE continua a riporre fiducia nel GDPR e nel generale quadro di protezione dei dati personali (e, specificamente, biometrici), che si basa anche sull'attività dei legislatori e dei Garanti nazionali. Negli USA, laddove manca una disciplina generale in materia di privacy a livello federale, una strada abbastanza simile è seguita a livello statale, dato che spesso una disciplina sui dati biometrici (e quindi sulle TRF) è contenuta in leggi generali sulla privacy (generalmente, dei consumatori). Tuttavia, il contenuto della disciplina differisce di molto, sia perché nei regimi statunitensi le regole sui dati biometrici sembrano più specifiche e non semplicemente "appiattite" su quelle riservate ai dati sensibili (art. 9 GDPR), sia soprattutto perché in ambito UE la legittimità del trattamento continua a ruotare intorno al

[79] Cfr. B. Marchetti, L. Parona, *La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio*, in *DPCE online*, 1, 2022, 237 ss.; D. Almeida, K. Shmarko, E. Lomas, *The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks*, in *AI and Ethics*, 2, 3, 2022, 377 ss.; D. Utegen, B.Z. Rakhmetov, *Facial recognition technology and ensuring security of biometric data: comparative analysis of legal regulation models*, in *Jour. Dig. Techn. and Law*, 1, 3, 2023, 825 ss.

[80] Cfr. E. Palmerini, E. Stradella (a cura di), *Law and Technology. The Challenge of Regulating Technological Development*, Pisa, 2013: R. Brownsword, K. Yeung (a cura di), *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes*, Oxford-Portland, 2008; U. Pagallo, *Intelligenza Artificiale e diritto. Linee guida per un oculato intervento normativo*, in *Sistemi intelligenti*, 3, 2017, 615-636.

consenso dell'interessato, anche con riguardo al trattamento esclusivamente automatizzato. Da questo punto di vista, negli USA, laddove la teoria del consenso in materia di privacy non assuma la stessa centralità europea, la disciplina subisce meno quelle critiche sulla validità ed effettività del consenso che possono riguardare i trattamenti di dati personali basati sull'impiego di TRF.

Probabilmente anche per questo motivo l'UE sta per "rafforzare" il GDPR con l'introduzione dell'*AI Act* che, in linea generale, qualifica come ad alto rischio il settore della "identificazione biometrica" deputato ad alcuni utilizzi: in tal modo alle tutele stabilite dal GDPR, si aggiungeranno opportunamente le garanzie – non basate sul consenso – stabilite dal Regolamento per i sistemi ad alto rischio. A questo riguardo, può evidenziarsi una ulteriore differenza tra esperienza europea e statunitense, nella misura in cui, come accade anche per gli impieghi in ambito pubblico (v. art. 5 *AI Act*), la tendenza dell'UE è quella di legare a doppio filo la disciplina sulla identificazione biometrica – e quindi sulle TRF – a quella sull'IA in generale, mentre negli USA questo legame non risulta mai esplicitato, dato che la regolamentazione delle tecnologie biometriche avviene a prescindere (anzi, in mancanza) di una regolamentazione dell'IA. Di fatto, l'UE sembra dare per scontato che le TRF (*rectius*: le tecnologie biometriche) si basino sempre su sistemi di IA: ammesso che questo sia vero, tale impostazione costringerà, anche in sede giurisprudenziale, a provare questa circostanza, in assenza della quale la tutela dell'*AI Act* – tra l'altro operante in senso forte "solo" per le TRF ad alto rischio – non potrebbe invocarsi. In questo senso, le normative statunitensi, che basano l'applicazione della disciplina sulla mera coincidenza tra tecnologia impiegata e definizione rispettivamente stabilita nell'atto legislativo, sembrano garantire maggiori certezze.

In ambito pubblico, i modelli sembrano somigliarsi maggiormente in relazione alla disciplina. È comune, infatti, la previsione di restrizioni legate agli utilizzi delle forze dell'ordine per la prevenzione e repressione dei reati: spesso gli impieghi sono consentiti solo per reati gravi, mentre prende piede in entrambe le esperienze il meccanismo autorizzatorio che richiede un vaglio preventivo da parte dell'autorità giudiziaria. Anche in questo caso, l'UE sta reputando opportuno "rafforzare" la disciplina prevista dalla LED con il divieto espresso (con relative eccezioni) dall'art. 5 *AI Act* in materia di "identificazione biometrica in tempo reale". Tuttavia, non possiamo dimenticare che la regolamentazione in ambito pubblico in Europa proviene dal livello "federale" – pur con tutte le virgolette del caso –, mentre negli USA essa scaturisce dall'attività legislativa statale. Il rapporto è clamorosamente invertito anche con riferimento all'imposizione di moratorie relative all'utilizzo di TRF: mentre nell'UE il Parlamento ha imposto una moratoria cui gli Stati membri (v. Italia) in alcuni casi si sono adeguati faticosamente o debolmente, la stessa esigenza negli USA è venuta "dal basso", arrivando a coinvolgere i sindaci delle città, considerato che a livello federale la proposta di introdurre una moratoria non è stata presa in considerazione dal Congresso.

Questa considerazione consente di mettere a fuoco la differenza probabilmente più pregnante che va delineandosi tra i due modelli: da una parte uno Stato federale all'interno del quale sono vigenti regimi fortemente

DPCE online
ISSN: 2037-6677

divergenti, dall'altra una organizzazione – non costituita come Stato federale – che punta a introdurre una disciplina unitaria negli Stati membri, al netto del residuo margine di discrezionalità consentito in relazione ad aspetti specifici.

La vera scommessa dell'UE, che riguarda non soltanto la regolamentazione delle TRF ma in generale (e forse in maniera ancora più evidente) la regolamentazione dell'IA e delle nuove tecnologie, è questa: tentare una "fuga in avanti" rispetto agli altri competitor mondiali – tra cui gli USA – scommettendo sulla armonizzazione normativa e sulla certezza del diritto per gli operatori[81], con l'obiettivo di recuperare posizioni sul piano dello sviluppo tecnologico[82] e – perché no – garantire ai cittadini dell'UE un quadro maggiormente rispettoso dei diritti fondamentali[83]. Solo il tempo dirà quali saranno gli effetti di questa scommessa, ma la strada appare tracciata.

Alberto Orlando
Dipartimento di Scienze Giuridiche
Università del Salento
alberto.orlando@unisalento.it

[81] Cfr. M. Graziadei, *La regolazione del rischio e il principio di precauzione: Stati Uniti ed Europa a confronto*, in *Sistemi intelligenti*, 2, 2017, 499 ss.; C. Cath, S. Wachter, B. Mittelstadt, M. Taddeo, L. Floridi, *Artificial Intelligence and the 'Good Society': the US, EU, and UK approach*, in *Sci Eng Ethics*, 24, 2018, 505 ss.; Cfr. E. Chiti, B. Marchetti, *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in *Riv. reg. merc.*, 1, 2020.
Sulle politiche dell'UE in materia di scambio di dati, anche genetici, per la lotta alla criminalità transfrontaliera, cfr. L. Scaffardi, Next Generation Prüm *e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, in *federalismi.it*, 8, 2021, 200 ss.

[82] Cfr. E.C. Raffiotta, *Dalla* self-regulation *alla* over-regulation *in ambito digitale: come (e perché) di un necessario cambio di prospettiva*, in *Oss. fonti*, 2, 2023, 246-267.

[83] Cfr. A. Bradford, *Digital empires: The global battle to regulate technology*. Oxford, 2023.