

Collezione di Giustizia Penale

dedicata a Massimo Nobili

e diretta da Marcello L. Busetto, Alberto Camon, Claudia Cesari, Enrico Marzaduri, Daniele Negri

NUOVE TECNOLOGIE, DATI BIOMETRICI E PROCEDIMENTO PENALE

a cura di
Claudia Cesari



Wolters Kluwer

CEDAM

Collezione di Giustizia Penale

dedicata a Massimo Nobili

e diretta da Marcello L. Busetto, Alberto Camon, Claudia Cesari,
Enrico Marzaduri, Daniele Negri

17

REVISORI

Rossano Adorno, Valentina Bonini, Silvia Buzzelli, Francesco Caprioli, Stefania Carnevale, Fabio Cassibba, Donato Castronuovo, Elena Maria Catalano, Massimo Ceresa-Gastaldo, Maria Grazia Coppetta, Marcello Daniele, Giovannangelo De Francesco, Maria Lucia Di Bitonto, Filippo Raffaele Dinacci, Franco Della Casa, Benedetta Galgani, Paola Maggio, Oliviero Mazza, Francesco Morelli, Vania Patané, Pier Paolo Paulesu, Tommaso Rafaraci, Paolo Renon, Andrea Scella, Luigi Stortoni, Giulio Ubertis, Elena Valentini, Gianluca Varraso, Daniele Vicoli.

COMITATO DI REDAZIONE

Alessandra Barberini, Marianna Biral, Gianluca Borgia, Eleonora Dei-Cas, Salvatore Formicola, Fabio Nicolichia, Niccolò Tronchin.

Ogni volume pubblicato nella collana è stato approvato dai direttori e – con l’eccezione degli atti congressuali – sottoposto a “doppio referaggio cieco” (*double blind peer review*) secondo il regolamento della collana. Il regolamento e la documentazione relativa alla revisione delle singole opere sono conservati dall’editore e dai direttori.

NUOVE TECNOLOGIE, DATI BIOMETRICI E PROCEDIMENTO PENALE

a cura di

Claudia Cesari



Wolters Kluwer

CEDAM

Il volume costituisce il frutto della ricerca svolta dagli Autori nell'ambito del progetto dal titolo "*Nuove tecnologie, dati biometrici e procedimento penale*", Finanziato dall'Unione Europea – *NextGenerationEU* – Missione 4 Istruzione e ricerca – Componente 2 *Dalla ricerca all'impresa* – Investimento 1.1, Avviso PRIN 2022 DD N. 104 del 2/2/2022, codice progetto MUR 2022CWNCH8 e coordinato dall'Università di Macerata, con le Università di Bologna, di Ferrara e di Pisa.

Copyright 2026 Wolters Kluwer Italia S.r.l.
Via Bisceglie n. 66 - 20152 - Milano

È espressamente vietato ogni utilizzo di questa opera per l'addestramento di **processi di apprendimento automatico e intelligenza artificiale**, tra cui in particolare di IA generativa. In caso di violazione, l'editore si riserva il diritto di intraprendere le opportune azioni legali a tutela dei propri diritti.

I diritti di traduzione, di memorizzazione elettronica, di riproduzione e di adattamento totale o parziale, con qualsiasi mezzo (compresi i microfilm e le copie fotostatiche), sono riservati per tutti i Paesi.

Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume/fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941, n. 633. Le riproduzioni diverse da quelle sopra indicate (per uso non personale - cioè, a titolo esemplificativo, commerciale, economico o professionale - e/o oltre il limite del 15%) potranno avvenire solo a seguito di specifica autorizzazione rilasciata da EDISER Srl, società di servizi dell'Associazione Italiana Editori, attraverso il marchio CLEARedi Centro Licenze e Autorizzazioni Riproduzioni Editoriali. Informazioni: www.clearedi.org.

L'elaborazione dei testi, anche se curata con scrupolosa attenzione, non può comportare specifiche responsabilità per eventuali involontari errori o inesattezze.

Stampato da GECA - Divisione Libri di CISCRA S.p.A.
Via Belvedere, 42 - 20862 Arcore (MB)

INDICE SOMMARIO

INTRODUZIONE

CLAUDIA CESARI

Introduzione	XI
--------------------	----

PARTE PRIMA

DATI, TECNOLOGIE, FENOMENI

DISPOSITIVI ELETTRONICI INDOSSABILI E PROVA PENALE

LAURA BARTOLI - ALBERTO CAMON

Parte I. *Brave new world*

1. <i>La privacy nella Rete: dal world wide web all'internet of things</i>	3
2. <i>Dall'internet of things all'internet of bodies</i>	5
3. <i>Nuove forme di sorveglianza? La prospettiva americana su riservatezza e trackers</i>	9
4. <i>Come funzionano i fitness tracker</i>	13
5. <i>Lo smart watch come testimone</i>	15

Parte II. Intanto, in Europa

1. <i>Tecnologia universale, soluzioni continentali</i>	17
2. <i>Liceità del trattamento e qualità del consenso</i>	20
3. <i>Segue. La limitazione delle finalità e la minimizzazione dei dati</i>	25
4. <i>E le forze dell'ordine? L'art. 8 Conv. e.d.u.</i>	29
5. <i>Segue. La necessità dell'ingerenza</i>	32
6. <i>Le conseguenze processuali</i>	34
7. <i>La riservatezza nelle indagini: la direttiva 'LED' (2016/680) e il d.lgs. n. 51 del 2018</i>	35

8. Segue. <i>Le categorie particolari</i>	37
9. <i>Conclusioni</i>	40

IL BRACCIALETTO ELETTRONICO: PROSPETTIVE INEDITE PER UNO STRUMENTO COLLAUDATO

ELENA VALENTINI

1. <i>Premessa definitoria</i>	43
2. <i>Uno strumento ancora utile?</i>	45
3. <i>Il braccialetto elettronico in Italia: un esordio timido, un presente che incalza</i>	47
4. <i>Le diverse tecnologie impiegate</i>	54
5. <i>Possibili ricadute probatorie</i>	56
6. <i>Uno sguardo al futuro</i>	65
7. Segue. <i>Il controllo a distanza del consumo di alcol</i>	67
8. Segue. <i>Monitoraggio elettronico e controllo dei migranti</i>	70
9. <i>Gli "altri" braccialetti elettronici</i>	78
10. <i>Conclusioni</i>	81

ACCESSO AI DISPOSITIVI ELETTRONICI E PRINCIPIO NEMO TENETUR SE DETEGERE: PASSWORDS BIOMETRICHE ED ALFA NUMERICHE, ORDINI DI DECRITTAZIONE E DI PRODUZIONE

GIACOMO COTTI

1. <i>L'accesso ai dispositivi elettronici: una sfida per la giustizia penale</i>	91
2. <i>Il versante sovranazionale</i>	94
3. Segue. <i>Uno sguardo comparato</i>	98
4. <i>Obbligo di rivelazione della password e diritto al silenzio: codici alfanumerici</i>	102
5. Segue. <i>Chiavi d'accesso biometriche</i>	107
6. <i>Obblighi di decrittazione e di produzione</i>	111
7. <i>Collaborazione "spontanea" e valutazione del "silenzio"</i>	115
8. <i>Cooperazione "fittizia" e attacchi a "forza bruta"</i>	119
9. <i>Obbligo di rivelazione della password e privilegio contro l'autoincriminazione</i>	121
10. <i>Conclusioni</i>	124

I SISTEMI DI RICONOSCIMENTO FACCIALE IN FASE DI INDAGINE: UNA BREVE ANALISI

STEFANO BILLI

1.	<i>Una breve ricognizione sui sistemi di riconoscimento facciale.....</i>	125
2.	<i>Le criticità dei sistemi di riconoscimento facciale con riguardo al processo penale; problemi di una disciplina “incompiuta”.....</i>	132
3.	<i>Segue. Il “pendio scivoloso” degli appigli preesistenti nella fase delle indagini preliminari.....</i>	135
4.	<i>Segue. La disciplina del c.d. “decreto capienze”.....</i>	137
5.	<i>“Artificial Intelligence Act” e riconoscimento facciale.....</i>	141
6.	<i>Conclusioni.....</i>	145

IL RICONOSCIMENTO FACCIALE ALL'INTERNO DEL PROCESSO, TRA CONTORSIONI DEL SISTEMA E RICADUTE MANCATE

VALERIA BOSCO

1.	<i>Il difficile inquadramento all'interno del sistema probatorio.....</i>	147
2.	<i>Le analogie e le differenze con l'istituto della ricognizione ex art. 213 c.p.p.</i>	150
3.	<i>L'utilizzo dei risultati del riconoscimento tramite la perizia e la consulenza tecnica.....</i>	153
4.	<i>Il vaglio preliminare ai fini del soddisfacimento dei criteri della prova scientifica.....</i>	154
5.	<i>L'ammissibilità come prova atipica.....</i>	160
6.	<i>Conclusioni.....</i>	166

IL RICONOSCIMENTO FACCIALE DALL'AI ACT ALL'ORDINAMENTO ITALIANO: LE DIRETTRICI DI UN'EVOLEZIONE NECESSARIA

CLAUDIA CESARI

1.	<i>Lo stato dell'arte: tecnologie di riconoscimento e ricadute concettuali e sistematiche.....</i>	169
2.	<i>L'AI Act: le indicazioni del framework europeo.....</i>	173
3.	<i>L'impatto sul sistema interno, tra legislazione codicistica e novelizzazione.....</i>	182

PARTE SECONDA

USO, CONSERVAZIONE, CIRCOLAZIONE

QUALE FUTURO PER LA PROVA BIOMETRICA?
RIFLESSIONI AL CROCEVIA TRA GARANZIE
DELL'INDIVIDUO E ACCERTAMENTO PENALE

ELEONORA DEI-CAS

1. <i>Dalla fallacia umana, a quella della macchina</i>	193
2. <i>Il “divieto-non divieto” e “l’alto rischio insufficientemente governato” dell’AI Act a proposito di riconoscimento biometrico remoto</i>	203
3. <i>Futuribili per una normativa interna improntata alle garanzie individuali</i>	210

I WEARABLES NEL PROCESSO ITALIANO

LAURA BARTOLI

1. <i>Introduzione</i>	221
2. <i>Dal sensore alla sentenza: un percorso tortuoso</i>	222
3. <i>Livello 1: il dato grezzo</i>	223
4. <i>Livello 2: l’informazione elaborata</i>	226
5. <i>I mezzi di acquisizione: le intercettazioni</i>	229
6. <i>Segue. Il sequestro di oggi</i>	230
7. <i>... e di domani</i>	234
8. <i>Livello 3: gli ordini di produzione</i>	235
9. <i>Livello 4: i dati resi manifestamente pubblici</i>	239
10. <i>Interpretazione</i>	240
11. <i>Valutazione</i>	244
12. <i>Conclusioni</i>	245

L'INCESSANTE ESPANSIONE DELLA BANCA DATI
BIOMETRICA EURODAC CONSULTABILE
(ANCHE) PER FINALITÀ DI CONTRASTO

LORENZO AGOSTINO

1. <i>Origini ed evoluzione della banca dati Eurodac</i>	247
2. <i>Le (blande) procedure di accesso a Eurodac per finalità di contrasto</i>	250

3.	<i>Riconoscimento facciale tramite Eurodac.....</i>	255
4.	<i>Eurodac in un contesto di interoperabilità: rischi di elusione delle (già inadeguate) garanzie.....</i>	258

LA CONSULTAZIONE E LO SCAMBIO AUTOMATIZZATI DI DATI BIOMETRICI (...E NON SOLO) NEL “QUADRO PRÜM II”

NICOLÒ DI PACO

1.	<i>Introduzione.....</i>	261
2.	<i>Il procedimento per la consultazione e lo scambio dei dati biometrici: regole e criticità.....</i>	267
3.	<i>Segue. La circolazione delle immagini facciali.....</i>	277
4.	<i>L'accesso ai police records fra problemi di traduzione e questioni di ordine generale.....</i>	281
5.	<i>Alcune riflessioni conclusive.....</i>	288
AUTORI.....		295

INTRODUZIONE

CLAUDIA CESARI

L'impatto dei fulminei, sorprendenti sviluppi tecnologici sul sistema della giustizia penale, in genere, e del rito penale, in particolare, è indubbiamente uno degli ambiti di ricerca oggi giorno più interessanti e più necessari.

Da anni in modo più episodico, e in tempi recenti in maniera invece più intensa, la dottrina è chiamata a interrogarsi su come le tecnologie stiano modificando la vita individuale e collettiva, e con essa le articolazioni principali del contesto sociale, a partire dalle strutture processuali e dalle loro logiche fondanti. In maniera rapida quanto pervasiva, prima la telematica e il digitale, oggi l'Intelligenza Artificiale, modificano le coordinate stesse del nostro mondo, le direttrici fondamentali del vivere civile, le pratiche del quotidiano, le relazioni umane, persino le chiavi di lettura di base della realtà, come lo spazio e il tempo. Inesorabilmente, tutto questo si riflette sul mondo della giustizia e il processo penale non può sottrarvisi: metodi, tecniche, valori, diritti, concetti fondamentali sono soggetti a una inevitabile torsione, che impone una revisione degli schemi tradizionali e una riflessione innovativa su ciò che va fatto per adeguare la normativa a una realtà che è già profondamente cambiata e in perenne mutamento.

In questo contesto, uno spazio speciale è occupato dal rapporto fra le nuove tecnologie e il corpo umano, come oggetto di misurazione, valutazione, osservazione, controllo: usata, quando non asservita, la persona fisica entra sempre di più in una relazione del tutto nuova con le tecnologie avanzate, specialmente quelle *AI based*, imponendo una riflessione innovativa sulle regole che la governano, specie in settori delicatissimi come quello processual-penalistico.

Di qui l'analisi svolta in questo volume, posto a chiusura della ricerca PRIN sul tema «Nuove tecnologie, dati biometrici e procedimenti penali». La prospettiva scelta è, come si vedrà, ampia, giacché si è tenuto conto non solo della nozione più specifica di dato biometrico, inteso come informazione tratta dal corpo umano a fini squisitamente identificativi, ma di un'area semanticamente più estesa, che include più possibili impieghi di

dati estratti dalla persona fisica e che a fini processuali possono essere rilevanti. Su questi si è svolta un'analisi ad ampio spettro, che si dedica – parafrasando l'art. 3, §1 n. 34 dell'*AI Act* – alle tecnologie che consentono il «trattamento tecnico specifico» di dati corporei di vario tipo («relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica») a vari fini. Un approfondimento che si è articolato altresì su diversi piani, dal tipo di uso che si può fare delle informazioni in esame, allo strumentario processual-penalistico di riferimento, dalla normativa europea a quella nazionale, dall'impiego nel rito ai problemi di conservazione e circolazione dei dati, in un'analisi che tiene conto delle sfide a numerosi livelli e in tutte le fasi del rito, poste dalla raccolta ed elaborazione di simili informazioni.

Per gli approfondimenti dei vari temi trattati, non si può che rinviare ai singoli contributi, ma preme sin d'ora portare l'attenzione al filo rosso che affiora nella trama degli studi svolti e li collega nitidamente: l'esigenza di una revisione legislativa urgente, che traduca in regole chiare come, con quali limiti e a quali fini dati di questo tipo possano essere raccolti e utilizzati in sede processuale. Ciò che emerge da ogni contributo, pur nella specificità dei problemi trattati, infatti, è come le tecnologie che raccolgono ed elaborano dati biometrici mettano in discussione molti capisaldi del sistema. Dalle garanzie tradizionali ai concetti di fondo sui quali si basano, dai principi costituzionali ad istituti consolidati dell'ordinamento, tutti in qualche modo “vanno in crisi” nell'impatto con questa dimensione nuova della conoscenza: le definizioni si slabbano, le garanzie mostrano la corda, la normativa si fa lacunosa e inadeguata, i punti di riferimento tradizionali (per tutti il diritto alla privacy o la normativa sulle intercettazioni) che hanno sinora fatto da sponda per gestire le novità tecnologiche sul piano processuale, non bastano più. La conseguenza – anche questa più volte rappresentata nei lavori svolti – è la tendenza della realtà ad occupare le zone franche dell'ordinamento, a imporsi comunque nel vuoto di regole e garanzie, con il rischio che diritti e libertà fondamentali vengano messi a repentaglio sistematicamente e che il legislatore arrivi in qualche modo “a cose fatte”, quando prassi pericolose o gestioni corrive si saranno già affermate e il sistema sarà pericolosamente avvezzo ad usi impropri di tecnologie sempre più invasive (e non più disposto a rinunziarvi).

A queste esigenze il presente lavoro intende dare il proprio contributo, prospettando non solo le criticità del sistema, ma anche i possibili percorsi per gestirle, nella consapevolezza che solo affrontandole lucidamente, soppesando e bilanciando in modo razionale gli interessi in gioco, si possa assicurare che il processo penale faccia uso degli strumenti più innovativi offerti dalla tecnologia senza per questo sacrificare oltre il tollerabile i diritti del singolo e le garanzie metodologiche del rito.

PARTE PRIMA

DATI, TECNOLOGIE, FENOMENI

DISPOSITIVI ELETTRONICI INDOSSABILI E PROVA PENALE

LAURA BARTOLI, ALBERTO CAMON *

DISPOSITIVI ELETTRONICI INDOSSABILI E PROVA PENALE

SOMMARIO: Parte I. *Brave new world*. — 1. La *privacy* nella Rete: dal *world wide web* all'*internet of things*. — 2. Dall'*internet of things* all'*internet of bodies*. — 3. Nuove forme di sorveglianza? La prospettiva americana su riservatezza e *trackers*. — 4. Come funzionano i *fitness tracker*. — 5. Lo *smart watch* come testimone. — Parte II. Intanto, in Europa. — 1. Tecnologia universale, soluzioni continentali. — 2. Liceità del trattamento e qualità del consenso. — 3. *Segue*. La limitazione delle finalità e la minimizzazione dei dati. — 4. E le forze dell'ordine? L'art. 8 Conv. e.d.u. — 5. *Segue*. La necessità dell'ingerenza. — 6. Le conseguenze processuali. — 7. La riservatezza nelle indagini: la direttiva 'LED' (2016/680) e il d.lgs. n. 51 del 2018. — 8. *Segue*. Le categorie particolari. — 9. Conclusioni.

Parte I — *Brave new world*

1. *La privacy nella Rete: dal world wide web all'internet of things*

Abbiamo ormai imparato quali e quante trappole per il diritto alla *privacy* stiano acquattate fra le maglie della Rete. Un esempio noto sono i *cookies*: quando visitiamo un sito, nel nostro computer viene depositato un piccolo programma — il *cookie*, appunto — che ci pedina e documenta le nostre attività nel *web*; alcuni di questi programmi si disinstallano appena lasciamo la pagina, altri restano attivi per mesi o anni; la maggior parte possono essere adoperati solo dal sito che li ha creati, alcuni possono es-

* Nonostante il lavoro sia frutto di una riflessione condivisa, la redazione della Parte I è opera di Alberto Camon; la Parte II è di Laura Bartoli.

serlo anche da siti “affiliati”. Li possiamo rifiutare ma – sempre ammesso che l’operazione riesca¹ – la navigazione ne risentirebbe.

I *cookies* sono la punta dell’*iceberg*. I server che ospitano i siti tengono un registro nel quale archiviano i nostri dati: indirizzo IP, data e ora della connessione, informazioni immesse quando compiliamo un modulo... Ancora: i *web beacons* sono minuscoli segnalatori incastonati in una pagina *web*: ogni volta che carichiamo la pagina, avvisano la compagnia che li ha installati². Naturalmente questi strumenti — e altri: l’esemplificazione è largamente incompleta — possono essere usati insieme, schiudendo scenari distopici: «qualsiasi sito visitato, qualsiasi link cliccato, qualsiasi messaggio Facebook spedito, qualsiasi video guardato su YouTube, tutto viene tracciato»³.

Tutto ciò è ormai noto. Meno conosciuti, forse, alcuni sviluppi recenti, che segnano nuove declinazioni della rete: l’“internet delle cose” e l’“internet dei corpi”. Molti dei fattori che stanno alla base della rivoluzione di internet — l’aumento massiccio della potenza di elaborazione e della capacità d’archiviazione dei computer, la miniaturizzazione degli apparecchi, la diffusione delle comunicazioni *wireless*, la digitalizzazione di enormi masse di dati, il crollo dei costi di produzione dei congegni — stanno producendo effetti oltre i confini del cyberspazio. Stiamo entrando in un mondo «inondato di sensori»⁴ che registrano movimenti, suoni, luci, potenziali elettrici, temperatura, umidità, posizione; un mondo popolato da “oggetti incantati”⁵, nel quale apparecchi d’uso comune — automobili, forni, bilance, impianti di riscaldamento, orologi, gioielli... — sono dotati di sensori e collegati in rete. Sistemi automatizzati che spengono

¹ Qualche anno fa è stato messo a punto «un insolito “cookie zombie”, [...] in grado di “resuscitare” quando un utente sceglie di disattivare l’ad tracking o cancellare i tracking cookie»; in questo modo le aziende riescono a bypassare «ogni intenzione esplicita degli utenti, comprese l’impostazione “non tracciare”, la navigazione in incognito, altri tipi di browsing privato e la cancellazione dei cookie» (S. ZUBOFF, *Il capitalismo della sorveglianza*, trad. it., 2^a ed., Luiss, Roma, 2025, p. 177 s.).

² J. GEARY, *Tracking the trackers: What are cookies? An introduction to web tracking*, in *the-guardian.com*, 23 aprile 2012.

³ B. TURNER, *When Big Data Meets Big Brother: Why Courts Should Apply United States v. Jones to Protect People’s Data*, 16 N.C. J.L. & Tech. 377 (2015), p. 382.

⁴ E. HABER, *The Wiretapping of things*, 53 U.C. Davis L. Rev. 733 (2019), p. 748.

⁵ «*Enchanted objects*» è un’espressione coniata da D. ROSE in un *TED Talk* ([youtube.com/results?search_query=http%3A%2F%2Ftedxtalks.ted.com%2Fvideo%2FTEDxBerkeley-David-Rose-Enchant](https://www.youtube.com/results?search_query=http%3A%2F%2Ftedxtalks.ted.com%2Fvideo%2FTEDxBerkeley-David-Rose-Enchant)) e successivamente ripresa da molti (a esempio, A. McEWEN, H. CASSIMALLY, *Designing the Internet of Things*, Wiley, Chichester, 2014, p. 16; nella letteratura italiana, G. SARTOR, *L’intelligenza artificiale e il diritto*, Giappichelli, Torino, 2022, p. 15). A sua volta, la formula evoca un celebre adagio di A.C. CLARKE (it.wikipedia.org/wiki/Tre_leggi_di_Clarke): «qualunque tecnologia sufficientemente avanzata è indistinguibile dalla magia».

l'allarme, aprono la serranda del garage, accendono le luci e lo stereo, riscaldano la cena quando il proprietario s'appresta a fare ritorno a casa; frigoriferi che ordinano da soli il latte quando sta finendo; boccette di medicinali che registrano quando una pillola viene prelevata e avvertono il paziente che ha scordato di prenderla⁶; forchette intelligenti che monitorano quando e quanto velocemente si mangia⁷; tappeti destinati alle case degli anziani che misurano i loro passi allo scopo di prevenire cadute e fratture⁸...: il novero degli oggetti che possono essere collegati a internet è limitato soltanto dalla fantasia degli inventori⁹. Tutti questi marchingegni sono in grado di comunicare — l'uno con l'altro o con persone — senza l'intervento attivo del titolare e generano un flusso di dati imponente e senza soluzioni di continuità.

Queste informazioni possono essere di per se stesse private, come quando attestano le attività compiute all'interno delle mura di casa¹⁰. Inoltre, esse vengono conservate dalle compagnie alle quali sono trasmesse, prestandosi ad essere combinate e scandagliate con le tecniche d'analisi dei *big data*; per questa via anche dati apparentemente neutri ed innocenti, opportunamente raggruppati, diventano come le tessere d'un mosaico e compongono ritratti intimi e dettagliati dei nostri gusti, propensioni, interessi, abitudini: «in un mondo di sensori interconnessi, qualsiasi cosa può svelare qualcosa»¹¹.

2. *Dall'internet of things all'internet of bodies*

Negli ultimi anni, all'interno dell'internet delle cose è andata a poco a poco emergendo una categoria più stretta, chiamata internet dei corpi.

Secondo una classificazione che gode d'un certo credito, lo sviluppo

⁶ V. perma.cc/Y3D3-YT4U.

⁷ V. perma.cc/W3S3-7KKB.

⁸ S. R. PEPPE, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153 (2011), scaricabile da scholar.law.colorado.edu/articles/177, p. 1168.

⁹ M. ASHTON, *Debugging the real world: robust criminal prosecution in the internet of things*, 59 *Ariz. L. Rev.* 805 (2017), p. 808.

¹⁰ A. BIANCHINI, *Always On, Always Listening: Navigating Fourth Amendment Rights in a Smart Home*, 86 *Geo. Wash. L. Rev. Arguendo* 1 (2018), p. 7 s.; M.K. OHLHAUSEN, *The Internet of Things and The FTC: Does Innovation Require Intervention?*, in ftc.gov/sites/default/files/documents/public_statements/internet-things-ftc-does-innovation-require-intervention/131018chamber.pdf, p. 4 s.

¹¹ S.R. PEPPE, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 *Texas law review* 85 (2014), scaricabile da ssrn.com/abstract=2409074, p. 119.

degli strumenti che ne fanno parte è passato attraverso tre stadi: il “corpo esterno”, il “corpo interno”, il “corpo fuso”¹². La prima generazione è nata con gli smartphones, che ormai non si limitano a navigare in rete e ad ospitare app ma sono equipaggiati con bussole, GPS, accelerometri, sensori di luce ambientale, giroscopi. Poi sono arrivati i *wearables*: strumenti elettronici indossabili dalle svariate fogge — braccialetti, orologi, vestiti, scarpe, tatuaggi elettronici¹³, occhiali, cuffie, anelli, cinghie, spille, ciondoli. A seconda dei modelli, permettono all’utente di monitorare e condividere battito cardiaco, pressione sanguigna, temperatura corporea, ritmo respiratorio, livelli di stress, esposizione ai raggi ultravioletti, sudorazione, tasso d’idratazione, livello d’ossigeno nel sangue, giorni d’ovulazione, durata e qualità del sonno, passi fatti, distanze percorse, tragitti, velocità, calorie bruciate, piani saliti o scesi, stato mentale (passivo, eccitato, pessimista, ansioso, equilibrato)¹⁴.

A questi apparecchi, pensati soprattutto per il fitness e ormai molto popolari, se ne affiancano altri dall’uso più spiccatamente sanitario, per i quali si parla già da tempo di “telemedicina” e di medicina personalizzata: polsini che misurano la pressione e si sincronizzano con lo smartphone, dove un’app riporta i risultati su un grafico e li inoltra periodicamente al medico¹⁵; dispositivi adoperati dai diabetici per monitorare il livello di glucosio¹⁶; reggiseni che registrano piccole variazioni della temperatura, che a loro volta possono indicare un tumore agli stadi iniziali¹⁷; e così via. Alcune aziende specializzate offrono un “ecosistema” chiuso di dispositivi e servizi¹⁸: lo stesso brand può offrire lo smartwatch, lo sfigmomanometro connesso, la bilancia intelligente, il termometro 2.0, il materasso che misura la qualità del sonno e una sorta di conchiglia da applli-

¹² A.M. MATWYSHYN, *The internet of bodies*, 61 *Wm. & Mary L. Rev.* 77 (2019), p. 94.

La tripartizione è ripresa da C. AMATO, *Internet of Bodies: Digital Content Directive, and beyond*, 12 *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 181 (2021), p. 183 s.

¹³ Q. HARDY, *Big Data in Your Blood*, in *The New York Times*, 7 settembre 2012.

¹⁴ Cfr. E.S. BROTTEN, “Every Move You Make, Every Step You Take, I’ll be Watching You”: *Is Wearable Data Your Next Discovery Tool in Personal Injury Litigation?*, portal.criticalimpact.com/newsletter/newslettershow5.cfm?contentonly=1&content=24578&id=2987; N. CHANDLER, *How FitBit Works*, electronics.howstuffworks.com/gadgets/fitness/fitbit.htm; Q. HARDY, *Big Data in Your Blood*, cit.; S. R. PEPPET, *Regulating the Internet of Things*, cit., p. 93 s.

¹⁵ V. perma.cc/874Z-8H65.

¹⁶ M. SWAN, *Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0*, *J. Sens. Actuator Netw.* 2012, 1, scaricabile da mdpi.com/2224-2708/1/3/217, p. 222.

¹⁷ V. perma.cc/EG6E-MUYA.

¹⁸ È il *core business* di Withings, compagnia che costruisce esclusivamente apparecchi per la telemedicina personalizzata.

care alle pareti della toilette in grado di eseguire settimanalmente un'analisi delle urine. I dati sono trasmessi e visualizzati in un'unica app, così da offrire un quadro d'insieme sullo stato di salute della persona, anche a seconda degli obiettivi selezionati e dei *device* acquistati (per esempio: chi è interessato al dimagrimento potrebbe fornirsi di orologio contapassi e bilancia). Sottoscrivendo un abbonamento, l'individuo riceve elaborazioni ulteriori: un punteggio che esprime una valutazione della salute a lungo termine; un progetto di routine per migliorare il proprio risultato; uno o più controlli da parte di personale medico qualificato nonché le analisi svolte in autonomia dall'intelligenza artificiale. Esiste perfino il bracciale che aiuta a superare le dipendenze e le cattive abitudini, trasmettendo una piccola scarica elettrica quando l'utente, inavvertitamente, incappa nel vizio: basta selezionare dalla app la mania da sconfiggere — il fumo, l'alimentazione smodata, il ruminare, la scarsa obbedienza alla sveglia mattutina — e l'indossabile provvede a riconoscere l'attività e punire il trasgressore¹⁹.

Le tecnologie di seconda generazione sono composte da dispositivi collocati all'interno del corpo o che entrano in contatto col corpo rompendo la pelle: pacemakers che trasmettono i dati via *wi-fi* al computer del paziente e da lì a quello del medico; impianti cocleari che includono funzionalità basate sul *bluetooth*; pillole ingeribili dotate d'un trasmettitore interno; pancreas artificiali connessi a internet e gestiti da un'app per cellulare; suture dotate di sensori che raccolgono dati sulle ferite in via di guarigione...²⁰.

I dispositivi di terza generazione fondono la mente umana con computer esterni connessi al *web*; la maggior parte è ancora allo stato sperimentale.

In queste pagine ci fermeremo soprattutto sugli strumenti della prima categoria, ma faremo qualche incursione anche su quelli della seconda. Si tratta di congegni che, più ancora di quelli che compongono l'*Internet of things*, sollevano preoccupazioni per la tenuta del diritto alla *privacy*²¹. In qualche misura essi mescolano il mondo fisico e biologico

¹⁹ Il dispositivo si chiama Pavlok: *shop.pavlok.com*.

²⁰ A.M. MATWYSHYN, *The internet of bodies*, cit., p. 103 s.

²¹ M.M. CHRISTOVICH, *Why Should We Care What Fitbit Shares - A Proposed Statutory Solution to Protect Sensitive Personal Fitness Information*, 38 *Hastings COMM. & ENT. L.J.* 91 (2016), p. 101.

Questo lavoro riguarda gli apparecchi che raccolgono dati dell'utente, non quelli che collezionano dati altrui. Non toccheremo cioè i dispositivi indossabili che registrano informazioni dall'ambiente circostante, mettendo così in discussione la *privacy* dei terzi che interagiscono con essi, consapevolmente o no. Il primo e più noto esempio è stato Google

con quello digitale²²; corpi e bit si fondono, la carne umana s'intreccia con *hardware*, *software* e algoritmi²³, il confine fra uomo e macchina si fa sfumato²⁴. Tutto questo permette di raccogliere dettagli intimi della vita degli utenti²⁵; sfumature ricche e minuziose su chi siamo, come ci comportiamo, quali sono i nostri gusti e persino le nostre intenzioni. Il numero e la profondità delle inferenze che possono essere tratte aumentano se dati provenienti da fonti diverse vengono aggregati: un accelerometro e un giroscopio, adoperati insieme, mostrano se i movimenti dell'utente sono costanti e uniformi oppure tremolanti e tesi, e questo consente di dedurre il suo livello di rilassamento; se s'aggiunge un rilevatore della frequenza cardiaca, s'arriva a riconoscere le emozioni. Oppure: misurazioni del ritmo cardiaco accoppiate a registrazioni della respirazione rivelano non solo le abitudini d'allenamento ma anche l'uso di cocaina, eroina, tabacco, alcool, ognuno dei quali produce una sorta d'univoca firma biometrica²⁶.

A guardar bene, si tratta di dati analoghi a quelli che, se fossero confidati a un medico, sarebbero coperti dal segreto professionale; ed anzi, un colloquio con un dottore si esaurisce in un singolo incontro o in più specifici incontri, mentre queste app spalmano nel tempo il monitoraggio, acquisendo una massa d'informazioni più significativa di quelle che verrebbero date al medico²⁷.

Gli apparecchi sono onnipresenti: «*always on, always sensing, always collecting, and always communicating*»²⁸, diventano parte di noi; hanno accesso

Glass, ma in seguito ne sono arrivati molti altri. Sull'argomento si possono vedere Z. TAKHSHID, *Wearable AI, Bystander Notice, and the Question of Privacy Frictions*, forthcoming B.U. L. Rev., scaricabile da papers.ssrn.com/sol3/papers.cfm?abstract_id=4693396, p. 102 s.; A.D. THIERER, *The Internet of things and wearable technology: addressing privacy and security concerns without derailing innovation*, 21 Rich. J.L. & Tech. 6 (2015), jolt.richmond.edu/jolt-archive/v21i2/article6.pdf, p. 53 s.; con riguardo all'ordinamento italiano, E. GERMANI, L. FEROLA, *Il wearable computing e gli orizzonti futuri della privacy*, in *Dir. informaz. informat.*, 2014, p. 75 s.

²² C. AMATO, *Internet of Bodies*, cit., p. 182; E. PAUWELS, S.W. DENTON, *The Internet of Bodies: Life and Death in the Age of AI*, 55 Calif. Western L. Rev. 221 (2018), p. 221; K.E. TAPP, *Smart devices won't be "smart" until society demands an expectation of privacy*, 56 U. Louisville L. Rev. 83 (2017), p. 86.

M. ASHTON (*Debugging the real world*, cit., p. 809) parla d'un «portale fra il cyberspazio e il mondo reale».

²³ A.M. MATWYSHYN, *The internet of bodies*, cit., p. 80.

²⁴ M. SWAN, *Sensor Mania*, cit., p. 248.

²⁵ K. SAPHNER, *You Should Be Free to Talk the Talk and Walk the Walk: Applying Riley V. California to Smart Activity Trackers*, in *Minn. Law Rev.*, (2016), p. 1715 s.

²⁶ S. R. PEPPE, *Regulating the Internet of Things*, cit., p. 93 s.

²⁷ D. GRAY, *A right to go dark*, 72 SMU L. Rev. 621 (2019), p. 655 s.

²⁸ Così A.D. THIERER, *The internet of things*, cit., p. 60. In seguito l'immagine è stata ripresa da A. BIANCHINI, *Always On, Always Listening*, cit.

alle nostre esperienze, alle nostre memorie; ricordano per noi; tengono traccia dei nostri spostamenti, condizioni di salute, umori. Un autore si spinge a dire che accedervi significa penetrare i segreti più riposti, perlustrare i meandri della mente umana, mettere a repentaglio l'inviolabilità della psiche²⁹. Quest'ultima osservazione è probabilmente eccessiva; malgrado ciò, è vero che siamo dinnanzi ad un salto di qualità: *l'internet of things* irrompe in un santuario della *privacy*, permette di controllare e misurare elettronicamente attività finora inosservabili, apre una finestra che s'affaccia all'interno delle case³⁰; ma *l'internet of bodies* si spinge più in là: apre una finestra che s'affaccia all'interno del corpo umano.

3. Nuove forme di sorveglianza? La prospettiva americana su riservatezza e trackers

Il difficile rapporto fra i *wearables* e il diritto alla riservatezza merita di essere inquadrato, sia pure brevemente, anche da un altro punto di vista. Secondo studiosi d'oltreoceano, un fenomeno nuovo sta spostando i concetti di sorveglianza, di *privacy*, di attentato alla *privacy*. Dal Panopticon al Grande Fratello, l'idea tradizionale di sorveglianza è associata ad una relazione di potere fra chi guarda e chi è guardato; la stessa parola francese *surveiller* descrive l'azione di chi, dall'alto, scruta attentamente qualcuno o qualcosa. Ma questi modelli non descriverebbero più perfettamente la realtà attuale.

Oggi la minaccia non viene soltanto dall'esterno ma anche da noi stessi; adoperando varie tecniche e strumenti, come appunto i *wearables*, stiamo iniziando a misurarci in maniera granulare: quanto dormiamo, dove andiamo, come e cosa respiriamo, cosa mangiamo, come passiamo il nostro tempo. Raccogliamo i dati che ci riguardano, li immagazziniamo da qualche parte nel *cloud*, diamo a terzi poteri d'accesso, li postiamo sui social. Ne risulta una relazione non più verticale ma orizzontale: fra pari o persino in favore del sorvegliato, che non subisce ma agisce. Diversamente dalla distopia orwelliana, nei social network la sorveglianza non punta a distruggere la soggettività ma in qualche misura a costruirla; non si tratta solo di mettere in comune informazioni ma di condividere se

²⁹ D. GRAY, *A right to go dark*, cit., p. 653 s., secondo il quale acquisire i dati registrati dai *wearables* sarebbe in contrasto con il V emendamento della costituzione statunitense.

³⁰ FTC Staff, *Internet of things* (report dal workshop su: *The Internet of Things: Privacy and Security in a Connected World*, 19 novembre 2013), in ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf, p. 17

stessi come modo per costruire un'identità. Qualcuno parla al riguardo di “autosorveglianza”³¹; qualcun altro, di “sorveglianza partecipativa”³².

Sono riflessioni suggestive, che stanno riscuotendo molto successo³³ e in effetti colgono alcuni aspetti. Al tempo stesso, presentano un rischio: l'enfasi posta sulla scelta di “autocontrollarsi” potrebbe condurre a negare in radice l'esigenza di proteggere informazioni liberamente raccolte e cedute. Il pericolo traspare chiaramente dalle righe di chi sottolinea una mutazione: i problemi tradizionali della *privacy* si verificano nell'ambito di un'interazione tra un individuo e una controparte; siccome gli interessi dell'uno e dell'altra collidono, il rapporto dev'essere regolato dal diritto; nella *self-surveillance*, invece, gli interessi della controparte scomparirebbero perché la controparte, semplicemente, non esiste³⁴. Portata a questi limiti, l'impostazione mostra difetti gravi.

Sotto molti profili, la decisione dell'utente è meno libera e meno consapevole di quel che si suppone. La raccolta dei dati è di regola automatica, nel senso che viene effettuata in modalità “*set it and forget it*”: dopo la prima configurazione, non è necessario dare un input manuale volta per volta. Inoltre, il setting di default dei *wearables* (come, in generale, quello di vari apparecchi che fanno parte dell'*Internet of things*) è generalmente impostato sulla soluzione che massimizza la cessione delle informazioni³⁵.

³¹ J. KANG, K. SHILTON, D. ESTRIN, J. BURKE, M. HANSEN, *Self-surveillance Privacy*, 97 *Iowa Law Review* 809 (2012), p. 812 s.

³² A. ALBRECHTSLUND, *Online Social Networking as Participatory Surveillance*, in *First Monday*, marzo 2008, scaricabile da researchgate.net/publication/220166794_Online_Social_Networking_as_Participatory_Surveillance, p. 5 s.

³³ L'idea dell'“autosorveglianza” è stata ripresa da tanti autori: cfr. R. CHIRGWIN, *Welcome to “uber-veillance” says Australian Privacy Foundation*, in theregister.com/2015/01/13/its_already_too_late_for_privacy, 13 gennaio 2015; M.M. CHRISTOVICH, *Why Should We Care*, cit., p. 102 s.; C. DEL ROSSO, C.M.BAST, *Protecting online privacy in the digital age: Carpenter v. United States and the fourth amendment's third-party doctrine*, 28 CATH. U. J. L. & TECH 89 (2020), p. 105; S.I. FRIEDLAND, *Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things is Changing the Face of Privacy*, 119 W. Va. L. Rev. 891 (2017), p. 893; ID., *I Spy: The New Self-Cybersurveillance and the “Internet of Things”*, 72 Wash. & Lee L. Rev. 1459 (2015), p. 1464 s.; C. NACKENOFF, *“Only the Beginning, Only Just the Start. Mostly I’m Silent”: New Constitutional Challenges with Data Collection Devices Brought into the Home*, 79 Maryland Law Review 88, p. 103. V. pure — ma in prospettiva non perfettamente coincidente — N.M. RICHARDS, *The dangers of surveillance*, 2017, 126 Harv. L. Rev. 1934 (2013).

³⁴ J. KANG-K. SHILTON-D. ESTRIN-J. BURKE-M. HANSEN, *Self-surveillance Privacy*, cit., p. 825 s.

³⁵ Cfr. N. CHANDLER, *How FitBit Works*, cit.; C. LAROSE, *On the Twelfth Day of Privacy, My True Love Gave to Me ... 12 Different Types of Wearables!*, in lexology.com, 24 dicembre 2014; A. SUI, W. SUI, S. LIU, R. RHODES, *Ethical considerations for the use of consumer wearables in health research*, 9 *Digital Health* 1 (2023), p. 3; A. RODIS, *Fitbit data and the fourth amendment: why the collection of data from a Fitbit constitutes a search and should require a warrant in light of Carpenter v.*

Proprio per questo, qualche anno fa negli Stati Uniti scoppiò uno scandalo: un giornalista scoprì che i Fitbit (uno dei *fitness tracker* più popolari) registravano le attività sessuali di tutti gli utenti, catalogandole secondo una scala che andava da “moderato” a “vigoroso”; a causa delle impostazioni predefinite del Fitbit, questi dati erano accessibili a chiunque attraverso una semplice ricerca su Google³⁶.

Il consenso del titolare, del resto, soffre di molti limiti. L'informazione sulla *privacy* è spesso deficitaria: la maggior parte dei *wearables* non hanno uno schermo, cosicché, per controllare la *policy* del produttore, occorre cercarla altrove: sulla scatola, sul sito della compagnia, su un'app associata al dispositivo³⁷; quando si riesce a trovarla, spesso è incompleta o sibillina³⁸, soprattutto per quanto riguarda gli usi che, dei dati ceduti, possono essere fatti³⁹; quando è completa, spesso diventa obsoleta rapidamente, perché ogni giorno che passa il progresso delle tecniche d'analisi rende possibile ricavare nuove inferenze dai dati già raccolti⁴⁰.

Ancora: in linea di massima il consenso alla cessione dei dati può essere rifiutato ma, per usare alcune funzioni dell'apparecchio, e in certi casi addirittura per usare l'apparecchio stesso, l'utente è obbligato ad aprire un account sul sito del produttore e a riversare lì i dati raccolti⁴¹. Se qualche aspetto della politica del produttore non piace si può cercarne un altro; ma per certi tipi di dispositivo il mercato è ristretto e non c'è concorrenza⁴².

United States, 29 *Wm. & Mary Bill of Rts. J.* 533 (2020), p. 550; B. TURNER, *When Big Data Meets Big Brother*, cit., p. 392.

³⁶ N. CHAURIYE, *Wearable Devices as Admissible Evidence: Technology is Killing Our Opportunity to Lie*, 24 *Cath. U. J. L. & Tech* 495 (2016), p. 503 e p. 526.

³⁷ G. JOHNSON, *Privacy and the Internet of Things: Why Changing Expectations Demand Heightened Standards*, 1 *Wash. U. Jur. Rev.* 345 (2019), p. 354; S.R. PEPPE, *Regulating the Internet of Things*, cit., p. 139 s.; Z. TAKHSHID, *Wearable AI*, cit., p. 13.

³⁸ Secondo una ricerca della *National privacy authority* statunitense, per i due terzi dei dispositivi manca una descrizione esauriente di come i dati vengono raccolti, usati, conservati e ceduti, mentre i tre quarti dei produttori non avvisa il consumatore che può cancellare i dati dall'apparecchio. Cfr. A.N. KITCHEN, *Smart devices and criminal investigations: protecting suspects' privacy and fourth amendment rights*, 54 *Criminal Law Bulletin* (2017), scaricabile da papers.ssrn.com/sol3/papers.cfm?abstract_id=3028119, p. 28 s.

³⁹ J. KANG, K. SHILTON, D. ESTRIN, J. BURKE, M. HANSEN, *Self-surveillance Privacy*, cit., p. 824 s.

⁴⁰ M.M. CHRISTOVICH, *Why Should We Care*, cit., p. 107 s.

⁴¹ Z. HUSSAIN, *Wary of Wearables: IP, Privacy, and Data Security Concerns*, in *lawpractice-today.org*, 14 gennaio 2016; G. JOHNSON, *Privacy and the Internet of Things*, cit., p. 354 («consumers are presented with a “choice”, but that choice is little more than the manufacturer stating “take it or leave it” — either accept the terms of use, or don't use the products»); A. RODIS, *Fitbit data and the fourth amendment*, cit., p. 545 s.; A.D. THIERER, *The internet of things*, cit., p. 29; M. SWAN, *Sensor Mania*, cit., p. 231.

⁴² J. KANG-K. SHILTON-D. ESTRIN-J. BURKE-M. HANSEN, *Self-surveillance Privacy*, cit., p. 824 s.

Si dirà: è pur sempre possibile non usare affatto gli apparecchi. A guardar bene, però, anche questa decisione non è del tutto libera, perché l'uso di alcuni dispositivi dell'*Internet of bodies* sta diventando progressivamente “meno facoltativo”⁴³. Può capitare che il datore di lavoro richieda d'indossare un badge di tracciamento della posizione⁴⁴; che un'impresa di trasporti si attenda che i suoi autisti indossino indumenti o dispositivi che monitorano il loro stato d'allerta⁴⁵; fino ad arrivare ad un'area in cui la libertà sostanzialmente scompare, quella dei dispositivi adoperati per ragioni mediche: possiamo davvero dire che Ross Compton, l'uomo che portava un *pacemaker* i cui dati sono stati utilizzati per accusarlo d'incendio doloso⁴⁶, abbia “scelto” d'usare il *pacemaker*?

In definitiva, nella maggior parte dei casi manca quella che un illustre studioso nordamericano chiama la «scelta volontaria significativa» dell'interessato⁴⁷; ci stiamo dirigendo verso una società della sorveglianza ma non lo facciamo con piena consapevolezza: «camminiamo come sonnambuli»⁴⁸.

Del resto, quand'anche tutto ciò non fosse vero; persino nei pochi casi e per le poche persone per le quali si potrebbe pensare ad una decisione libera ed informata, andrebbe comunque considerato che ormai una grossa porzione delle attività umane s'è spostata *online*; per la maggior parte dei servizi, il consumatore non ha altra opzione che turarsi il naso e cliccare “accetto”: dire che gli individui hanno una scelta, quando l'alternativa è chiamarsi fuori da tutta la tecnologia del terzo millennio, equivale a dire che una scelta realistica non c'è⁴⁹.

Per molti decenni s'è pensato, sull'una e sull'altra sponda dell'oceano, che le informazioni spontaneamente rivelate ad un terzo non potessero

⁴³ F. NICOLAI, M.-H. MARAS, J. TRAUTMANN, J. SCHNEIDER, *When objects betray you: the Internet of Things and the privilege against self-incrimination*, 33 *Information & Communications Technology Law* 255 (2024), scaricabile da publications.cispa.de/, p. 14 s.

⁴⁴ A.M. MATWYSHYN, *The internet of bodies*, cit., p. 101

⁴⁵ A.M. MATWYSHYN, *The internet of bodies*, cit., p. 83 s.

⁴⁶ *Infra*, Parte I, § 5.

⁴⁷ Nell'impostazione di O.S. KERR, *Implementing Carpenter. The digital fourth amendment*, 18 dicembre 2018, scaricabile da papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257, la presenza d'una “scelta volontaria significativa” esclude che, per raccogliere le informazioni disseminate in internet dall'interessato, si debbano applicare le tutele accordate dal IV emendamento della costituzione federale statunitense.

V. anche S.I. FRIEDLAND, *Drinking from the Fire Hose*, cit., p. 891 s., il quale, con un curioso ossimoro, parla d'un «*consensual and inadvertent tool that undermines privacy protection*».

⁴⁸ M.M. CHRISTOVICH, *Why Should We Care*, cit., p. 105.

⁴⁹ B. TURNER, *When Big Data Meets Big Brother*, cit., p. 422 s.; C. SLOBOGIN, *Subpoenas and Privacy*, 54 *DePaul Law Review* 805 (2005), p. 829.

godere di particolare protezione da parte dell'ordinamento, perché l'interessato avrebbe spontaneamente abdicato alle sue aspettative di riservatezza⁵⁰; quest'idea è entrata in crisi e da più parti s'avverte l'esigenza d'un ripensamento, perché tenerla ferma porterebbe ad un inaccettabile squilibrio nel rapporto fra autorità e cittadino; quasi ogni cosa che facciamo produce dati, e gran parte di questi dati sono condivisi, consapevolmente o inconsapevolmente, con altri; quella che un tempo sarebbe stata una piccola eccezione alle garanzie costituzionali, oggi se ne mangerebbe gran parte⁵¹: «persino i nostri documenti più privati — quelli che in altre epoche avremmo chiuso al sicuro nel cassetto della scrivania o distrutto — ormai risiedono su server di terze parti»⁵².

4. Come funzionano i fitness tracker

Abbiamo visto che l'*internet of bodies* comprende una gamma di congegni ampia e variegata. Qui non è possibile passarli in rassegna tutti, ma

⁵⁰ La concezione è stata sistematizzata negli U.S.A., dove va sotto il nome di "*third party doctrine*"; essa risale ad una pronuncia degli anni Settanta, nella quale la Corte suprema stabilì che gli organi dell'indagine non avevano bisogno d'un mandato per chiedere ad una banca di rivelare le registrazioni relative alle operazioni d'un cliente (*United States v. Miller*, 425 U.S. 435 (1976)).

In Italia manca un'elaborazione concettuale autonoma della categoria, ma se ne rinvencono applicazioni specifiche con riguardo a svariati strumenti d'indagine; si pensi alle pronunce sul pedinamento satellitare di un'autovettura (fra le più recenti, Cass. sez. IV, 21 aprile 2022, n. 21856, Bresciani, in *C.e.d.*, rv. 283386 - 01); all'affermazione secondo cui «affinché scatti la protezione dell'art. 14 Cost., non basta che un certo comportamento venga tenuto in luoghi di privata dimora; ma occorre, altresì, che esso avvenga in condizioni tali da renderlo tendenzialmente non visibile ai terzi» (Corte cost., 16 maggio 2008, n. 149); all'indirizzo secondo il quale le comunicazioni svolte attraverso ricetrasmittenti possono essere intercettate senza un previo decreto dell'autorità giudiziaria (per tutte, Cass., Sez. I, 20 maggio 1997, n. 5894, Bottaro ed altri, in *C.e.d.*, n. 207931 — 01); sono, tutte, prese di posizione riconducibili ad un'idea analoga alla *third party doctrine*.

⁵¹ B. TURNER, *When Big Data Meets Big Brother*, cit., p. 38, 425 e p. 433 s.

Riflessioni analoghe in A. BIANCHINI, *Always On, Always Listening*, cit., p. 4 s.; M.M. CHRISTOVICH, *Why Should We Care*, cit., p. 95 s.; C. DEL ROSSO, C.M. BAST, *Protecting Online Privacy*, cit., p. 91 s.; A.E. DRAFT, *Pacemakers, Fitbits, and the fourth amendment: privacy implications for medical implants and wearable technology*, 2019 *Mich. St. L. Rev.* 511, p. 531 s.; I. FRIEDLAND, *Drinking from the Fire Hose*, cit., p. 909 s.; E. HABER, *The Wiretapping of things*, cit., p. 757; M. TOKSON, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 *Harv. L. Rev.* 1790 (2022), p. 1791 s.

Per un'appassionata difesa della *third party doctrine* v. tuttavia O. KERR, *The Case for the Third-Party Doctrine*, 107 *Mich. Law Rev.* 561 (2009).

⁵² Così N. GORSUCH, nella *dissenting opinion* a *Carpenter v. United States*, 585 U.S. 296 (2018).

può essere utile un telegrafico ragguaglio tecnico su quelli che più frequentemente sono adoperati nel processo, i *fitness trackers*.

I sensori di cui sono dotati — accelerometri, giroscopi, barometri, altimetri, termometri... — traducono fenomeni fisici come movimento, pressione, posizione, altitudine, temperatura in informazioni digitali⁵³. I dati vengono temporaneamente stivati all'interno degli apparecchi ma sono destinati ad essere sovrascritti in tempi abbastanza rapidi (qualche giorno)⁵⁴, perché di solito i *wearables* hanno una memoria ridotta⁵⁵.

I dispositivi indossabili sono progettati per essere usati in combinazione con app installate su *smartphones* e con siti web; di solito, sfruttando il *bluetooth*, una rete *wi-fi* o un cavo⁵⁶, scaricano i dati sull'app che a sua volta li riversa nel *cloud*⁵⁷; ma esistono anche modelli che non passano attraverso l'app. Nel *cloud* le informazioni vengono conservate, analizzate, elaborate, raggruppate in grafici; l'utente può controllare il suo profilo e prendere conoscenza delle sue abitudini e dei suoi miglioramenti (o fallimenti) e ricevere suggerimenti forniti da esperti di fitness e nutrizione⁵⁸. Non è raro che i dati siano volontariamente postati anche in siti ulteriori, per esempio quelli che raggruppano consumatori con gli stessi interessi: ciclisti, runner e così via.

Questi cenni sono sufficienti per introdurre un tema sul quale dovremo tornare. L'importanza dei valori incisi vorrebbe che la normativa sull'acquisizione processuale dei dati raccolti dai dispositivi indossabili fosse chiara, pensata, unitaria. Al momento non è così: i dati possono essere in molti luoghi (fisici o virtuali): nel *wearable*, nello *smartphone* associato al *wearable*, nel *cloud*, o anche in viaggio fra l'uno e l'altro di questi luoghi⁵⁹; e la disciplina che ne regola l'acquisizione cambia ogni volta, a seconda della fonte da cui la prova viene ricavata.

⁵³ S.R. PEPPET, *Regulating the Internet of Things*, cit., p. 98; v. anche A.H. RAYMOND, S.J. SHACKELFORD, *Jury glasses: wearable technology and its role in crowdsourcing justice*, 17 *Cardozo J. Conflict Resol.* 115, (2015), p. 121.

⁵⁴ Per esempio, i modelli più diffusi di Fitbit contengono informazioni dettagliate degli ultimi sette giorni e, per gli apparecchi di fascia più alta, i totali giornalieri dell'ultimo mese: cfr. N. CHANDLER, *How FitBit Works*, cit.; W. KENDALL, "Outrunning" the fourth amendment: a functional approach to searches of wearable fitness tracking devices, 43 *S. Ill. U. L. J.* 333 (2019), p. 336 s.

⁵⁵ K. SAPHNER, *You Should Be Free to Talk the Talk*, cit., p. 1717.

⁵⁶ M. ASHTON, *Debugging the real world*, cit., p. 808; M. SWAN, *Sensor Mania*, cit., p. 220.

⁵⁷ J. EVANS, K. RINGROSE, *From Fitbits to Pacemakers: Protecting Consumer Privacy and Security in the Healthtech Age*, 68 *Clev. St. L. Rev. Et Cetera* 1 (2019), p. 2.

⁵⁸ J. KANG, K. SHILTON, D. ESTRIN, J. BURKE, M. HANSEN, *Self-surveillance Privacy*, cit., p. 813 s.

⁵⁹ F. NICOLAI-M.H. MARAS-J. TRAUTMANN-J. SCHNEIDER, *When objects betray you*, cit., p. 17 s.

5. *Lo smart watch come testimone*

Di solito gli strumenti e le tecniche che da un lato si mostrano pericolosi per il diritto alla riservatezza, dall'altro si rivelano preziosi per l'indagine penale: i *wearables* non fanno eccezione⁶⁰.

La prima volta che un *fitness tracker* viene usato in un'aula di giustizia è nel 2014, in Canada, in un processo civile: una giovane donna rimasta ferita in un incidente si rivolge ad uno studio legale; per provare l'entità del danno subito, il difensore decide di adoperare il Fitbit della ragazza, il quale mostra che, a causa dell'incidente, il suo livello d'attività è inferiore a quello medio d'una donna della stessa età e professione⁶¹.

Pochi mesi dopo, i *wearables* entrano nel processo penale. Jeannine M. Risley, una signora americana, è a Lancaster per lavoro e passa la notte nella casa del suo capo, nell'ala riservata agli ospiti. Racconta alla polizia che un intruso s'è introdotto nell'abitazione, è entrato nella camera da letto dove lei dormiva, l'ha trascinato in bagno e violentato; durante la colluttazione, ha perso il suo Fitbit. L'apparecchio viene poi ritrovato dalla polizia in sala da pranzo; gli investigatori scaricano i dati e scoprono che la donna aveva camminato in giro tutta la notte e non era mai andata a dormire, come invece aveva sostenuto. Risley viene incriminata per «*false reports to law enforcement*» e chiude la vicenda con un *plea bargaining*⁶².

Da quel momento, è un'escalation. Le vicende più citate dai giuristi statunitensi sono il caso Compton e il caso Dabate. La casa di Ross Compton, cinquantanove anni, prende fuoco. Compton, che ha gravi problemi di salute, dice alla polizia che, non appena ha visto le fiamme, ha infilato alcuni effetti personali in una valigia e in qualche borsa, ha rotto con un bastone il vetro della finestra della sua camera da letto, ha scaraventato fuori borse e

⁶⁰ Cfr. A.G. FERGUSON, *The "Smart" Fourth Amendment*, 102 *Cornell Law Rev.* 547 (2017), p. 560 s.; N. SHAKOORY, *Wearables: your next trial witness?*, in *San Francisco Daily Journal*, 10 dicembre 2014.

⁶¹ Cfr. E.S. BROTTEN, *"Every Move You Make"*, cit.; N. CHAURIYE, *Wearable Devices as Admissible Evidence*, cit., p. 597; S. GIBBS, *Court sets legal precedent with evidence from Fitbit health tracker*, in *theguardian.com*, 18 novembre 2014; S. GRIFFITHS, *Fitbit data is now being used in COURT: Wearable technology is set to revolutionise personal injury and accident claims*, in *dailymail.co.uk*, 17 novembre 2014; P. OLSON, *Fitbit Data Now Being Used In The Courtroom*, in *forbes.com*, 17 novembre 2014.

⁶² Commonwealth v. Risley, Criminal Docket: CP-36-CR-0002937-2015.

Sul caso Risley si vedano N. CHAURIYE, *Wearable Devices as Admissible Evidence*, cit., p. 495 s.; C. COBLE, *Can Your Fitbit Data Be Used Against You in Court?*, in *findlaw.com*, 21 marzo 2019; M. MOON, *Fitbit tracking data comes up in another court case*, in *sg.news.yahoo.com/2015-06-28-fitbit-data-used-by-police.html*, 28 giugno 2015; M. SNYDER, *Police: Woman's fitness watch disproved rape report*, *abc27.com*, 19 giugno 2015.

valigia, è uscito dalla finestra, ha caricato tutto in macchina ed è scappato. La polizia ottiene un mandato per estrarre i dati memorizzati nel *pacemaker* di Compton. Un cardiologo li esamina e riferisce che era estremamente improbabile che Compton avesse davvero fatto tutto quel che aveva detto nel breve tempo che avrebbe avuto a disposizione. Compton viene accusato d'incendio doloso aggravato e frode assicurativa⁶³.

Richard Dabate racconta alla polizia che, dopo essere tornato a casa, ha dovuto affrontare un intruso; la moglie Connie, a sua volta, era rinca-sata durante lo scontro e l'intruso le ha sparato. Sennonché, il Fitbit di Connie racconta una storia diversa: la moglie è ancora viva quando, secondo Richard, sarebbe già stata uccisa da un pezzo. Richard Dabate verrà condannato per l'omicidio della moglie⁶⁴.

Come spesso capita quando si tratta d'usare nel processo penale nuovi ritrovati tecnologici⁶⁵, gli Stati Uniti aprono la strada, ma ben presto la tendenza contagia altri ordinamenti; dati estratti da *wearables* sono usati come prova in Germania⁶⁶, nel Regno Unito, in Australia⁶⁷; vengono usa-

⁶³ *Man's pacemaker data used against him in arson case*, in [cbsnews.com/news/mans-cardiac-pacemaker-data-led-to-arson-charges/](https://www.cbsnews.com/news/mans-cardiac-pacemaker-data-led-to-arson-charges/), 11 febbraio 2017; A.E. DRAFT, *Pacemakers, Fitbits, and the fourth amendment*, cit., p. 512; M.-H. MARAS, A.S. WANDT, *State of Ohio v. Ross Compton: Internet-enabled medical device data introduced as evidence of arson and insurance fraud*, 24 *Int. Journ. evid. proof* 321 (2020); M. REARDON, *Your Alexa and Fitbit can testify against you in court*, in [cnet.com/tech/mobile/alexa-fitbit-apple-watch-pacemaker-can-testify-against-you-in-court/](https://www.cnet.com/tech/mobile/alexa-fitbit-apple-watch-pacemaker-can-testify-against-you-in-court/), 5 aprile 2018.

⁶⁴ N. BLACK, *Fitbit data, other digital evidence used by prosecution in murder case*, in [legalnews.com](https://www.legalnews.com/), 29 maggio 2017; C. BRONDONI, *Smascherare un killer con il Fitbit*, [wired.it/articolo/fitbit-omicidio-prova-dabate/](https://www.wired.it/articolo/fitbit-omicidio-prova-dabate/), 4 agosto 2024; D. CASSENS WEISS, *Murdered woman's Fitbit data inconsistent with husband's story, police say*, in [abajournal.com](https://www.abajournal.com/), 25 aprile 2017; A. RODIS, *Fitbit data and the fourth amendment*, cit., p. 534 s.; D.A. STEIN, *The Fitbit Murder and Our New Digital Witnesses*, in [goldmandefense.com/fitbit-murder-new-digital-witnesses/](https://www.goldmandefense.com/fitbit-murder-new-digital-witnesses/); N. WETSMAN, *Behind the expert testimony in the "Fitbit murder" trial*, in [theverge.com](https://www.theverge.com/), 12 maggio 2022.

Il mandato d'arresto di Dabate è reperibile in documentcloud.org/documents/3678236-Dabate-Arrest-Warrant.html.

⁶⁵ A. CAMON, *Il cacciatore di Imsi*, in *Arch. pen.*, 2020, p. 177.

⁶⁶ In un'indagine per omicidio condotta verso la fine del 2016, le autorità sequestrano lo smartphone d'un sospettato; questi, secondo i dati di una app dell'apparecchio, poco dopo il delitto aveva fatto uno sforzo corrispondente a circa due rampe di scale; la polizia pensa che avesse trascinato il cadavere giù per un argine, l'avesse buttato nel fiume e fosse risalito. Allora un uomo della stessa corporatura, fornito d'un telefono analogo, ripete lo stesso stesso percorso, portando un peso sulle spalle; infine i dati registrati dall'app sono confrontati con quelli presi dal telefono sotto sequestro, per vedere se siano compatibili. Cfr. M. BURGESS, *From Fitbits to PlayStations, the justice system is drowning in digital evidence*, in [wired.co.uk](https://www.wired.co.uk/) (20 aprile 2018).

⁶⁷ Myrna Nilsson è assassinata a Adelaide, nel 2017. Secondo la nuora, è stata assalita da un gruppo di uomini in seguito ad un alterco nei pressi di casa, ma l'apple watch della vittima ne aveva registrato gli spostamenti, i consumi di calorie, il battito cardiaco, e i dati risultavano incompatibili con la successione temporale degli avvenimenti raccontata dalla

ti per incriminare e condannare, ma anche per scagionare⁶⁸. E fanno la loro comparsa anche nei palazzi di giustizia italiani. In una vicenda che ha attirato molto l'attenzione della stampa locale⁶⁹, un noto medico bolognese è accusato d'aver ucciso la moglie e la suocera; il suo Apple watch dimostrerebbe che, nelle notti dei due omicidi, aveva salito una rampa di scale: quella che separava il suo appartamento da quelli delle vittime. In primo grado il processo s'è concluso con una condanna all'ergastolo; nella sentenza, i dati estratti dall'app Salute dell'iPhone adoperato dall'imputato vengono considerati «uno dei riscontri più significativi a sostegno dell'ipotesi accusatoria»⁷⁰.

Pubblici ministeri e difensori di tutto il mondo si stanno accorgendo della miniera d'oro che si trova al polso delle parti processuali⁷¹; i *wearable* sono una «scatola nera del corpo umano»⁷², un esercito di piccole spie⁷³ pronte a testimoniare contro, o a favore, dei propri utenti⁷⁴.

Parte II — Intanto, in Europa

1. Tecnologia universale, soluzioni continentali

Gli Stati Uniti, dunque, stanno affrontando il cosiddetto *translation problem*⁷⁵. La grammatica del pubblico potere cristallizzata nella Costitu-

nuora, conducendo così all'incriminazione di quest'ultima. Cfr. R. JONES, *Apple Watch Health Data Is Being Used as Evidence in an Australian Murder Trial*, in gizmodo.com, 2 aprile 2018.

Una rassegna dei casi giudiziari più famosi in J.G. BROWNING-L. ANGELO, *The changing practice of law: Alexa, testify: new sources of evidence from the internet of things*, 2 Tex. B. J. 506 (2019).

⁶⁸ Cfr. J.G. BROWNING, *Technology and litigation practice: part II: using technology efficiently, ethically: "fit" to admit? Emerging sources of digital evidence*, 96 *The Advocate* 16 (2001); A. RODIS, *Fitbit data and the fourth amendment*, cit., p. 546 s.

⁶⁹ Cfr., per esempio, A. BACCARO-L. MULEO, *Giampaolo Amato, l'ex medico della Virtus incastato dallo smartwatch: «dormivo», l'orologio dice che era sveglio*, in corrieredibologna.corriere.it, 28 settembre 2023; G. CANÈ, *Quando lo smartwatch diventa la "prova" di un delitto: l'omicidio di Bologna e i casi precedenti*, in corriere.it, 28 settembre 2023; M. MADONIA, *Il medico Giampaolo Amato e la condanna all'ergastolo: «Per me vuol dire morire in carcere, non sono un mostro»*, corrieredibologna.corriere.it, 17 ottobre 2024.

⁷⁰ Trib. Bologna, 14 gennaio 2025, Amato, *inedita*, p. 90.

⁷¹ J.G. BROWNING, L. ANGELO, *The changing practice of law*, cit., p. 507.

⁷² E.S. BROTTEN, *Every Move You Make*, cit.

⁷³ A.G. FERGUSON, *The Internet of Things and the Fourth Amendment of Effects*, 104 *Cal. Law Rev.* 807 (2016), p. 818.

⁷⁴ P. AUGUSTINE, *Wearable Evidence: Why the Pennsylvania Judiciary Should Require a Warrant to Search Wearable Technology*, 17 *Journ. Techn. Law & Policy* (2017), tjp.law.pitt.edu/ojs/tjp/article/view/197, p. 2; A.N. KITCHEN, *Smart devices and criminal investigations*, cit., p. 12 e p. 45; K. SAPHNER, *You Should Be Free to Talk the Talk*, cit., p. 1691.

⁷⁵ L'efficace espressione è di M. WASHINGTON-N. RICHARDS, *Digital Civil Liberties and*

zione — con i suoi oltre 230 anni di storia — fatica a dettare regole per le nuove forme di interazione tra individuo e autorità: con l'avvento del digitale, la realtà si è messa a parlare anche un'altra lingua. Dall'altro lato dell'Atlantico, gli ordinamenti nazionali stanno affrontando dilemmi simili. Nonostante le costituzioni liberali siano più recenti del IV emendamento americano, soffrono spesso dello stesso limite: sono state pensate quando era fisicamente impossibile mettere le mani sui nudi dati. Tutt'al più, si poteva intervenire sulle loro fonti, che andavano protette da invadenze eccessive; l'attenzione si attestava così sulle persone, indagato in testa; sui luoghi dove si svolge la loro vita privata; sulle carte e sui canali con cui si scambiano messaggi⁷⁶.

Solo gli autori di fantascienza potevano immaginare un mondo in cui le informazioni non hanno né luogo né corpo: un mondo in cui è possibile leggere nel pensiero e in cui, quindi, è necessario proteggersi anche da un pericolo tanto subdolo⁷⁷. Non siamo in una situazione identica⁷⁸, ma probabilmente siamo più vicini a quegli scenari che non alla realtà che le costituzioni intendevano governare: le garanzie tradizionali, ancora attuali e necessarie per il mondo delle cose, sono strumenti imperfetti, se non inadeguati, per governare il digitale.

the Translation Problem, in D.K. BROWN-J. TURNER-B. WEISSER (a cura di), *The Oxford Handbook of Criminal Process*, Oxford University Press, Oxford, 2019, p. 365 ss., con interessanti riferimenti anche al tema dei riflessi che la telemedicina e i dispositivi indossabili hanno sull'accertamento penale.

Sul tema v. anche M. CAIANIELLO, *Criminal Process faced with the Challenges of Scientific and Technological Development*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 27 (2019), f. 4, p. 267-291.

⁷⁶ Da una premessa simile muove l'analisi di O.S. KERR, *The Digital Fourth Amendment*, Oxford University Press, Oxford, 2025.

⁷⁷ È la premessa narrativa di un romanzo che, non a caso, è oggi acclamato come un classico moderno: P.K. DICK, *Ubik* (1969), Mondadori, Milano, 2021. In un mondo dove esistono persone in grado di leggere la mente altrui, organizzati in agenzie di spionaggio, i protagonisti lavorano per una «agenzia prudenziale», cioè: un'azienda che assicura la riservatezza dei pensieri dei propri clienti grazie alle capacità dei propri impiegati, gli inerciali, anti-talenti in grado di azzerare il campo generato dai telepatti.

⁷⁸ Sebbene il Garante per la protezione dei dati personali italiano, in un'intervista, abbia utilizzato immagini non lontane: «alcuni smart watch idonei alla rilevazione biometrica [...] possono, poi, rivelare le reazioni emotive dell'utente alla visione di determinate immagini. Il controllo cui ci esponiamo può superare, dunque, persino la dimensione corporea e attingere al pensiero»: R. CORCELLA, *Dispositivi indossabili: i rischi per la privacy. Che fine fanno le informazioni raccolte?*, in *Corriere della Sera*, 4 marzo 2021. In termini appena meno allarmati: Gruppo di lavoro articolo 29 per la protezione dei dati, *Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti*, 16 settembre 2014, p. 5: «alcuni sviluppi dell'IoT, se incontrollati, possono spingersi fino a sviluppare una forma di sorveglianza delle persone [...] illegale ai sensi della legislazione dell'UE». Il documento considera espressamente i *wearable devices* alla pagina successiva.

Lo sfondo, insomma, è identico; su questa sponda dell’oceano, però, il ragionamento dei giuristi non può esserlo. L’ordinamento statunitense ha senza dubbio fatto da apripista: è quello che per primo ha dovuto fare i conti con l’evoluzione tecnologica ed è quindi naturale guardarlo come si guarda un faro: è e resta un punto di riferimento per chi cerca soluzioni⁷⁹. Ma se l’America innova, recita l’adagio, l’Europa regola: l’interprete continentale si trova di fronte a una trama forse fin troppo fitta di principi e regole a tutela della *privacy*.

Il punto di partenza ineludibile sono le Carte europee dei diritti, molto più flessibili o molto più recenti delle costituzioni nazionali. La Convenzione e.d.u., riconosce il diritto al rispetto della vita privata e familiare (art. 8 Conv. e.d.u.); la stessa tutela è accordata anche dalla piccola Europa, quanto alle sue aree di competenza, con la Carta di Nizza: l’art. 7 CDFUE protegge a sua volta la vita privata e familiare, il domicilio e le comunicazioni di «ogni persona». La disposizione più eloquente ai nostri fini è però l’art. 8 CDFUE, che conferisce a ogni individuo il diritto «alla protezione dei dati di carattere personale che lo riguardano».

L’affermazione di principio ha aperto un cantiere permanente cui lavorano insieme autorità indipendenti, istituzioni europee e parlamenti nazionali; insieme, hanno prodotto un ordito normativo che consta di numerosi regolamenti, direttive e linee guida: il primo testo, il più noto, è il Regolamento generale sulla protezione dei dati personali⁸⁰ (d’ora innanzi: GDPR), cui si sommano la direttiva “e-Privacy”⁸¹, il Regolamento sul

⁷⁹ L’argomento ritorna in molte analisi legate alla disciplina del capitalismo digitale e delle sue ripercussioni: anche in settori assai distanti dalla procedura penale, le opportunità e le spaccature create dalla tecnologia sono arrivate prima negli Stati Uniti e, quindi, sono state studiate (e, a volte, regolate) prima là; alcuni autori affermano che, per quanto si dia conto di un fenomeno «globale», l’anticipo americano «conduce inevitabilmente» al confronto tra «scenario giuridico statunitense» e i successivi «modelli europei»: A. LAS CASAS, *Il Data Act nello scenario del capitalismo dell’informazione: dai “dati personali” ai “dati”*, in V. BACHELET-G. MARINO-A. RACANO (a cura di), *Data Act. Accesso equo ai dati e loro utilizzo: profili sistematici e applicativi nell’orizzonte del diritto privato*, Wolters Kluwer, Milano, 2025, p. 4.

⁸⁰ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, entrato in vigore nel 2018.

⁸¹ Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, aggiornata nel 2009.

Il provvedimento appartiene alla generazione normativa precedente rispetto al GDPR e i rapporti tra i due non sono sempre chiari: v. CEPD, *Parere 5/2019 sull’interazione tra la direttiva e-Privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati*, versione 1.0, adottata il 28 gennaio 2020, disponibile alla pagina edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_en.

trattamento dei dati da parte delle istituzioni europee⁸², il Data act⁸³ e la cosiddetta ‘Law Enforcement Directive’ (LED), che stabilisce un quadro normativo sul trattamento dei dati «da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali»⁸⁴.

L’insieme di norme che riguarda più da vicino l’accertamento è senza dubbio l’ultimo che, insieme all’art. 8 Conv. e.d.u., si rivolge direttamente agli investigatori. Non dobbiamo però dimenticare che i dispositivi indossabili sono innanzi tutto prodotti disponibili sul mercato: la quantità e la qualità dei dati che gli inquirenti riescono a trarne dipendono dalle regole imposte ai produttori delle apparecchiature e ai fornitori dei servizi: come vedremo, l’intreccio avrà conseguenze dirette anche sulla qualità dell’accertamento. Conviene dunque ricostruire i tratti principali della disciplina, senza pretese di esaustività, sottolineando di volta in volta le previsioni più significative ai nostri fini⁸⁵. Per farlo, partiremo dai capisaldi stabiliti dal GDPR per il trattamento dei dati personali; passeremo infine alle cautele che l’art. 8 Conv. e.d.u. e la LED dettano alle forze dell’ordine.

2. *Liceità del trattamento e qualità del consenso*

Lo strumento normativo da cui conviene partire è il Regolamento generale sulla protezione dei dati, che costituisce l’architettura normativa di ogni forma di raccolta e lavorazione di informazioni personali. Esso

La Commissione ha presentato una proposta di regolamento per sostituire la direttiva *e-Privacy*, aggiornandola tanto al GDPR quanto all’avanzare della tecnologia: Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), 10 gennaio 2017 (COM/2017/010).

⁸² Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio del 23 ottobre 2018, cit.

⁸³ Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull’accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828, pienamente efficace a partire dal 12 settembre 2025.

⁸⁴ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

⁸⁵ Per un’analisi più completa, ma comunque rivolta al migliore esame del processo penale, v. I. NERONI REZENDE, *Criminal Justice and Data Protection. Communication Metadata under EU Human Rights Law*, Giappichelli-Routledge, Torino, 2026, p. 12 ss.

stabilisce innanzi tutto una serie di principi del trattamento, cui si affianca una lista di diritti dell'individuo.

Partiamo dei primi, elencati dall'art. 5 GDPR e approfonditi dalle disposizioni successive⁸⁶: essi dispongono che i dati personali devono essere gestiti «in modo lecito, corretto e trasparente nei confronti dell'interessato» (art. 5 n. 1 GDPR). Le condizioni di liceità del trattamento sono meglio illustrate dall'articolo seguente: la prima, senz'altro la più importante, è il consenso dell'interessato, e abbiamo già visto che questa legittimazione può essere più fragile di come appare⁸⁷. Specie in un'infrastruttura digitale complessa, che prevede l'interazione tra diversi dispositivi (indossabili, *smart-phone*, archivi dei *data center*), varie applicazioni e piattaforme, è facile perdere l'orientamento: mappare i sentieri percorsi dai dati è difficile, così come non è immediato comprendere cosa viene rilevato, né quali informazioni può svelare quel materiale. Prima che entrasse in vigore il GDPR, il predecessore del Comitato europeo per la protezione dei dati personali aveva suonato un campanello d'allarme: in un simile campo da gioco, il rischio è quello di accontentarsi di un consenso «di bassa qualità»⁸⁸, un benessere di facciata che di fatto sposta l'autonomia decisionale e il controllo dei dati dall'utente all'azienda digitale⁸⁹. Non l'espressione di una vera scelta, insomma, ma una “foglia di fico” cibernetica.

Consapevole dei rischi, il Regolamento ha provato almeno ad arginarli. Il ‘consenso dell'interessato’, secondo l'art. 4 n. 11 GDPR, deve essere specifico, inequivoco, informato e consapevole: in altre parole, l'utente deve avere la possibilità di autodeterminarsi⁹⁰, di prendere scelte

⁸⁶ L'elencazione qui svolta non è completa: per ragioni di spazio, ci limitiamo a citare i principi generali che avranno un ruolo nella trattazione successiva. Per un'analisi puntuale v. C. KUNER-L.A. BYGRAVE-C. DOCKSEY-L. DRECHSLER (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, e in particolare il contributo di C. DE TERWAGNE, *Article 5. Principles relating to processing of personal data*, *ibidem*, p. 309 ss.

Nel panorama italiano, è indispensabile la consultazione di G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

⁸⁷ V. *retro*, Parte I, § 3.

⁸⁸ Gruppo di lavoro articolo 29 per la protezione dei dati, *Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti*, 16 settembre 2014, disponibile alla pagina ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_it.pdf, p. 8.

⁸⁹ A questo riguardo, alcuni autori si spingono a parlare di “post-consent regime”: M. WANG, *The Quantified Body: Identity, Empowerment and Control in Smart Wearables*, in *ArXiv pre-print* n. arXiv:2506.15991, 19 giugno 2025, p. 2.

⁹⁰ Il lessico euronunitario deve molto alla pionieristica elaborazione della *Informationel-*

meditate su di sé e sulla condivisione delle informazioni che lo riguardano. Di più: per essere libera, la volontà del soggetto deve potersi formare senza timore di conseguenze negative; come ha precisato il Comitato europeo per la protezione dei dati, «il consenso può costituire la base legittima appropriata solo se all'interessato vengono offerti il controllo e l'effettiva possibilità di scegliere se accettare i termini proposti o rifiutarli senza subire pregiudizio»⁹¹; se mancassero tali requisiti, il trattamento sarebbe illegittimo. In termini ancora più diretti, «[il consenso] è valido soltanto se l'interessato è in grado di operare realmente una scelta e non c'è il rischio di raggiri, intimidazioni, coercizioni o conseguenze negative significative (ad es. costi aggiuntivi sostanziali) in caso di rifiuto»⁹².

Le cautele sono ancora più intense per i dati che appartengono a «categorie particolari», che l'art. 9 GDPR individua. Si tratta di informazioni capaci di svelare «l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale», nonché i «dati genetici, dati biometrici [...], dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona» (art. 9 comma 1 GDPR). Sono elementi assai sensibili, che riguardano aspetti personalissimi della vita di un individuo: perciò, in linea di massima, il loro trattamento è vietato. Gli indossabili ne prelevano a iosa: lo *smartwatch* magari non rileva dati biometrici in senso stretto⁹³ — quelli, cioè, che consentono di identifica-

le *Selbstbestimmung*: il diritto all'autodeterminazione informativa postulato prima dalla dottrina tedesca e poi affermato dalla Corte costituzionale tedesca come un corollario della dignità umana: BVerG, I senato, 15 dicembre 1983, 1 BvR 209/83, § 146 ss. Per un approfondimento dogmatico v. K.M. LINZBACH, *Additiver Grundrechtseingriff und informationelle Selbstbestimmung. Grundrechtsdogmatik als Legitimationsproblem*, Mohr Siebeck, Tübingen, 2025.

⁹¹ CEPD, *Linee-guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, versione 1.1, adottate il 4 maggio 2020, p. 5, disponibili alla pagina edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_it.

⁹² *Ivi*, p. 10. Lo stesso Comitato ha avuto modo di ribadire questi principi con forza proprio riguardo alle interazioni tra individui e grandi piattaforme digitali che offrono al consumatore una scelta apparente: acconsentire alla pubblicità comportamentale o pagare un abbonamento: CEPD, *Parere 8/2024 sul consenso valido nel contesto dei modelli "consenso o pagamento" attuati dalle piattaforme online di grandi dimensioni*, 17 aprile 2024, p. 19 ss., disponibile alla pagina: edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en.

⁹³ Anche se esistono tanto forme di riconoscimento dell'andatura (v. per esempio C. ÁLVAREZ-APARICIO-A. GUERRERO-HIGUERAS-M.A. GONZÁLEZ-SANTAMARTA-A. CAMPAS-VEGA-V. MATELLÁN-C. FERNÁNDEZ-LLAMAS, *Biometric recognition through gait analysis*, in *Nature — Scientific reports*, 2022, 12, n. 14530), quanto metodi di individuazione univoca che sfruttano il ritmo cardiaco: il considerando n. 15 del AI Act li menziona entrambi come forme di «identificazione biometrica». Questi ultimi metodi, detti di *internal biometrics*, dovrebbero essere esatti e difficili da ingannare: se il viso può essere riprodotto così accuratamente da indurre in errore i sistemi di riconoscimento automatico, il battito del cuore è meno esposto. Sarebbe molto più complesso falsificarlo con precisione. Sul tema V. A.R.J. MITCHELL-D. AH-

re univocamente una persona — ma di certo produce informazioni relative alla salute del soggetto che indossa l'apparecchio⁹⁴. Anche a loro, quindi, si applica il divieto stabilito dall'art. 9 GDPR⁹⁵.

Il testo elenca poi le circostanze capaci di far cadere lo sbarramento e giustificare l'elaborazione di ciò che si trova all'interno delle classi protette: il fatto che l'interessato renda i dati «manifestamente pubblici» (art. 9 comma 2 lett. *e* GDPR), per esempio, elimina la restrizione, così come il consenso esplicito dell'interessato, per una o più finalità specificate (art. 9 comma 2 lett. *a* GDPR); l'accordo del soggetto, qui, presenta requisiti più stringenti: è, insomma, un requisito diverso da quello previsto dall'art. 6 GDPR, tanto che, per trattare le informazioni “sensibili”, occorre una nuova manifestazione di volontà.

La tutela dell'individuo è rafforzata anche tramite modalità più sottili e pragmatiche: l'art. 25 GDPR è intervenuto sul sistema in modo da rendere praticamente ineludibile l'intervento dell'utente. La disposizione detta infatti due standard ai produttori e ai programmatori dei dispositivi riassunti negli slogan *privacy by design* e *privacy by default*. Sin dalla progettazione degli apparecchi, occorre predisporre le «misure tecniche e organizzative adeguate [...] ad attuare in modo efficace i principi di protezione dei dati [...] e a integrare nel trattamento le necessarie garanzie» (art. 25 comma 1 GDPR). Insomma: il costruttore non può mettere a punto un apparecchio, metterlo sul mercato e preoccuparsi dopo di come quello raccoglie e tratta i dati personali. Lo stesso principio si applica ai *software* e al *pre-set* del dispositivo: le impostazioni predefinite devono essere congegnate in modo tale da impedire accessi ai dati non espressamente autoriz-

LERT-C. BROWN-M. BIRGE-A. GIBBS, *Electrocardiogram-based biometrics for user identification – Using your heartbeat as a digital key*, in *Journal of Electrocardiology*, 80 (2023), p. 1 ss.; per una rassegna dei metodi e delle tecnologie impiegate a questi fini v. D. MELTZER-D. LUENGO, *ECG-Based Biometric Recognition: A Survey of Methods and Databases*, in *Sensors*, 2025, doi: 10.3390/s25061864. Il programma di trasferimento tecnologico della NASA ha registrato almeno due brevetti sulla biometria basata sull'elettrocardiogramma: un programma, HeartBeatID, che considera oltre 190 parametri statistici per identificare univocamente una persona a partire dal battito (la scheda si trova alla pagina: technology.nasa.gov/patent/top2-186); e un sensore capace di rilevare i dati che servono (la scheda si trova alla pagina: technology.nasa.gov/patent/TOP2-202). A quanto risulta, però, non esistono al momento applicazioni capaci di sfruttare il dispositivo indossabile commerciale a fini di identificazione biometrica.

⁹⁴ In questo senso v. Commissione europea, Direzione generale per la salute e la sicurezza alimentare, *Assessment of the EU Member States' rules on health data in the light of GDPR*, 12 febbraio 2021, disponibile alla pagina health.ec.europa.eu/publications/assessment-eu-member-states-rules-health-data-light-gdpr_en, p. 14 e p. 190.

⁹⁵ Secondo alcuni è una proiezione moderna del segreto professionale cui il medico è sempre stato tenuto: L.A. BYGRAVE-L. TOSONI, *Art. 4 (15). Data concerning health*, in C. KUNER-L.A. BYGRAVE-C. DOCKSEY-L. DRECHSLER (a cura di), *The EU General Data Protection Regulation (GDPR)*, cit., p. 218 s.

zati. Inoltre, il produttore deve limitare le opzioni di *default* alla raccolta delle sole informazioni che servono, trattenerle per il tempo strettamente necessario e trattarle solo per finalità legittime, specifiche ed esplicite⁹⁶. Il dispositivo deve essere pensato per funzionare al meglio, con il minimo impatto possibile sulla riservatezza⁹⁷. Ogni deviazione dal modello deve raccogliere l'adesione libera ed esplicita del soggetto, compiutamente informato e protetto da eventuali ritorsioni: il consenso, ancora una volta, diventa il principale «argine rispetto al rischio di un uso secondario dei dati» poiché con esso è «il consumatore a definire il perimetro del trattamento, vietando *ex ante* forme d'indebito sfruttamento dei propri dati»⁹⁸. In Europa, quindi, la mancata modifica delle impostazioni predefinite non basterebbe a legittimare il trattamento di dati né tantomeno la loro pubblicazione; il produttore non potrebbe nascondersi dietro a un consenso presunto, né dietro ragioni economiche o di funzionalità del sistema: il diritto alla *privacy* viene prima.

Non tutti i produttori sembrano adeguarsi volentieri al quadro che abbiamo tracciato: Fitbit è stato recentemente denunciato a tre Garanti nazionali — quello italiano, austriaco e olandese — da un'associazione di attivisti per il rispetto del diritto alla riservatezza. Stando agli attori, sarebbe impossibile registrare un profilo e accedere alle funzionalità del dispositivo senza autorizzare espressamente il trasferimento dei propri dati fuori dall'Unione europea: barrare la casella con cui si acconsente all'operazione è una condizione necessaria per proseguire nell'apertura dell'*account*, che è necessario per fruire del prodotto. In altre parole, l'impresa porrebbe il consumatore davanti a una scelta: usare il braccialetto e rinunciare alle tutele offerte dal GDPR, o non usarlo affatto. L'unico modo offerto dal sistema per revocare il proprio consenso sarebbe la cancellazione del profilo; le cose non andrebbero meglio nemmeno per gli abbonati ai servizi premium: anche per loro, la sola possibilità di mantenere intatte le garanzie del diritto alla riservatezza consisterebbe nell'uscire dal sistema e rendere effettivamente inutile il *tracker* acquistato⁹⁹.

⁹⁶ Approfondiremo tutte le espressioni al § successivo.

⁹⁷ Per ulteriori specificazioni ed esempi v. CEPD, *Linee guida 4/2019 sull'articolo 25. Protezione dei dati fin dalla progettazione e per impostazione predefinita*, Versione 2.0, 20 ottobre 2020, disponibili alla pagina edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and-it

⁹⁸ Commissione parlamentare d'inchiesta sulla tutela dei consumatori e degli utenti, Audizione del Presidente del Garante per la protezione dei dati personali del 16 febbraio 2022. La trascrizione integrale è disponibile alla pagina garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9745988.

⁹⁹ Per una scheda di sintesi delle accuse e per gli atti depositati presso i diversi uffici

La strategia dell'azienda, per come descritta, pare a suo modo lineare: di fatto, il produttore si assicura così tre diverse fonti di profitto. La prima consiste nella vendita dei dispositivi, che promette un incasso relativamente basso e, soprattutto, occasionale; la seconda deriva dagli abbonamenti premium, che generano un flusso di entrate più stabile ma comunque non astronomico. L'ultima, maggiore di diversi ordini di grandezza, deriva dalla vendita dei dati a terze parti — per esempio: ad agenzie pubblicitarie, o a data base di informazioni anonimizzate e poi vendute a ricercatori. Sarebbe tutto regolare, se l'utente fosse messo nelle condizioni di scegliere consapevolmente se autorizzare tale sfruttamento economico e starà al Garante irlandese, cui sono state trasmesse le segnalazioni per competenza, decidere se l'assetto attuale rispetta il requisito oppure no. La decisione pare destinata a dettare specifiche importanti per tutta l'industria: se le lamentele degli attivisti fossero accolte, la principale sorgente di introiti prevista dal modello imprenditoriale sarebbe messa a rischio; la sua sostenibilità economica, di conseguenza, potrebbe uscirne incrinata.

Il braccio di ferro tra attivisti e giganti del digitale pare utile per riflettere su un aspetto: per quanto criticato, il consenso “di alta qualità” costituisce comunque una garanzia sufficientemente robusta da meritare tentativi di elusione; altrove, come abbiamo visto, non esiste o quasi. Certo, la sua forza è difficile da determinare sulla carta: è direttamente proporzionale alla consapevolezza nell'uso dei dispositivi, alla conoscenza (pur sommaria) dei modelli di impresa digitale, alla educazione della cittadinanza quanto ai diritti e ai rischi legati alla condivisione bulimica di dati personali.

3. Segue. *La limitazione delle finalità e la minimizzazione dei dati*

Un altro dei cardini del trattamento riguarda gli scopi per cui i dati sono raccolti, scopi che devono essere espliciti e determinati: occorre insomma spiegare al soggetto perché si registrano quelle informazioni e a che uso saranno destinate. D'un verso, il principio è legato a doppio filo al requisito della lealtà e della legalità: non può essere “di alta qualità” il consenso espresso a scatola chiusa, senza che l'utente sappia a quale scopo verranno usate le informazioni. D'altro canto, la chiara affermazione dell'obiettivo è essenziale anche per tutte le altre cause di legittimazione del trattamento; l'oggetto del contratto disegna il confine del lecito: si

v. *Your Fitbit is useless – unless you consent to unlawful data sharing*, 31 agosto 2023, disponibile alla pagina noyb.eu/en/your-fitbit-useless-unless-you-consent-unlawful-data-sharing.

può raccogliere senz'altro quanto è strettamente necessario per l'adempimento della obbligazione stabilita; specifiche norme di legge possono autorizzare la cernita di informazioni a prescindere dalle scelte del singolo, ma solo per raggiungere la meta stabilita dalla norma. Per tutto ciò che va oltre, si dovrà cercare una diversa legittimazione: un nuovo assenso dell'utente; un altro contratto; un'altra norma e così via.

Sul terreno che ci riguarda, l'impianto normativo ha risvolti pratici di non poco momento. Come abbiamo visto, molti dispositivi indossabili connessi puntano a sostituire accessori di uso comune come l'orologio da polso. Almeno la funzione base, quella assolta anche dall'oggetto non connesso, dovrebbe essere disponibile anche a chi non volesse acconsentire al trattamento dei propri dati: in altre parole, chi acquista uno *smart watch* dovrebbe poter leggere l'ora senza essere costretto ad autorizzare la raccolta e la trasmissione dei propri dati. Tutto ciò che si colloca oltre l'uso più elementare dell'apparecchio dovrebbe essere attivato dall'individuo, che dovrebbe poter scegliere per quali ulteriori finalità autorizzare la raccolta. Una linea guida, pur datata, si spinge fino a teorizzare il diritto di accendere e spegnere ciascun sensore a seconda delle scelte dell'utente secondo il principio della granularità del consenso: la consapevolezza del soggetto e la sua espressione di volontà dovrebbe estendersi a ciascuna funzionalità degli apparecchi¹⁰⁰. Realizzare appieno tale direttiva sarebbe probabilmente difficile dal punto di vista tecnico; in alternativa, si è proposto di prevedere un pulsante capace di mettere *offline* tutte le funzioni aggiuntive dell'apparecchio: una sorta di "modalità aereo" che molti dispositivi oggi contemplano. Il soggetto, insomma, dovrebbe essere in grado di decidere quando produrre dati e a quale fine autorizzare la loro elaborazione. Il mercato degli indossabili magari non rispetta tali requisiti alla lettera: la possibilità di "staccare la spina" a ciascuna unità di rilevazione non è diffusa: in altri termini, non è detto che l'utente riesca a decidere quali dati vengono prodotti; può però scegliere quali dati trasmettere selezionando le funzionalità. Per esempio, la *privacy policy* che Apple ha dettato per la app 'Salute' descrive tutti i servizi che il *software* è in grado di offrire — può tracciare il sonno, il ciclo mestruale, gli stati mentali, i farmaci da assumere e altro ancora — grazie ai dati carpiati dall'orologio connesso e alle informazioni volontariamente introdotte dall'utente. Il documento precisa inoltre che ogni funzione può essere selezionata o deselezionata in ogni momento: se l'interessato non volesse più raccogliere dati sul proprio battito cardiaco, potrebbe entrare nella app e

¹⁰⁰ Gruppo di lavoro articolo 29 per la protezione dei dati, *Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti*, cit., p. 22 s.

smettere di rilevare l'informazione¹⁰¹. Nulla ci assicura che il sensore sarà effettivamente spento; il telefono, però, interromperà la cernita; anche se esistesse, il materiale andrebbe perso.

Il principio di limitazione della funzione comporta poi due importanti corollari: costituisce il cardine attorno al quale bisogna organizzare il trattamento, che può legittimamente riguardare solo la quantità di dati che è necessaria e sufficiente per raggiungere lo scopo; non può e non deve estendersi oltre. Il precetto, noto come 'principio di minimizzazione dei dati', ha anche un versante temporale: le informazioni raccolte devono essere conservate per il lasso di tempo che serve a realizzare il fine dichiarato e illustrato all'individuo.

Ancora una volta, da questo insieme di regole derivano istruzioni assai concrete per i produttori di indossabili. Una modalità operativa che consente di rispettare i precetti e, al tempo stesso, di ottimizzare le prestazioni dei dispositivi consiste nel trasmettere e archiviare i soli dati aggregati e cancellare quelli grezzi da cui l'informazione è estratta. Un esempio aiuterà a chiarire il discorso: tra i sensori più diffusi ci sono l'accelerometro e il giroscopio, in grado di rilevare rispettivamente l'accelerazione, insieme alla direzione, e la velocità di rotazione. I dati captati direttamente dai sensori, a seconda di come sono elaborati, possono fornire una miriade di informazioni diverse: dallo stile di guida di chi indossa il dispositivo — cosa che potrebbe interessare molto a una compagnia di assicurazioni; al numero di passi percorsi durante una camminata o durante un allenamento; ad attività del soggetto come fumare o mangiarsi le unghie, normalmente collegate al livello di stress o di noia e, quindi, allo stato di benessere psicologico del soggetto¹⁰². Le semplici rilevazioni dell'apparecchio, insomma, possono dire moltissimo: basta interrogarle con algoritmi diversi, capaci di mettere insieme i frammenti che servono per arrivare a un determinato risultato conoscitivo. Una volta arrivati all'informazione desiderata, però, è praticamente impossibile tornare indietro: dalle tracce dei sensori si può calcolare indifferentemente il numero di passi o il numero di sigarette che la persona ha fumato; dal numero di passi, invece, non si può procedere a ritroso per tornare ai dati grezzi e, quindi, grazie a una nuova elaborazione, al numero di sigarette. Per questo è importante che le tracce grezze vengano diffuse il meno possibile: se queste

¹⁰¹ La *privacy policy* qui descritta è consultabile alla pagina: apple.com/legal/privacy/data/en/health-app.

¹⁰² S. QUADIR-N.S. KAHN-G. ANJUM-N. UDDIN, *A wearable sensors dataset for stress & boredom associated activity recognition*, in *Data in Brief*, 54 (2024), n. 110550, doi: 10.1016/j.dib.2024.110550.

venissero regolarmente trasmesse e stoccate, sarebbe molto più difficile garantire la riservatezza. Per evitare tali pericoli, la maggior parte degli indossabili le lavorano direttamente sul dispositivo, in modo da trasmettere e archiviare soltanto l'esito, che varia al variare della funzione commerciale dell'oggetto: si tratterà del numero di passi per un *fitness tracker* o del numero di sigarette fumate per il bracciale che fulmina i disobbedienti. I dati grezzi prodotti dal sensore vengono di norma eliminati, sovrascritti nel giro di poche ore: di loro non c'è più bisogno, anzi: conservarli avrebbe delle controindicazioni, e non solo sul piano giuridico. Il volume di materiale prodotto dai sensori sarebbe esorbitante: se tutti i telefoni, tutti gli orologi e tutti gli anelli caricassero tutti i dati prodotti, lo spazio sarebbe ben presto insufficiente. Inoltre, le informazioni sarebbero difficili da proteggere: i protocolli di sicurezza degli indossabili, di norma, non sono esattamente inespugnabili; intromettersi nel dialogo tra dispositivi ed esfiltrare dati non sarebbe troppo difficile per eventuali malintenzionati¹⁰³. Per tutte queste ragioni, quindi, i dati aggregati sono trasmessi e salvati senza conservare quelli grezzi, e dal punto di vista del diritto alla riservatezza, è una soluzione quasi perfetta¹⁰⁴, ma getta i semi da cui na-

¹⁰³ La potenza di calcolo e la batteria di un dispositivo così piccolo non sono in grado di eseguire protocolli crittografici troppo complessi: le comunicazioni tra l'indossabile e il dispositivo "madre" (normalmente: lo *smart phone*) sono tendenzialmente vulnerabili; una delle migliori difese, quindi, consiste nel non raccogliere ciò che non si vuole perdere. Un esempio di questa dinamica è offerto dalla cronaca recente. Secondo un giornalista d'inchiesta, dati particolarmente sensibili sarebbero stati rubati o venduti da un'azienda che produce un peculiare dispositivo indossabile: una fascia da posizionare intorno alla fronte per rilevare onde cerebrali così da ottenere informazioni su come allenare sia la concentrazione, sia il rilassamento. Lo strumento è diventato particolarmente popolare tra gli atleti professionisti, che sarebbero state le vittime della fuga di notizie: lo scoop sostiene infatti che il governo cinese avrebbe ottenuto i dati prodotti dal monitoraggio delle attività cerebrali di sportivi di primo piano, come Jannik Sinner e Charles Leclerc, e li avrebbe utilizzati nel tentativo di addestrare soldati o robot (v. S. RIGGIO, *Sinner e Leclerc al centro di un'accusa di spionaggio: «La Cina ruba i dati sul loro cervello raccolti con la "bandana" elettronica»*, in *Corriere della sera* (web), 19 settembre 2025). L'impresa si è subito difesa con un comunicato molto asciutto che, per prima cosa, chiarisce che «nessuno dei prodotti [...] trasmette dati biometrici grezzi ai nostri server. Le applicazioni elaborano i segnali [...] localmente sul dispositivo dell'utente e [tali informazioni] sono automaticamente eliminate a ogni uso»: FocusCalm, *Official statement*, consultabile alla pagina focuscalm.com.

¹⁰⁴ Gruppo di lavoro articolo 29 per la protezione dei dati, *Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti*, cit., p. 21 ss. lamentava per verità una violazione del diritto dell'interessato ad accedere ai dati, già garantito dall'art. 15 GDPR e oggi notevolmente rafforzato dall'entrata in vigore del Data Act. Il mutamento del quadro normativo, ad ogni modo, non dovrebbe modificare significativamente le conclusioni cui siamo giunti: il Data Act obbliga il produttore a condividere con l'utente tutto il materiale generato dai dispositivi «con la stessa qualità di cui [ne] dispone» (art. 4 comma 1 Data Act): il *data holder* è tenuto a dare accesso a tutto ciò che ha raccolto, non a ciò che non ha. Il testo,

scono le questioni più spinose per l'uso di quelle informazioni nel processo penale: le affronteremo a tempo debito¹⁰⁵.

4. *E le forze dell'ordine? L'art. 8 Conv. e.d.u.*

Arriviamo al cuore del problema che ci riguarda. Il fiume di informazioni prodotto dai sensori non nasce per aiutare gli investigatori a gettar luce sull'accaduto, anzi: come abbiamo visto, scorre in un alveo ben definito, scandito da briglie e serramenti tutti volti a limitare la raccolta dei dati sulla base della funzione commerciale da assolvere. Eppure può costituire una fonte preziosa anche ai fini dell'indagine penale: il dispositivo può dare indicazioni utili sull'orario della morte di chi lo indossava; può offrire una quantificazione più o meno approssimativa delle distanze percorse; può mostrare le calorie consumate o il battito cardiaco... può perfino lanciare l'allarme e chiamare i soccorsi in autonomia dopo una caduta traumatica¹⁰⁶. Giova ripeterlo: non sono dati formati nel corso di un'indagine, in esecuzione di una misura di sorveglianza occulta del sospettato. Al monitoraggio, qui, le persone si sono sottoposte volontariamente, pur ad altri fini: i dati sono formati, raccolti e archiviati fuori dal processo, secondo norme che nulla hanno a che vedere con l'accertamento. Quali mezzi di tutela della riservatezza si possono quindi far valere su questo terreno, storicamente connotato da un interesse pubblico schiacciante?

Come abbiamo anticipato, i punti di riferimento principali sono due. Un primo scudo è offerto dall'art. 8 Conv. e.d.u., che protegge la «vita privata e familiare» dalle intrusioni arbitrarie delle autorità, qualsiasi forma esse assumano. Grazie a tale flessibilità, la Corte di Strasburgo si è espressa su un catalogo impressionante di misure: dalle perquisizioni al riconoscimento facciale.

Le interferenze sono valutate con un vaglio che si fa più o meno esigente a seconda dell'intromissione denunciata: più profonda è la limitazione, più severo è lo scrutinio sulle garanzie, sulle procedure e sui rimedi previsti dagli ordinamenti nazionali per evitare che il diritto non sia ecces-

insomma, sembra imporre alle imprese digitali un obbligo di trasparenza, e non invece l'allargamento della collezione di dati. È ancora presto per sapere come verranno interpretate le disposizioni, pienamente applicabili dal 13 settembre 2025. A giudicare dal tenore letterale, sembra però che la soluzione descritta nel testo sia destinata a rimanere ferma. Nello stesso senso, in dottrina, N. SCANDELLI, *Prodotti connessi e dati generati: profili tecnologici*, in V. BACHELET-G. MARINO-A. RACANO, *Data Act*, cit., p. 78.

¹⁰⁵ V. *I wearables nel processo italiano*, in *questo volume*, § 3.

¹⁰⁶ V. A. LANA, *Smartwatch gli salva la vita: chiama i soccorsi mentre lui è incosciente*, in *corriere.it*, 22 settembre 2019.

sivamente compresso. Non è questa la sede per ripercorrere la giurisprudenza della Corte e.d.u. sull'art. 8 in tutte le sue pieghe¹⁰⁷; possiamo però riassumere il metodo che adotta nella valutazione di quei profili. Nel corso degli anni, infatti, i giudici di Strasburgo hanno elaborato veri e propri "test": schemi capaci di scomporre il loro ragionamento in passaggi successivi, riproposti in modo tendenzialmente omogeneo. Ci sarà utile esaminare brevemente quello applicato in materia di tutela dei dati, anche perché sarà una guida preziosa nell'esame della legislazione italiana e nella lettura delle evoluzioni più recenti¹⁰⁸.

Il palinsesto ricalca le previsioni dell'art. 8 comma 2 Conv. e.d.u. e si divide in tre passaggi: l'ingerenza deve essere «prevista dalla legge»; deve perseguire un fine legittimo e deve essere «necessaria» in una «società democratica».

Il primo segmento consiste in un'analisi approfondita del quadro normativo nazionale¹⁰⁹. I giudici di Strasburgo non si limitano a prendere atto dell'esistenza di una legge interna che prevede determinati poteri, ma esaminano la qualità delle disposizioni sotto diversi profili. Innanzi tutto, l'ordinamento deve sottrarre l'interferenza all'arbitrio dell'autorità: deve quindi dettare presupposti, condizioni e controlli all'esercizio di un potere che, senza argini, trasmoderebbe in tirannia¹¹⁰. Il sistema dei contrappesi

¹⁰⁷ Per un panorama completo v. Corte e.d.u., *Guide on Article 8 of the European Convention on Human Rights*, 28 febbraio 2025, disponibile al sito ks.echr.coe.int/; Corte e.d.u., *Guide to the Case-Law of the European Court of Human Rights. Data protection*, 31 agosto 2025, *ivi*.

¹⁰⁸ Le indicazioni della Corte e.d.u. ci torneranno utili soprattutto nel chiederci come il giudice debba valutare la prova prodotta dal dispositivo indossabile: v. *I wearables nel processo italiano*, cit., § 11.

¹⁰⁹ Val la pena ricordare che la Corte e.d.u. adotta una nozione autonoma di 'legge': non sono compresi solo gli atti normativi avente forza di legge, ma anche tutte le linee guida, regole, circolari che ne chiariscono l'applicazione, nonché l'interpretazione e l'applicazione dei precetti da parte della giurisprudenza. Per una recente riaffermazione del metodo v. Corte e.d.u., Sez. III, 16 novembre 2021, *Särgava c. Estonia*, ric. n. 698/19, § 86.

¹¹⁰ Corte e.d.u., 25 giugno 1997, *Halford c. Regno Unito*, ric. n. 20602/92, § 49. La Corte e.d.u. non ha gli stessi poteri delle Corti costituzionali: normalmente giudica su casi specifici, dove un individuo assume la qualità di 'vittima' e lamenta la violazione dei suoi diritti. Per quanto riguarda gli strumenti di sorveglianza occulta, però, i giudici di Strasburgo hanno raggiunto un approdo parzialmente diverso: a determinate condizioni, lo status si può presumere. Se una legge prevede il controllo indiscriminato delle comunicazioni, per esempio, non serve che il singolo ricorrente dimostri di essere caduto sotto sorveglianza — potrebbe essere una prova particolarmente gravosa: non è detto che lo spiato si accorga delle spie e sia in grado di documentare la loro attività. L'esistenza della misura, per come disciplinata, basta a far sorgere la qualità di 'vittima' ai sensi della Convenzione: in quei casi, il vero oggetto del giudizio non sarà un caso concreto, ma l'impianto normativo

deve farsi più stringente per le misure più pericolose, sia per il loro potenziale intrusivo che per come si realizzano. La sorveglianza GPS, per esempio, è stata considerata meno allarmante dell'intercettazione di comunicazioni: secondo la Corte, quindi, il legislatore non è tenuto a spiegare le stesse forze. Anche le modalità esecutive hanno un loro peso: i mezzi d'indagine occulti o i metodi di trattamento automatizzato dei dati personali devono essere circondati di garanzie più strette¹¹¹. La legge, infine, deve essere accessibile e prevedibile: entrano quindi in gioco anche l'interpretazione e l'applicazione del precetto, che possono chiarire il testo od offuscarlo¹¹².

Questo, in breve, è lo scacchiere disegnato dalla giurisprudenza della Corte: è all'interno di tali quadri che dobbiamo ora collocare il problema degli indossabili, almeno dal punto di vista della 'qualità della legge'. In altre parole: quali sono le garanzie minime che rendono la loro acquisizione compatibile con la Convenzione e.d.u.? La prima variabile di cui tenere conto è lo strumento scelto dagli investigatori che, come vedremo, possono valersi di più mezzi per racimolare le informazioni¹¹³: se fossero carpite con un'intercettazione, si dovrebbe applicare il vaglio più rigido dei mezzi di sorveglianza occulta; se fossero prese con un sequestro, come accade quasi sempre, lo scrutinio potrebbe farsi più largo.

Il secondo fattore da considerare riguarda il tipo di dati raccolti: più sono sensibili, più si innalzerà il livello di garanzie richiesto¹¹⁴. Le informazioni generate dagli indossabili, almeno quelle relative alla salute, sono senz'altro in grado di svelare «gli aspetti più intimi [...] o più rilevanti della

in quanto tale: Corte e.d.u., Grande Camera, 4 dicembre 2015, *Zakharov c. Russia*, ric. n. 47143/06, § 170-179. Alla sorveglianza di massa è stato equiparato, come vedremo, l'accesso indiscriminato e diretto da parte delle autorità a dati immagazzinati da *service provider*: Corte e.d.u., *Podchasov c. Russia*, cit., § 55.

¹¹¹ Corte e.d.u., Sez. III, 4 luglio 2023, *Glukhin c. Russia*, ric. n. 11519/20, § 83.

¹¹² Per un esempio recente c. Corte e.d.u., Sez. 5, 13 febbraio 2025, *Macharik c. Repubblica Ceca*, ric. n. 51409/19, § 42-44: le norme di diritto nazionale che consentivano il sequestro di una casella di posta elettronica erano difficili da individuare; in ogni grado di giudizio si è discusso di quale fosse l'articolo di legge che consentiva la misura e ciascun collegio ha deciso diversamente. Tutte le garanzie prescritte erano state rispettate; anzi: proprio perché si erano avvalsi della previsione sbagliata, gli investigatori avevano affrontato un controllo più rigido del dovuto. Il diritto al giusto processo disciplinato dall'art. 6 Conv. e.d.u. era stato pienamente rispettato, ma l'art. 8 Conv. e.d.u. no: la base legale era evidentemente troppo confusa per i requisiti di prevedibilità.

¹¹³ V. *I wearables nel processo italiano*, cit.

¹¹⁴ Per orientarsi nella valutazione, la Corte e.d.u. fa spesso riferimento alla Convenzione n. 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale: Tra le «categorie speciali di dati», quelle da proteggere più intensamente, figurano anche quelli relativi «alla salute o alla vita sessuale» dell'individuo (art. 6).

vita o dell'identità di un individuo»¹¹⁵; non si arriva allo stesso livello di incisività delle intercettazioni, ma l'operazione è senz'altro più invadente della mera richiesta di un indirizzo IP o del tracciamento del GPS.

5. *Segue. La necessità dell'ingerenza*

Il secondo gradino del test adottato dalla Corte e.d.u. prevede un esame del fine perseguito dall'autorità pubblica, ma sul profilo non serve soffermarsi troppo: la Convenzione afferma esplicitamente che la «difesa dell'ordine» e la «prevenzione dei reati» sono scopi legittimi. Possiamo così passare all'ultimo segmento dello schema, secondo il quale le interferenze devono essere necessarie «in una società democratica» (art. 8 Conv. e.d.u.; art. 9 Conv. n. 108). Dal testo, i giudici di Strasburgo hanno tratto numerose implicazioni. Per prima cosa, le azioni degli investigatori devono rispondere a un «impellente bisogno sociale»¹¹⁶ e rispettare un rapporto di proporzione tra l'incisività dell'intervento e il fine (legittimo) perseguito; la valutazione, questa volta, non si appunta sul mero dato normativo o sulla sua interpretazione; scende invece nel concreto. L'equilibrio appare particolarmente delicato quando sui due piatti della bilancia si trovano rispettivamente l'indagine penale, che porta con sé un interesse pubblico palese, ma a intensità variabile; e le informazioni estratte da *wearables*, capaci di monitorare continuamente lo stato fisico (e a volte psicologico) di chi li indossa. La riservatezza dei dati relativi alla salute è sempre stata considerata come «un principio vitale del sistema giuridico di tutte le Parti Contraenti della Convenzione», sia perché consente di tutelare la *privacy* dell'individuo, sia perché protegge la fiducia nel medico e nel servizio sanitario¹¹⁷: se quanto condiviso col dottore rischiasse di finire in piazza, il cittadino, probabilmente, non rivelerebbe dettagli imbarazzanti, ma utili alla diagnosi e alla cura. Per l'acquisizione di cartelle cliniche «tradizionali» la Corte e.d.u. svolge quindi uno scrutinio stretto: si chiede se le circostanze del caso concreto rendano necessaria l'adozione del provvedimento; se l'interesse pubblico alla rivelazione del materiale è sufficientemente intenso; se le autorità nazionali, nel motivare le loro decisioni, hanno ben

¹¹⁵ Corte e.d.u., Sez. V, 28 novembre 2024, *Le Marrec c. Francia* (dec.), ric. n. 52319/22, § 78.

¹¹⁶ Corte e.d.u., *Glukhin c. Russia*, cit., § 89 («pressing social need» nella dicitura inglese); Corte e.d.u., Sez. III, 30 maggio 2017, *Trabajo Rueda c. Spagna*, § 42 («besoin social imperieux» nelle sentenze in francese).

¹¹⁷ Corte e.d.u., 25 febbraio 1997, *Z. c. Finlandia*, ric. n. 22009/93, § 95.

considerato tutti gli interessi in conflitto, svolgendo una valutazione di proporzionalità adeguata¹¹⁸.

Ed è qui che il discorso sulle informazioni prodotte dagli indossabili si fa sfaccettato: l'argomento, per loro, non vale allo stesso modo. L'utente non si confida con uno specialista; autorizza un'azienda a misurare i segnali rilevanti e le consente espressamente di salvare tutto il materiale sui suoi server, o addirittura a rivenderlo a fini esclusivamente commerciali¹¹⁹. Il fatto che i dati estratti dai *wearable* non siano frutto di esami ospedalieri consente di allentare il bilanciamento? O si dovrebbe applicare lo stesso metro anche a loro? La seconda opzione sembra la migliore: anche se non è in gioco la fiducia nel sistema, la giurisprudenza convenzionale è chiara: se le informazioni raccolte riguardano «un aspetto particolarmente importante della vita o dell'identità di un individuo», il margine d'apprezzamento dello stato si restringe¹²⁰. Inoltre, se osserviamo il problema dal punto di vista dell'interessato, gli equilibri non sembrano cambiare di molto: il fatto che i dati provengano da una app e non da un ospedale poco ha a che vedere con l'intimità delle notizie, che non dovrebbero essere raccolte a prescindere da una valutazione attenta. Il vaglio dovrebbe essere insomma severo almeno per quanto riguarda quella categoria di materiale; i dispositivi indossabili ne raccolgono però molto altro che non condivide la stessa etichetta: per esempio, il numero di passi rilevato o i piani di scale saliti non sembrano poter cadere nella categoria dei dati sanitari; per loro potrebbero valere regole meno rigide, ma non lasche al punto da rendere l'esercizio di potere del tutto incongruo.

¹¹⁸ In questo senso v. Corte e.d.u., Z. c. Finlandia, cit., § 96 ss.: nel caso di specie, le autorità nazionali hanno sequestrato le cartelle cliniche della ricorrente e costretto i suoi medici a testimoniare in udienza. Il processo pendeva contro il marito della donna, accusato di aver stuprato una terza persona che aveva contratto il virus HIV a seguito della violenza. Gli inquirenti cercavano quindi di stabilire il momento a partire dal quale l'imputato fosse a conoscenza dell'infezione anche tramite la diagnosi della moglie, a sua volta contagiata. La Corte ha ritenuto che l'interesse pubblico, date le circostanze, fosse in grado di vincere la riservatezza.

¹¹⁹ La differenza, in alcuni ordinamenti, è cruciale: negli Stati Uniti, per esempio, il principale statuto federale sulla protezione dei dati sanitari (il HIPAA - *Health Insurance Portability and Accountability Act*) si applica soltanto alle cliniche, alle assicurazioni e ai loro partner; non ad app commerciali che raccolgono informazioni sul benessere delle persone. Per un quadro complessivo del tema, v. O. FEHER, *RFK Jr. Wants Us to Trust Health Tracking Devices and Apps. Should We?*, in *progressivepolicy.org*, 3 settembre 2025.

¹²⁰ Corte e.d.u., Sez. V, 4 giugno 2013, Peruzzo e Martens c. Germania, ric. n. 7841/08, § 41; Corte e.d.u., Grande Camera, 10 aprile 2007, Evans c. Regno Unito, ric. n. 6339/05, § 77.

6. *L'impatto sul processo*

Abbiamo visto finora quali sono i confini che la Convenzione e.d.u. traccia nel consentire (limitate) ingerenze nella vita privata delle persone, ma se un elemento è raccolto in palese violazione dell'art. 8 Conv. e.d.u., potrà essere utilizzato? O la sua valutazione compromette l'accertamento agli occhi della Corte e.d.u.?

Dal punto di vista della Convenzione, il rispetto della riservatezza e l'accertamento giudiziario sono due faccende del tutto separate. Certo, talvolta i profili si sovrappongono al punto da essere trattati in maniera congiunta¹²¹; sono però assai più numerosi i casi in cui le valutazioni si mantengono parallele. In materia di prove, la Corte e.d.u. limita i propri poteri in modo esplicito: non perde occasione per affermare che le condizioni di ammissibilità e utilizzabilità del materiale dipendono esclusivamente dagli ordinamenti interni; la Corte di Strasburgo può censurare quegli aspetti solo se, nel caso concreto, la gestione dell'elemento è stata tale da contaminare tutto il procedimento rendendolo ingiusto. Si è formulato un discorso analogo per la valutazione delle risultanze: è riservata alle autorità nazionali; i giudizi espressi nella motivazione dei provvedimenti sono quindi invalicabili, salvo che non siano del tutto mancanti o palesemente viziati da errori grossolani di fatto o di diritto¹²². Se i dati degli indossabili, quindi, fossero raccolti male, se fossero prelevati in maniera sovrabbondante o se fossero interpretati in maniera sbagliata, l'art. 6 Conv. e.d.u. non sarebbe automaticamente violato; lo sarebbe solo se l'uso delle informazioni compromettesse l'equità del processo.

Per orientarsi, i giudici possono contare su tre indici: il primo, su cui torneremo tra poco, è la qualità degli elementi su cui poggia la ricostruzione. La fonte delle informazioni; il modo con cui sono estratte e maneggiate; la maniera in cui sono conservate: questi e altri fattori influiscono sulla loro affidabilità e accuratezza. Se la decisione fosse presa sulla base di prove che non hanno il necessario valore dimostrativo, l'art. 6 Conv. e.d.u. sarebbe violato. Un secondo fattore che la giurisprudenza valorizza è la correttezza del procedimento probatorio. Il modo — confor-

¹²¹ Corte e.d.u., *Yalçinkaya c. Turchia*, cit., § 368 ss.; in quel caso, la connessione tra le due doglianze era talmente stretta da ritenere superflua la trattazione del ricorso quanto all'art. 8 Conv. e.d.u.: la ricca argomentazione relativa all'art. 6 Conv. e.d.u. si è ritenuta sufficiente. La scelta della maggioranza è stata criticata in un'opinione di minoranza (*dissenting opinion* del giudice Serdighes, § 10 ss.), che riteneva necessario un esame completo anche dei profili concernenti il rispetto della vita privata.

¹²² Per una riaffermazione recente e autorevole dei principi v. Corte e.d.u., *Yalçinkaya c. Turchia*, cit., § 303, 304 e 316.

me o meno alle altre regole della Convenzione — con cui il materiale è stato acquisito costituisce un punto di partenza, ma non di arrivo: il processo può comunque risultare equo se la difesa ha la possibilità di esprimere le proprie obiezioni e confutare quanto prodotto. Infine, le corti nazionali devono mostrare di aver ascoltato e considerato gli argomenti dell'imputato: la motivazione dovrebbe affrontare esaustivamente tutti i dubbi sollevati. Può dividerli o ritenerli infondati, non può invece ignorarli. Anche tale indicazione, lo vedremo, ci tornerà utile.

7. *La riservatezza nelle indagini: la direttiva 'LED' (2016/680) e il d.lgs. n. 51 del 2018*

Veniamo all'ultimo atto determinante per l'uso dei dati prodotti dagli indossabili: la direttiva che si occupa della protezione dei dati personali nello specifico ambito della «prevenzione, indagine, accertamento e perseguimento di reati» e traspunta in Italia con il d.lgs. 18 maggio 2018, n. 51. Prima della sua approvazione, il diritto eurounitario tutelava le informazioni raccolte dall'autorità giudiziaria soltanto nel momento in cui venivano trasferite all'estero¹²³; il testo del 2016, invece, detta garanzie di *privacy* minime dirette alle autorità nazionali¹²⁴.

Il passo è stato accolto con entusiasmo dagli esperti di diritto alla *privacy*, mentre ha destato una palpabile preoccupazione presso chi delle indagini si occupa quotidianamente: le forze di polizia. La nozione di 'trattamento' accolta dalla direttiva comprende «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione» di dati personali, cioè: ogni operazione che possa essere concepita nell'ambito di un'indagine¹²⁵. Una importante conferen-

¹²³ Secondo alcuni commentatori, le norme previgenti (Decisione quadro 2008/977/GAI, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale) sarebbero state talmente limitate nello scopo, talmente sbilanciate a favore della sicurezza pubblica, talmente poco cogenti da sfiorare l'irrilevanza: P. DE HERT-V. PAPA-KOSTANTINOU, *The New Police and Criminal Justice Data Protection Directive. A First Analysis*, in *New Jour. Eur. Crim. Law*, 7 (2016), f. 1, p. 8.

¹²⁴ Per una dettagliata analisi v. I. NERONI REZENDE, *Criminal Justice and Data Protection*, cit., p. 43 ss.

¹²⁵ Sull'estensione esatta della norma v. C. JASSERAND, *Law enforcement access to personal*

za di Europol del 2019, significativamente intitolata *Paradise Lost? Policing in the age of data protection*, fu dedicata allo studio delle nuove disposizioni e degli effetti che avrebbero spiegato sulle loro attività¹²⁶; dal loro punto di vista, preoccuparsi troppo della riservatezza avrebbe potuto rendere le indagini meno incisive o meno celeri.

Come il GDPR, sia la direttiva che il decreto che il d.lgs. n. 51 del 2018 stabiliscono alcuni principi generali per la protezione dei dati personali: devono essere «trattati in modo lecito e corretto»; essere «raccolti per finalità determinate, espresse e legittime» (art. 3 comma 1 lett. *b* d.lgs. n. 51 del 2018) e devono risultare «adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati» (art. 3 comma 1 lett. *c* d.lgs. n. 51 del 2018). La consonanza con i principi espressi dalla giurisprudenza della Corte e.d.u. è evidente: si ribadisce che il raggio d'azione di chi raccoglie materiale è limitato nelle finalità — nel nostro caso: l'indagine e l'accertamento di reati — e nel perimetro. Le necessità del caso guideranno la mano degli inquirenti e del giudice: occorre prelevare e utilizzare quanto serve a raggiungere lo scopo — provare efficacemente una tesi — ma non di più. Le informazioni devono essere necessarie, ma anche sufficienti; se salvare l'intera memoria del dispositivo è l'unico modo che abbiamo per poter interpretare correttamente un singolo elemento, la misura non è eccedente: si dovranno semmai trovare modalità di scrutinio tali da evitare sacrifici inutili della riservatezza¹²⁷. Lo stesso vale per il vincolo dell'apparecchio: se servisse per compiere accertamenti impossibili da svolgere sulla copia, lo si potrà trattenere¹²⁸.

A questo quadro generale, la direttiva aggiunge una pennellata. All'art. 7, chiede alle autorità nazionali di distinguere, per quanto possibile, i fatti dalle valutazioni. La norma, trascritta all'art. 4 d.lgs. n. 51 del 2018,

data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?, in *Computer Law & Security Rev.*, 34 (2018), p. 154 ss.

¹²⁶ Europol's Data Protection Experts Network (EDEN), *Paradise Lost? Policing in the age of data protection*, 19-20 settembre 2019; il programma dei lavori è disponibile al sito: europol.europa.eu/publications-events/events/paradise-lost-policing-in-age-of-data-protection. Tra gli argomenti principali compare anche il problema dell'accesso ai dati prodotti dagli «smart devices», tra cui sono espressamente menzionati i *fitness tracker*.

¹²⁷ La Corte di giustizia tende poi ad anticipare l'applicazione delle garanzie. In un recente caso, la polizia aveva posto sotto sequestro un telefono e aveva cercato di forzare la cifratura per accedere ai suoi contenuti; i giudici di Lussemburgo hanno affermato che anche il «tentativo di accesso a dati personali contenuti in un telefono» costituisce a tutti gli effetti «trattamento» ai sensi della direttiva. Se così non fosse, ha affermato il collegio, le garanzie assicurate dalla direttiva sarebbero frustrate: Corte giust., Grande sezione, 4 ottobre 2024, C-548/21, *Bezirkshauptmannschaft Landeck*, § 69 ss.

¹²⁸ Come vedremo, l'ipotesi è forse più concreta per i *wearables* che per altri dispositivi: v. *I wearables nel processo italiano*, cit., § 5.

assume grande rilievo nel campo degli indossabili: un conto è dire che il dispositivo ha rilevato uno spostamento; altro è ritenere che, a partire da quell'elemento, si possa dimostrare l'innocenza o la colpevolezza dell'imputato. Il dato fornisce una base oggettiva per argomentare una tesi, ma l'elemento non deve confondersi con la sua interpretazione. La norma, come vedremo tra poco, dovrebbe orientare tanto gli investigatori quanto i tribunali nelle loro decisioni¹²⁹.

8. *Segue. Le categorie particolari*

Quanto abbiamo appena visto vale per tutti i dati personali; la direttiva individua poi determinate informazioni, da trattare con particolare attenzione e con garanzie rafforzate. L'art. 10 LED, a questo fine, isola i «dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale».

Anche in questo caso, le classi che sembrano riguardare più direttamente il tema degli indossabili sono quelle dei dati relativi alla salute¹³⁰ e alla vita sessuale dell'interessato e, nel considerarle, sarà bene tenere a mente l'approccio estensivo della Corte di giustizia. Essa, infatti, tende a considerare come dati sensibili non solo le informazioni che lo sono intrinsecamente, ma anche quelle che svelano uno degli aspetti intimi protetti se sottoposte a «un'operazione intellettuale di deduzione o di raffronto»¹³¹.

Il diritto dell'Unione stabilisce condizioni rafforzate per la liceità del loro trattamento, disegnando così tre cerchi concentrici: i dati non personali, che non devono essere gestiti con le garanzie della direttiva; quelli personali, che seguono il suo regime ordinario; quelli “sensibili”, che go-

¹²⁹ Per un esame dettagliato della disposizione v. M. TZANOU, Sub Art. 7, in E. KOSTA-F. BOHEM (a cura di), *The EU Law Enforcement Directive (LED). A commentary*, Oxford University Press, Oxford, 2024, p. 181 ss.

¹³⁰ L'art. 2 d.lgs. n. 51 del 2018 li definisce come le informazioni «attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute».

¹³¹ Corte giust., 1 agosto 2022, C-184-20, Vyriausioji tarnybinės etikos komisija, § 123. La decisione è stata emessa rispetto all'art. 9 GDPR, non rispetto all'art. 10 direttiva 2016/680. Come abbiamo visto, le due disposizioni non sono equivalenti, ma descrivono le categorie di dati sensibili in maniera identica, *verbatim*: su quel punto, la giurisprudenza resa rispetto a un testo può essere utile anche per l'interpretazione dell'altro.

dono di una protezione più intensa. A questo punto, sorge una complicazione: gli indossabili generano molte informazioni, alcune senza dubbio più delicate di altre; quali standard si devono applicare? Nel sistema della Convenzione e.d.u., come abbiamo visto, occorrerebbe partire dalla natura del singolo elemento prelevato: il test di necessità e proporzionalità si imposterebbe da qui, dalla profondità di una particolare interferenza. Le coordinate unionali, invece, sono diverse, anche perché la Corte di giustizia è un giudice delle norme e non dei casi concreti: deve occuparsi di *data protection* in generale e in astratto, a prescindere dalla complessiva equità di un singolo risultato. La promiscuità dei dati, qui, è gestita diversamente e, nel decidere su apparecchi come il telefono cellulare, la Corte di giustizia ha scelto l'approccio più cauto: dato che lo *smart phone* può contenere materiale di ogni sorta — non personale, personale e sensibile — le condizioni d'accesso devono essere sagomate per rispettare i requisiti più severi¹³². Ogni tentativo d'accesso si deve quindi conformare alle garanzie dell'art. 10 LED¹³³. Lo stesso principio dovrebbe valere per gli indossabili: anche loro producono informazioni di diversa qualità, ma quasi tutti generano e salvano *anche* dati sanitari; l'intero dispositivo dovrebbe quindi essere protetto dalla più stretta disciplina del trattamento delle informazioni che appartengono a categorie particolari, anche se non si riuscisse ad accedere al dispositivo o anche se non si utilizzasse a processo il materiale sensibile.

Veniamo ora alle protezioni disciplinate dall'art. 10 LED, trasposto pedissequamente in Italia dall'art. 7 d.lgs. n. 51 del 2018. Il testo autorizza il trattamento di quei dati «solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato». In aggiunta a tali condizioni generali, la norma elenca tre casi in cui la lavorazione dei dati è consentita: se «specificamente [prevista] dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento»; se è necessaria «per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica», «ferme le garanzie dei diritti e delle libertà» del soggetto; o infine se ha oggetto «dati resi manifestamente pubblici dall'interessato»¹³⁴.

La Corte di giustizia ha esaminato attentamente il testo, quasi parola per parola, individuando i contrappesi che devono bilanciare la violazione della sfera informativa più intima. Una prima indicazione arriva dall'av-

¹³² Corte giust., Grande sezione, 4 ottobre 2024, C-548/21, cit.

¹³³ Sui riflessi della pronuncia nell'ordinamento italiano v. *I wearables nel processo italiano*, cit., § 6.

¹³⁴ La disposizione riproduce quasi testualmente la sua omologa, l'art. 10 direttiva 2016/680.

verbio «solo», cui la Corte ha attribuito un senso forte: significa che le informazioni possono essere trattate in un numero necessariamente limitato di occasioni¹³⁵. Ciò significa che la legge nazionale deve prevedere i casi in cui è consentito eseguire una misura investigativa capace di acquisire dati sensibili; quegli strumenti di indagine, in altre parole, non possono essere ammessi per tutti i procedimenti com'è invece oggi per il sequestro italiano¹³⁶.

La Corte ha poi chiarito in cosa consiste il requisito della *stretta* necessità: esso impone al legislatore nazionale una valutazione di proporzionalità particolarmente severa, specie rispetto alla natura e alla gravità del reato per cui si procede: il fatto deve essere sufficientemente allarmante da spiegare l'intrusione. Nel predisporre un sistema di barriere adeguato, quindi, la serietà della fattispecie dovrebbe avere un ruolo importante¹³⁷ e autenticamente selettivo: presupposti talmente larghi da risultare più apparenti che reali non sarebbero riconosciuti come effettivi, poiché consentirebbero l'uso di strumenti più invasivi di quanto serve a raggiungere l'obiettivo¹³⁸.

L'art. 10 LED prevede infine che il trattamento sia assistito da «adeguate garanzie». Qualora l'atto d'indagine rischi di realizzare «un'ingerenza grave, o addirittura particolarmente grave» nei diritti fondamentali del singolo, la Corte identifica quel requisito nel controllo di un giudice o di un'autorità amministrativa indipendente: il delicato gioco di pesi e contrappesi istituito dalla direttiva deve trovare un arbitro, qualcuno di terzo che vegli sul rispetto delle regole in ciascun caso e che svolga anche una valutazione autonoma di proporzionalità in concreto¹³⁹.

La direttiva LED non precisa quale sanzione debba scattare alla violazione di tali regole; esse sembrano però destinate a tradursi in divieti di legge piuttosto specifici: se fosse così, l'ordinamento italiano potrebbe offrire risposte nette¹⁴⁰.

L'impianto previsto dalla direttiva è piuttosto stringente, ma occorre ricordare un elemento: lo schema di garanzie si infragilisce notevolmente se i dati sono resi «manifestamente pubblici» dal soggetto, cioè: se l'utente

¹³⁵ Corte giust., Grande sezione, 4 ottobre 2024, C-548/21, cit., § 108; Corte giust., 26 gennaio 2023, C-205/21, cit., § 118.

¹³⁶ Per l'esame più puntuale del tema v. *I wearables nel processo italiano*, cit., § 5.

¹³⁷ Corte giust., Grande sezione, 4 ottobre 2024, C-548/21, cit., § 99.

¹³⁸ Corte giust., 26 gennaio 2023, C-205/21, cit., § 129, che ha dichiarato inadeguate le garanzie predisposte dall'ordinamento bulgaro per la raccolta di campioni biologici: essa era possibile nelle indagini per reati dolosi perseguibili d'ufficio.

¹³⁹ Corte giust., Grande sezione, 4 ottobre 2024, C-548/21, cit., § 102.

¹⁴⁰ V. *I wearables nel processo italiano*, cit., § 6.

pubblica su social o su altre piattaforme di condivisione aperte i dati relativi, per esempio, all'ultimo allenamento.

9. Conclusioni

Gli scenari che abbiamo appena ripercorso appaiono lontanissimi: il fenomeno globale di erosione della *privacy* e l'avanzata dei giganti privati della tecnologia sembrano del tutto fuori portata rispetto all'accertamento penale. Eppure, le due dimensioni sembrano destinate a parlarsi in modo via via più fitto: il processo ha bisogno di informazioni, materiale che si trova sempre più spesso (e in quantità crescente) nelle mani di poche grandi aziende¹⁴¹.

Da questo intreccio derivano almeno tre conseguenze interessanti. Innanzitutto, la dimensione praticamente mondiale di alcune imprese rende il potere di un singolo stato assai più piccolo: il diritto nazionale, da solo, non riesce più a essere del tutto effettivo¹⁴². Cresce insomma il bisogno di politiche e azioni comuni: un soggetto più grande, se agisce compatto, può esercitare una pressione maggiore. In questo campo, quindi, il diritto dell'Unione Europea è destinato ad assumere un ruolo particolarmente rilevante.

Inoltre, il diritto (privato) che si applica alle industrie digitali ha conseguenze sempre maggiori anche sul sistema penale. Abbiamo visto come il diritto della *privacy* influenza la raccolta dei dati degli indossabili, ma non è che l'inizio: anche le decisioni aziendali possono avere un impatto inaudito sulla possibilità di svolgere determinati atti d'indagine. Una spia chiarissima della dinamica arriva ancora una volta dagli Stati Uniti, dove il contrasto giurisprudenziale sull'accesso ai dati prodotti con sistemi di *geofencing*¹⁴³ non è stato risolto dalla Corte suprema, ma da un cambio di policy di Google: l'azienda ha deciso di non salvare più determinate informazioni sui suoi server¹⁴⁴, troncando così la polemica sulla costituziona-

¹⁴¹ Basti pensare che Amazon, Google e Microsoft, da sole, detengono circa il 60% del mercato globale del *cloud*.

¹⁴² Per una valutazione sull'impatto (deludente) di una delle iniziative nazionali più strutturate — la NetzDG tedesca — v. W. ECHIKSON-O. KNOTT, *Germany's NetzDG. A key test for combatting online hate*, in *ceps.eu*, 22 novembre 2018.

¹⁴³ Sul tema v. H. AMSTER-B. DIEHL, *Against Geofences*, in *Stan. law rev.*, 74 (2022), p. 385 ss.; J. O'NEIL, *Much Ado About Geofence Warrants*, in *Harvard law rev.* (web), 18 febbraio 2025; O.S. KERR, *The ACLU's Response to My Post on the Fifth Circuit's Smith Ruling—And My Reply to the ACLU*, in *Reason* (web), 16 agosto 2024.

¹⁴⁴ V. a riguardo M. MCGRIFF, *Updates to Location History and new controls coming soon to Maps*, in *blog.google.com*, 12 dicembre 2023.

lità di mandati che rischiavano di essere troppo ampi. Rimosso il dato, rimosso il problema.

Infine, gli strumenti di tracciamento volontario sono sempre più diffusi e penetranti: le scelte su cosa può essere messo a disposizione dell'autorità giudiziaria non possono essere lasciate al caso o, peggio ancora, a un decisore privato. Abbiamo visto il tentativo europeo di stabilire nuovi limiti impostando il problema in termini di diritti umani, e ancora una volta il discorso sembra astratto, capace di esprimere molti buoni propositi e poche ricadute operative¹⁴⁵. Eppure qualcosa sta cambiando: anche grazie a un rinnovato impegno della Corte di giustizia dell'Unione europea, le procedure penali del vecchio continente iniziano a interrogarsi in termini nuovi.

¹⁴⁵ Per darsi un piano più dettagliato, la Commissione europea ha istituito un gruppo di lavoro sull'accesso alle informazioni digitali per un'efficace lotta alla criminalità: v. *High-Level Group (HLG) on access to data for effective law enforcement*, in *home-affairs.ec*, 22 novembre 2024.

IL BRACCIALETTO ELETTRONICO: PROSPETTIVE INEDITE PER UNO STRUMENTO COLLAUDATO

ELENA VALENTINI

SOMMARIO: 1. Premessa definitoria. – 2. Uno strumento ancora utile? – 3. Il bracciale elettronico in Italia: un esordio timido, un presente che incalza. – 4. Le diverse tecnologie impiegate. – 5. Possibili ricadute probatorie. – 6. Uno sguardo al futuro. – 7. *Segue*: il controllo a distanza del consumo di alcol. – 8. *Segue*: monitoraggio elettronico e controllo dei migranti. – 9. Gli “*altri*” braccialetti elettronici. – 10. Conclusioni.

1. *Premessa definitoria*

Una semplice ricerca su *google* testimonia come l'espressione *bracciale elettronico* venga comunemente impiegata per riferirsi a una ricca varietà di strumenti, diversi fra loro sul piano tanto morfologico quanto finalistico.

Innanzitutto, essa evoca un istituto noto alla disciplina processuale penale e al diritto penitenziario: quello che vede lo Stato imporre al singolo di indossare il dispositivo, con un atto di forza o una forma più o meno convincente di ricatto. Nel nostro sistema, al fine di monitorare l'ubicazione e gli spostamenti dell'imputato o del condannato; in quello di altri paesi, anche per sorvegliarne ulteriori condotte, in particolare il consumo di alcol.

Di bracciale elettronico spesso tuttavia si parla pure in rapporto ad apparecchiature pensate per scopi diversi da quelli perseguiti dal sistema penale o di prevenzione speciale. Se ne parla, però, quasi sempre per alludere a strumenti che l'individuo abbia comunque accettato di accogliere su di sé in modo non totalmente libero: è il caso dei dispositivi preposti a tracciare i movimenti degli stranieri irregolari¹; di quelli atti a sorvegliare bambini o anziani (e, più in generale, persone cognitivamente non auto-

¹ Ne daremo conto *infra*, al § 8.

sufficienti); è il caso, assurdo agli onori delle cronache nel periodo pandemico, dei dispositivi indossabili finalizzati a tenere sotto costante osservazione, al contempo, determinati parametri sanitari e la posizione fisica di chi li indossa: strumento che alcuni Stati hanno deciso di rendere obbligatorio per verificare sia il decorso della malattia sia la geolocalizzazione del paziente, così da osservare a distanza lo stato di salute dell'interessato ma anche l'effettivo rispetto, da parte sua, delle prescrizioni associate alla quarantena².

Nella sua eterogeneità, lo scenario appena abbozzato porta a isolare alcune caratteristiche, istintivamente associate all'idea di *braccialetto elettronico*, utili per ricostruire una definizione che, scevra da velleità classificatorie più ambiziose, semplicemente si propone di delimitare l'oggetto di questo scritto. Sulla scorta di tali peculiarità, l'espressione *braccialetto elettronico* verrà qui impiegata per indicare la *consapevole sottoposizione* di un individuo a un *monitoraggio*, attuato con *strumenti tecnologici*, posto in essere, *a distanza*, da parte di soggetti *terzi*, in modo *contestuale* e *non occulto*, reso possibile da un'imposizione coatta o grazie al rilascio di un *consenso*, di natura preventiva, *non propriamente libero* (poiché ottenuto attraverso forme di persuasione particolarmente stringenti).

Forme di monitoraggio con le caratteristiche appena indicate possono operare su iniziativa di attori diversi, non solo pubblici, ma anche privati. A tale secondo riguardo, un esempio ricorrente di vigilanza mediante dispositivi indossabili, parimenti evocato con l'espressione *braccialetto elettronico*, è quello "imposto" dal datore di lavoro, e non sempre onde garantire idonee condizioni di sicurezza nello svolgimento di determinate mansioni³. In contesti aziendali è infatti sempre più frequente imbattersi anche in strumenti tecnologici dichiaratamente intesi a rendere possibile o ad agevolare lo svolgimento di specifiche mansioni: strumenti la cui entrata in scena è stata guardata con allarmata diffidenza, nella misura in cui essi si prestano a tenere d'occhio anche la produttività del singolo.

² Stando a quanto riportato in rete, tra i paesi che hanno fatto ricorso a questo tipo di congegni si collocano sicuramente Western Australia, Hong Kong, Singapore. V. F. BALLO, *Il Covid-19 e le nuove frontiere tecnologiche: l'app Immuni e (il ritorno dei) braccialetti elettronici?*, in *giustiziainsieme.it*, 25 giugno 2020, S. SHARWOOD, *Australian state will install home surveillance hardware to make sure if you're in virus isolation, you stay here*, in *theregister.com*, 1° aprile 2025, L. MONTALTO MONELLA, *Coronavirus, a Hong Kong chi è in quarantena e monitorato con braccialetto elettronico*, in *it.euronews*, 19 marzo 2020, N. PENNA, *Contro il covid di importazione, Singapore rende obbligatorio il braccialetto elettronico per tutti gli arrivi dall'estero*, in *lastampa.it*, 10 agosto 2020.

³ A. INGRAO, *Il braccialetto elettronico tra privacy e sicurezza del lavoratore*, in *Diritto delle relazioni industriali*, 2019, p. 895.

Sebbene non coinvolga il rapporto tra individuo e pubblica autorità, la scelta del lavoratore di sottoporsi al controllo del “padrone” difficilmente può dirsi libera o incondizionata, potendo essere ottenuta attraverso pressioni oltremodo efficaci.

Benché in genere non evocato dall'espressione *braccialetto elettronico*, uno scenario non troppo dissimile può presentarsi anche nel mondo sanitario, dove il concreto esercizio del diritto alla salute talvolta passa anche per la sottoposizione a forme di controllo a distanza. Nonostante la chiara differenza rispetto all'ipotesi dei dispositivi di monitoraggio epidemiologico sperimentati durante la stagione del Covid (dispositivi che in alcuni stati esteri si poteva essere *obbligati* a indossare per scongiurare il contagio), anche in questo caso ci troviamo di fronte a una forma di costrizione: infatti, per quanto teoricamente libera, la scelta del paziente non sempre può dirsi davvero tale, essendo spesso resa ineludibile dallo stato di necessità in cui egli versa.

Ecco dunque che, pur appartenendo al mondo privatistico e comunque non coinvolgendo il rapporto tra individuo e agenzie del controllo pubblico, anche i casi appena indicati sono parimenti accomunati dallo stato di assoggettamento (o quantomeno di soggezione) di colui che si espone al controllo da remoto⁴.

Negli ultimi anni, le occasioni e gli strumenti in grado di propiziare specifiche declinazioni del monitoraggio digitale si sono moltiplicate, dando vita a una proliferazione silenziosa e pervasiva, che induce a interrogarsi sull'effettività e sulle conseguenze del consenso rilasciato da chi accetta di sottoporsi a sorveglianza, nonché sui possibili impieghi probatori, a fini penali, delle conoscenze procacciate da tali dispositivi.

2. *Uno strumento ancora utile?*

Intuibilmente, nelle prossime pagine ci concentreremo soprattutto sulla vigilanza elettronica regolata dal diritto penitenziario e processuale penale, volta a controllare la posizione fisica del bersaglio e applicabile anche a “supporto” di alcune misure preventive. Prima di farlo, è tuttavia opportuno svolgere una considerazione.

Nel momento in cui il braccialetto elettronico si accingeva a entrare in scena (le prime significative sperimentazioni oltreoceano risalgono agli

⁴ Tale variegata fenomenologia fa constatare un paradosso: solo i congegni indossati per ragioni estranee al sistema penale sono veri e propri braccialetti, avendo quelli impiegati a scopi penali le fattezze della cavigliera.

inizi degli anni '80⁵), lo strumento era, se non proprio infungibile, quasi tale. Rispetto ad oggi, determinate informazioni – in particolare quelle su posizione e movimenti delle persone – erano infatti molto più difficili da ottenere o da ricostruire *ex post*. Al contrario, ai giorni nostri chiunque lascia molte più tracce di sé e del proprio passaggio. Basti considerare che, oltre ad essere sottoposto a una miriade di “occhi tecnologici” (in spazi pubblici ma non solo), oggi ognuno di noi viaggia portando immancabilmente con sé uno *smartphone* (ossia uno strumento di cui è magari possibile ridurre la tracciabilità, senza però eliminarla del tutto); tanto che, come vedremo, tale *device* sta già affiancando e almeno in parte sostituendo i più tradizionali dispositivi indossabili⁶.

Questa constatazione – concernente appunto la possibilità di raccogliere a fini di controllo penale una miriade di tracce in precedenza destinate all'oblio ma oggi sempre più agevolmente reperibili – potrebbe indurre a ridimensionare l'importanza del braccialetto elettronico. Tanto più considerando lo sviluppo vertiginoso della tecnologia, che si presta a incasellare, incrociare ed elaborare una massa sempre più imponente di dati (così com'è dimostrato dalle enormi potenzialità tecnicamente offerte dalla possibilità di combinare riconoscimento facciale e geolocalizzazione).

Tuttavia, il braccialetto elettronico continua a conservare una sua persistente utilità, e non solo perché quella abbinata a tale strumento è una sorveglianza che si estrinseca in un contatto diretto tra “controllore” e bersaglio, senza alcuna mediazione; ma anche perché il monitoraggio reso possibile dal braccialetto scruta un individuo conscio di essere osservato in tempo reale, trovando la propria ragion d'essere nell'effetto deterrente generato dalle eventuali ricadute probatorie dei comportamenti registrati⁷. Soprattutto, l'utilità del braccialetto si spiega perché la consape-

⁵ L'idea fu elaborata negli anni '60, dallo psicologo comportamentale Ralph Kirkland Schwitzgebel (che poi cambiò il proprio nome in Robert S. Gable), attivo nella *behavioral telemetry*, che concepì per la prima volta l'idea di un dispositivo elettronico indossabile per monitorare persone a distanza e trasmettere segnali continui, pensandone esplicitamente l'utilizzo per soggetti in libertà vigilata e come alternativa alla detenzione (v. R.S. GABLE, *The Ankle Bracelet Is History: An Informal Review of the Birth and Death of a Monitoring Technology*, in *The Journal of Offender Monitoring*, vol. 27, n. 1, p. 4-8, e E. ANDERSON, *The Evolution of Electronic Monitoring Devices*, in *npr.org*, 24 maggio 2014). La prima applicazione da parte dell'autorità giudiziaria risale al 1983, da parte del giudice Jack Love del New Mexico, e ha visto porre a presidio della detenzione domiciliare la cavigliera elettronica NIMCOS.

⁶ V. *infra*, alla nota 54 e poi anche in seguito, nel testo.

⁷ In questo caso, la linea di demarcazione tra prevenzione e investigazione – peraltro sempre più sottile e sfumata (v. in tal senso A. NASCIBENI, “Fermento pre-investigativo” e analisi automatizzata di dati, in *Arch. n. proc. pen.*, 2024, p. 558, e A. CAMON, *Intelligenza artificiale*,

volezza del monitoraggio *in itinere* da parte di chi accetta di farsene bersaglio potrebbe prestarsi a scansare eventuali preclusioni o limiti normativi prescritti rispetto a mezzi di indagine che, preposti ad ottenere le medesime informazioni, dovessero invece operare in maniera occulta, o comunque senza il consenso preventivo o la piena consapevolezza del diretto interessato⁸.

Ora, quali che siano le ragioni sottese alle diverse forme di monitoraggio elettronico – siano o meno riconducibili a rapporti regolati dal diritto e dalla procedura penale – i risultati conoscitivi che ne derivano potrebbero comunque rivelarsi utili anche a fini di prova penale. Ed è proprio questo a giustificare un approfondimento del tema nell’ambito di questo progetto di ricerca.

Intuibilmente, questo scritto si concentrerà soprattutto sul braccialetto elettronico inteso nella sua accezione più tradizionale e familiare al processualpenalista: quella che vede lo Stato imporre il monitoraggio e l’individuo sottomettersi, sia pure *ob torto collo*. A seguire, daremo velocemente conto anche degli “*altri*” braccialetti elettronici cui si è fatto cenno in apertura, in quanto anch’essi possibili vettori di conoscenze utili all’accertamento penale.

3. *Il braccialetto elettronico in Italia: un esordio timido, un presente che incalza*

Nel mondo, e specie in paesi (come gli Usa e la Gran Bretagna) interessati da tassi di carcerizzazione assai elevati, il ricorso alla vigilanza digitale a fini penali si è progressivamente dilatato, fino ad assumere proporzioni impressionanti⁹. Sia pure in scala molto mino-

indagini preliminari e diritti di libertà, in *Cass. pen.*, 2025, p. 3007) – è negata in partenza: la consapevolezza di essere osservati risponde infatti a una funzione special-preventiva che fa leva proprio sulla futura utilizzabilità dei risultati conoscitivi della sorveglianza.

⁸ Si consideri, in particolare, che l’art. 5 dell’*AI Act* vieta l’uso di sistemi di identificazione biometrica remota negli spazi pubblici, salve eccezioni limitate e tassative (ricerca di vittime di sequestro o traffico di persone, prevenzione di una minaccia alla vita o sicurezza fisica di persone, localizzazione o identificazione di una persona sospettata di gravi reati puniti con una elevata pena detentiva); e comunque, anche in questi casi, con il necessario rispetto dell’art. 26 § 10 del medesimo Regolamento, che regola gli obblighi degli utilizzatori dei sistemi di intelligenza artificiale ad alto rischio. In generale, sul tema, v. G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*, in *Cass. pen.*, 2025, p. 638 ss., segnatamente 663 ss.

⁹ In particolare negli Stati Uniti, l’uso del monitoraggio nell’ambito del *criminal legal system* e del *civil immigration system* (del quale daremo conto *infra*, al § 8) ha portato a stimare che nel corso del 2022 sono state sottoposte a sorveglianza circa 360.000 persone, con una decuplicazione del numero dei sorvegliati rispetto al 2005. V. VERA INSTITUTE OF JUSTICE, *People on Electronic Monitoring* (v. vera.org/publications/people-on-electronic-monitoring). In propo-

re¹⁰, una vistosa tendenza all'ampliamento è ravvisabile anche nel nostro sistema, interessato da un'evoluzione legislativa sintomatica di aspettative crescenti verso tale forma di controllo.

Prima di interrogarci sul futuro, è opportuno innanzitutto ricostruire il presente, alla luce di una storia travagliata, che ha avuto inizio un quarto di secolo fa, quando il d.l. 24 novembre 2000, n. 341 (conv. con l. 19 gennaio 2001, n. 4) ha riconosciuto la possibilità di affiancare il controllo elettronico a distanza alla detenzione domiciliare, in fase tanto cautelare quanto esecutiva della pena.

Ripercorrendo per sommi capi tale storia, ne va innanzitutto evidenziato l'andamento singolare, che ha visto la disciplina positiva rimanere pressoché lettera morta per quasi tre lustri. Quando è chiamato a normare fenomeni indotti dall'evoluzione scientifica e tecnologica, il diritto tende in genere ad arrancare, a muoversi in ritardo; riguardo al braccialetto elettronico, invece, la dinamica è stata contraria, visto che, per lunghi anni, la fuga in avanti operata dal legislatore del 2000 è restata quasi del tutto priva di riscontro applicativo. Tanto da aver suscitato forti critiche per il conseguente e inutile spreco di risorse pubbliche destinate a tale fine¹¹.

A partire dal 2013 le cose sono cambiate, determinando, nel volgere di poco, l'insufficienza degli apparecchi disponibili rispetto alle esigenze della pratica giudiziaria. Questo rapido mutamento di scenario è stato innanzitutto figlio di precise indicazioni sovranazionali: oltre a quelle poi sfociate, nel 2014, in una Raccomandazione del Consiglio d'Europa volta a incentivare l'impiego della sorveglianza elettronica¹², decisiva in tal senso è stata la pronuncia, nel gennaio del 2013, della sentenza Torreggiani, che, tra le altre soluzioni suggerite per porre rimedio al cronico sovraffollamento degli istituti penitenziari italiani, ha incalzato il nostro Paese a po-

sito, va detto che il rapporto del *VERA Institute* non distingue tra controllo operato mediante dispositivi indossabili (braccialetti) e app *smartphone*, includendo tutte le forme di *Electronic monitoring (EM) digital tracking*.

¹⁰ Il 28 dicembre 2022, l'amministrazione dell'interno ha stipulato il contratto numero 30092, in vigore dal 1° gennaio 2023, per un servizio di «monitoraggio di soggetti mediante l'utilizzo di strumenti di sorveglianza elettronici, con servizi di monitoraggio, manutenzione correttiva ed evolutiva, nonché formazione, per un periodo di 45 mesi», al costo di 15.599.125. In linea con il precedente accordo (stipulato il 14 dicembre 2017), il nuovo contratto prevede l'attivazione di 1.000 dispositivi al mese, con la possibilità di utilizzarne fino al 20% in più, per un totale di 1.200 dispositivi.

¹¹ Si consideri, su tutto, il contenuto della delibera della Corte dei conti del 13 settembre 2012, n. 11/2012/G (resa disponibile dal sito *ristretti.it*), dove si evidenzia il costo esorbitante dell'operazione (v. in particolare le pagine 51-57).

¹² V. Raccomandazione CM/REC(2014) 4 del Comitato dei Ministri agli Stati Membri sulla Sorveglianza Elettronica.

tenziare anche tale modalità di controllo¹³. Parallelamente, si è fatta via via più impellente pure un'altra spinta, in un primo momento dovuta all'esigenza di ottemperare alla Convenzione di Istanbul e alla direttiva 2012/29/UE¹⁴, e che sarebbe poi scaturita nella progressiva edificazione di una procedura penale speciale, concepita quale strumento di contrasto alla violenza di genere e domestica.

Onde assecondare tutte queste sollecitazioni, il legislatore nazionale ha scelto di agire su più fronti. Innanzitutto, con una modifica all'art. 282-*bis* c.p.p. intervenuta nell'agosto del 2013¹⁵, è stata prevista la possibilità di porre la sorveglianza elettronica a presidio dell'allontanamento dalla casa familiare (misura oggi peraltro applicabile, ove si proceda per i reati di cui al comma 6 di tale disposizione, anche al di fuori dei limiti di pena previsti dall'articolo 280 c.p.p.). Pochi mesi dopo è arrivata l'innovazione dal maggiore impatto concreto, dovuta a uno degli interventi cosiddetti "svuotacarceri" (segnatamente il d.l. 23 dicembre 2013, n. 146, poi convertito con l. 21 febbraio 2014, n. 10), che, incappando in un'eclatante eterogenesi dei fini, ha maldestramente interpolato l'*incipit* dell'art. 275-*bis* c.p.p. In forza di tale variazione, il precetto tuttora obbliga il giudice cautelare ad associare *di default* il monitoraggio elettronico alla misura degli arresti domiciliari, potendo egli escludere l'applicazione del bracciale solo ove ritenga «non necessario» il ricorso a tale strumento, e dunque solo là dove sia in grado di dimostrarne e motivarne la superfluità. Se lo scopo della modifica all'art. 275-*bis* c.p.p. mirava a privilegiare il ricorso agli arresti domiciliari onde ridurre quello alla custodia in carcere, il suo effetto pratico è stato clamorosamente incongruo, essendosi risolto nell'ampliamento dello spazio operativo degli arresti domiciliari "elettronici" a discapito di quelli "semplici"¹⁶; così dando vita ad un «esempio calzante di *Net-Widening*»¹⁷.

¹³ Corte e.d.u., II Sez., 8 gennaio 2013, Torreggiani e altri c. Italia.

¹⁴ Il riferimento è naturalmente alla Convenzione del Consiglio d'Europa sulla prevenzione e la lotta alla violenza contro le donne e la violenza domestica, approvata dal Comitato dei ministri del Consiglio d'Europa il 7 aprile 2011, nonché alla "direttiva vittime" (dir. 2012/29/UE).

¹⁵ L'intervento è stato operato con d.l. 14 agosto 2013, n. 93, convertito con l. 15 ottobre 2013, n. 119.

¹⁶ In altri termini: nel rapporto tra custodia in carcere, arresti domiciliari elettronicamente monitorati e arresti domiciliari semplici, l'innovazione ha esteso l'ambito operativo degli "arresti domiciliari elettronici" al contempo riducendo quello degli arresti domiciliari controllati con metodi tradizionali, senza scalfire l'ambito di applicazione della custodia carceraria.

¹⁷ Così D. NEGRI, *Tecnologie e compressione della libertà personale: la sorveglianza con dispositivi elettronici dell'imputato sottoposto a misure cautelari*, in *Rev. Bras. de Direito Processual Penal*,

A seguire, con la L. 16 aprile 2015, n. 47 – e dunque nell’ambito di un disegno riformatore che ha investito la materia cautelare personale nel suo complesso – è stato aggiunto un comma 3-*bis* nel corpo dell’art. 275 c.p.p.: stando al precetto, quando sceglie la custodia in carcere il giudice deve specificare per quali ragioni ritiene inadeguati gli arresti domiciliari con braccialetto. Tale disposizione – a rigore superflua – risulta ben più fedele allo scopo cui dichiaratamente mirava già il legislatore del 2013, e individua l’ennesima fra le numerose esplicitazioni del principio di adeguatezza¹⁸.

All’esito delle interpolazioni rapidamente succedutesi nel biennio compreso dal 2013 al 2015, e in particolare per effetto della seconda (che, obbligandolo a spiegare per quali ragioni ha scelto di non associare il braccialetto elettronico agli arresti domiciliari, ha significativamente responsabilizzato il giudice cautelare), questo tipo di monitoraggio è finalmente decollato anche sul piano empirico, determinando il rapido esaurimento delle scorte di apparecchi messi a disposizione dell’autorità giudiziaria. Tanto che, appurata la difficoltà di attuare compiutamente quanto preteso dalla legge, le dotazioni tecnologiche sono state usate solo in abbinamento alla misura degli arresti domiciliari, senza che l’impiego nei confronti dei condannati in detenzione domiciliare e degli imputati attinti dall’allontanamento dalla casa familiare abbia effettivamente attecchito nella prassi. L’insufficienza delle dotazioni ha addirittura portato al fiorire di vere e proprie “liste d’attesa”: un *escamotage* informale (poiché problematicamente non previsto dalla legge) volto a gestire nel modo il più possibile ordinato le scorte messe a disposizione dell’autorità giudiziaria, onde scongiurare eventuali disparità di trattamento fra imputati ammessi agli arresti domiciliari con sorveglianza elettronica ed imputati costretti in carcere. Come noto, la situazione venutasi a creare all’indomani di quella stagione di riforme ha addirittura costretto le Sezioni unite a fornire indicazioni al giudice cautelare che, una volta appurata la carenza del dispositivo, si trovi a dover scegliere, in seconda battuta, tra la custodia in carcere e gli arresti domiciliari semplici (ossia non elettronicamente monitorati)¹⁹.

Dopo un periodo segnato da problemi dovuti all’avvicendamento tra

vol. 5, n. 3, 2019, p. 1262. L’espressione (che si deve a S. COHEN, *Punitive city. Notes on the dispersal of social control*, in *Contemporary Crises*, 1979, vol. 3, 4, p. 339 ss.) allude al fenomeno dell’ampliamento del controllo penale in forza del quale le misure alternative alla detenzione vanno ad aggiungersi a quest’ultima, e non a sostituirla.

¹⁸ Il principio di adeguatezza è declinato in via generale nel primo comma dell’art. 275, e, in termini specificamente riferiti alla custodia in carcere, negli artt. 275 comma 3 e 292 comma 2 lett. *c bis*, c.p.p.

¹⁹ Cfr. Cass., Sez. un., 28 aprile 2016, n. 20769, in *C.e.d.*, n. 266651, che ha chiarito come, in mancanza di braccialetto elettronico, «escluso ogni automatismo nei criteri di

diversi enti appaltatori (prima *Telecom* e poi *Fastweb*)²⁰, forieri di ulteriori ritardi e difficoltà nell'approntamento delle risorse tecnologiche, un significativo impulso a valorizzare la sorveglianza elettronica è poi arrivato con la pandemia²¹. Come già dopo la sentenza Torreggiani, anche in tale frangente la spinta è stata intuibilmente associata alla volontà di ridurre il ricorso al carcere, in uno scenario condizionato dall'esigenza di ridurre il più possibile il rischio di contagio, anche in fase esecutiva della pena²².

Se queste sono le tappe precedenti, gli ultimi anni descrivono un nuovo momento di svolta, simile a quello registratosi nel 2015 ma potenzialmente foriero di risvolti pratici più significativi. Il forte allarme suscitato dalla violenza di genere e di quella domestica ha infatti portato il legislatore a irrobustire i tratti di specialità della disciplina processuale approntata per scongiurare la reiterazione delle condotte che tipicamente contraddistinguono tali manifestazioni criminose. A partire dal 2019, con la cosiddetta legge sul “codice rosso”, i riformatori sono infatti a più riprese intervenuti sul rito cautelare gradualmente allestito per rispondere a tali forme di devianza, incrementandone i tratti di specialità e – ciò che più conta ai nostri fini – mostrando di fare grande affidamento sul monitoraggio elettronico. Non solo: nel 2017, come vedremo, il possibile ricorso alla sorveglianza elettronica è stato esteso anche al controllo sul rispetto delle prescrizioni imposte con le misure di prevenzione.

Ai nostri fini, e senza stare a descrivere nel dettaglio un sistema di regole intricato e di ormai faticosa lettura, i pilastri dell'ultima stagione di novelle che hanno investito la materia cautelare sono questi: la possibilità, accordata al giudice con la L. 19 luglio 2019, n. 69, di associare il monitoraggio elettronico al divieto di avvicinarsi alla vittima; la contestuale estensione della possibilità di applicare il divieto di avvicinarsi ai luoghi frequentati dalla persona offesa al catalogo di reati del “codice rosso”

scelta delle misure», il giudice debba svolgere una nuova valutazione, onde scegliere se ricorrere agli arresti domiciliari “semplici” o alla custodia cautelare in carcere.

²⁰ Dopo anni di proroghe e rinnovi con *Telecom*, nel 2017 il Ministero dell'interno ha bandito una procedura aperta, che ha portato alla stipula, nel dicembre dello stesso anno, del contratto con il RTI “*Fastweb S.p.A./ Vitrociset S.p.A.*” (Vitrociset è poi confluita in Leonardo), avente ad oggetto il «servizio di monitoraggio di soggetti con l'utilizzo di strumenti di sorveglianza elettronici (cd. braccialetto elettronico)». A tale contratto sono poi succedute proroghe successive. La convenzione in essere è tuttora con *Fastweb*.

²¹ V. sul punto F. BAILO, *op. cit.*

²² Stando al XVIII rapporto sulle condizioni di detenzione di Antigone (in *rapportoantigone.it*), grazie al cosiddetto decreto “Cura Italia”, dalle 251 applicazioni della detenzione domiciliare con braccialetto elettronico disposte nel 2019 si è passati alle 2.605 del 2020. La pandemia non ha invece inciso sul numero complessivo di imposizioni del braccialetto elettronico in fase cautelare (che sono state 2.618 nel 2020, 2.753 nel 2019 e 2.840 nel 2018).

(di cui all'art. 282-*bis* comma 6 c.p.p.) indipendentemente dal ricorrere dei presupposti edittali *ex* art. 280 c.p.p., operata con la legge 24 novembre 2023, n. 168 (c.d. "legge Roccella"); l'automatico abbinamento del monitoraggio elettronico all'allontanamento dalla casa familiare e al divieto di avvicinarsi ai luoghi abitualmente frequentati dalla vittima o alla vittima stessa: abbinamento che, già affidato alla discrezionalità del giudice rispettivamente con il d.l. n. 93 del 2013 e la legge n. 69 del 2019, è stato reso obbligatorio dalla l. n. 168 del 2023, con un irrigidimento destinato a ripercuotersi sul tasso di concreta operatività dello strumento²³; l'introduzione di un inedito criterio di priorità nell'esercizio dell'azione cautelare, stabilito sempre in relazione al catalogo dei reati del "codice rosso" e che, pur non intervenendo direttamente sulla disciplina dedicata al braccialetto elettronico, incide comunque sul suo spazio operativo, visto che sollecita il pubblico ministero a presentare la richiesta cautelare entro trenta giorni dall'iscrizione della notizia di reato nel registro *ex* art. 335 c.p.p.²⁴, peraltro nell'ambito di procedimenti per i quali già vigono regole volte a garantire una corsia preferenziale nello svolgimento delle indagini²⁵.

Come premesso, il braccialetto elettronico è poi sbarcato anche in un altro settore dell'ordinamento, ossia quello delle misure di prevenzione. Lo ha fatto con il d.l. 20 gennaio 2017, n. 14 (conv. con mod. con la legge 18 aprile 2017, n. 48), che, inserendo il comma 3-*bis* all'art. 6 del codice antimafia, ha introdotto la possibilità di associare modalità di controllo elettroniche a presidio del rispetto degli obblighi e delle prescrizioni ine-

²³ Con previsioni del tutto sovrapponibili, per il caso di mancato consenso all'applicazione del braccialetto elettronico da parte del destinatario delle misure dell'allontanamento dalla casa familiare o del divieto di avvicinarsi ai luoghi frequentati dalla vittima, il penultimo periodo del sesto comma dell'art. 282-*bis* c.p.p. e del primo comma dell'art. 282-*ter* c.p.p. impongono l'applicazione, anche congiunta, di una misura cautelare più grave «con lo stesso provvedimento».

²⁴ Si allude al meccanismo descritto dal combinato disposto degli artt. 362-*bis* c.p.p. e 127 comma 1-*bis* disp. att., che mira ad incentivare il concreto ricorso alle cautele personali, nella sostanza caldeggiando una celere presentazione della domanda *ex* art. 292 comma 1 c.p.p., con un meccanismo reso cogente dall'obbligo di trasmettere al procuratore generale presso la Corte d'appello i dati relativi al rispetto dei termini prescritti dall'art. 362-*bis* c.p.p.

²⁵ Il riferimento è qui al tenore dell'art. 362 comma 1-*ter* c.p.p., che prescrive di procedere all'ascolto della persona offesa entro termini particolarmente stringenti. L'obbligo è stato da ultimo rafforzato con la legge 2 dicembre 2025, n. 181, che, oltre ad aver ampliato il novero dei procedimenti in cui esso è destinato ad operare, specifica altresì che all'audizione della vittima debba procedere il pubblico ministero personalmente, là dove la persona offesa abbia «avanzato motivata e tempestiva richiesta» in tal senso; è comunque fatta «salva la possibilità di delegare la polizia con decreto motivato» (ma sempre che non si proceda per il delitto aggravato di cui all'art. 612-*bis* quarto comma c.p.).

renti alla sorveglianza speciale. Più di recente, e in particolare con la legge n. 168 del 2023, la medesima modalità di controllo è stata estesa anche alle prescrizioni cosiddette *anti-stalking* di cui all'art. 4, comma 3-*bis* del d.lgs. 6 settembre 2011, n. 159, applicabili agli indiziati di delitti di cui all'art. 4, comma 1 lett. *i-ter* del medesimo codice antimafia²⁶.

Gli effetti di questa nuova valorizzazione normativa della sorveglianza elettronica – pressoché automaticamente associata alle misure dell'allontanamento dalla casa familiare e del divieto di avvicinarsi alla persona offesa, come pure alla “sorveglianza speciale *anti-stalking*” – non si sono fatti attendere, se è vero che, all'indomani della “legge Roccella” del 2023, si è di nuovo riscontrata l'insufficienza delle dotazioni di apparecchi²⁷. A tale riguardo, *Fastweb* ha parlato di un «imprevedibile stravolgimento delle tipologie di braccialetti richieste rispetto alle previsioni contrattuali», e del «conseguente esaurimento delle scorte disponibili di dispositivi per il tracciamento di prossimità», dovuto alla «modifica della prassi seguita alle normative introdotte dalla legge 168/2023»²⁸.

Il salto qualitativo è palese: come torneremo a rimarcare, il cosiddetto «tracciamento di prossimità» postula infatti l'impiego di una tecnologia diversa da quella tradizionalmente impiegata per controllare il rispetto dell'obbligo di non allontanarsi dal domicilio caratteristico del presidio *ex* art. 284 c.p.p.; una tecnologia che, come vedremo subito, si presta a seguire ogni spostamento, tanto dell'imputato quanto della persona offesa, con un livello di intrusività davvero rimarchevole.

In tale quadro, va però segnalata un'ultima, recentissima novità, in grado di spostare gli equilibri di sistema: la legge 2 dicembre 2025, n.

²⁶ V. art. 6 comma 3-*ter* d.lgs. n. 159 del 2011. A differenza di quanto stabilito dal comma precedente (inserito nel 2017), questo precetto si esprime in termini perentori, prevedendo l'obbligatoria associazione del monitoraggio elettronico alle prescrizioni cosiddette *antistalking* imposte al prevenuto. In questo caso, la conseguenza della negazione del consenso da parte dell'interessato implica la fissazione di una durata della misura non inferiore a tre anni, oltre alla prescrizione di presentarsi all'autorità di pubblica sicurezza con cadenza almeno bisettimanale e imposizione (salva diversa valutazione) del divieto o dell'obbligo di soggiorno.

²⁷ L'effetto della “legge Roccella” è stato simile a quello già registratosi all'indomani delle modifiche del 2013-2015, ed è stato in qualche modo confermato dalla sentenza costituzionale n. 173 del 2024, che, oltre ad aver ritenuto non fondata la questione sull'impossibilità di stabilire una distanza dalla vittima inferiore a 500 metri, ha respinto le censure in ordine all'obbligatoria applicazione del dispositivo. V. in proposito F. MENDITTO, *Ancora sul braccialetto elettronico e sull'art. 7 d.l. n. 178/2024*, in *Sist. pen.*, 19 dicembre 2024.

²⁸ Il virgolettato è tratto da una nota indirizzata da *Fastweb* ai Tribunali, e i cui contenuti sono riportati da L. FERRARELLA, *Braccialetti elettronici anti stalking, la legge ne chiede di più ma le scorte sono esaurite: «I detenuti in attesa restano in cella»*, in *milano.corriere.it*, 10 aprile 2024.

181, ossia l'ennesima novella intervenuta per inasprire il regime cautelare (e non solo) previsto per gli indiziati dei reati espressione di violenza di genere e domestica.

Tra le copiose innovazioni inserite con questa riforma, va segnalata almeno quella sfociata nell'inserimento di un nuovo comma 3.1 in seno all'art. 275 c.p.p., in forza del quale, quando sussistono gravi indizi di colpevolezza in ordine ad una serie di delitti (tra cui spiccano quello di tentato omicidio e di tentato femminicidio, maltrattamenti, lesioni personali, mutilazioni genitali femminili, *stalking*, diffusione illecita di immagini o video sessualmente espliciti: tutti nelle forme aggravate precisate dalla disposizione), «sono applicate le misure degli arresti domiciliari o della custodia cautelare in carcere salvo che siano acquisiti elementi dai quali risulti che non sussistono esigenze cautelari ovvero nei casi in cui le stesse, anche in relazione al pericolo per la vita o l'integrità fisica o psichica della persona offesa, possano essere soddisfatte da altre misure cautelari».

Tale precetto si pone in decisa controtendenza, sebbene in senso tutt'altro che garantistico, e finirà per incidere sull'ambito operativo dell'allontanamento dalla casa familiare e del divieto di avvicinarsi alla persona offesa: misure nei confronti delle quali, anche ove abbinate alla sorveglianza elettronica già prevista come obbligatoria, il legislatore mostra evidentemente i primi segni di diffidenza, a beneficio degli arresti domiciliari, soggetti a una forma di monitoraggio meno problematica e più semplice da gestire da parte delle forze dell'ordine.

4. *Le diverse tecnologie impiegate*

Sulla scorta di quanto premesso, diverse sono le possibili forme di monitoraggio a fini penali e di prevenzione. Gli scopi della legge sono infatti perseguibili attraverso l'impiego, anche integrato, di forme di controllo fra loro diversificate. Anzi: sono proprio le nuove potenzialità dischiuse dallo sviluppo tecnologico ad aver determinato l'investimento politico sul braccialetto operato negli ultimi anni, volto a rafforzare il contrasto alla violenza di genere e domestica sul piano tanto cautelare quanto preventivo. Salvo difficoltà pratiche o malfunzionamenti, i dispositivi di ultima generazione permettono infatti di controllare il rispetto delle prescrizioni obbligatorie in cui si sostanziano i divieti di avvicinarsi a determinati luoghi o persone.

Benché incredibilmente la legge non ne faccia menzione – limitandosi a parlare di «procedure di controllo mediante mezzi elettronici o altri strumenti tecnici», senza specificarne i connotati: e dunque, in definitiva,

violando il principio di legalità²⁹ –, la pratica quotidiana presenta quattro scenari, distinti fra loro quanto a livello di pervasività e di tecnologia impiegata: il monitoraggio domiciliare, il monitoraggio con tracciamento, il solo tracciamento e il tracciamento di prossimità³⁰.

Mentre il *monitoraggio domiciliare* (che in genere si basa sulla tecnologia a radiofrequenza) si limita a verificare che il bersaglio non superi il perimetro di un determinato luogo, il *monitoraggio con tracciamento* prevede tanto il controllo all'interno di luoghi predefiniti, come il domicilio, quanto la possibilità di seguire gli spostamenti dell'imputato all'esterno. In caso di allontanamento non autorizzato o di manomissione dei dispositivi di controllo elettronico, viene generato un allarme, inviato al Centro di Monitoraggio Elettronico (CEM) per avvisare le forze di polizia. Dal canto suo, il cosiddetto *tracciamento* monitora i movimenti del soggetto, lanciando un *alert* ove la persona sottoposta a controllo acceda a determinate zone di esclusione o esca da zone di inclusione predefinite (senza che venga contestualmente effettuato anche il monitoraggio domiciliare). Infine, il quarto scenario è quello del *tracciamento di prossimità*, detto anche *anti-stalking*, normativamente previsto dal 2013 ma applicato in modo quantitativamente significativo solo di recente (dopo che il legislatore del 2023 ne ha sancito l'obbligatoria associazione alle misure di cui agli artt. 283-*bis* e 283-*ter* c.p.p.): in questo caso, anche la potenziale vittima viene dotata di un dispositivo (non da indossare ma da recare con sé) in grado di rilevare la presenza dell'aggressore nelle vicinanze e di generare un allarme presso il Centro di monitoraggio elettronico³¹.

Intuibilmente, gli scenari di sorveglianza consentiti dall'utilizzo della

²⁹ In tal senso, v. già D. NEGRI, *op. cit.*, p. 1266, che, dopo aver ricordato la svolta del 2013 (quando il legislatore ha deciso di estendere il controllo a distanza anche all'allontanamento dalla casa familiare), segnala come in tale frangente il governo si fosse limitato a stipulare una nuova convenzione con la società di telefonia concessionaria del servizio, onde ottenere una quota della fornitura di braccialetti munita della funzione GPS: «qui siamo addirittura di fronte alla eterointegrazione per via negoziale – cioè ad una forma di privatizzazione – di un elemento essenziale della fattispecie che regola l'intensità del potere cautelare».

³⁰ Questa sistematizzazione è tratta dai contenuti del «capitolato tecnico per l'affidamento di un servizio di monitoraggio di soggetti con l'utilizzo di strumenti elettronici», predisposto dal Ministero dell'interno, datato il 2 dicembre 2016 e reperibile sul sito *poliziadistato.it*. V. anche P. ALLEGRI, *Ventesimo rapporto sulle condizioni di detenzione. Dispositivi di monitoraggio elettronico*, in *rapportoantigone.it*, 8 aprile 2024.

³¹ Mentre il *track*, ossia il terminale impiegato dall'ipotetico *stalker*, ovviamente non fornisce alcuna indicazione in ordine alla posizione della persona offesa, il dispositivo in uso alla vittima emette un segnale acustico e un avviso di pericolo sul *display*. Gli allarmi di prossimità generano segnalazioni alla centrale operativa, e la relativa gestione verrà poi demandata alle forze dell'ordine preposte alla tutela della vittima.

tecnologia GPS, atta a seguire ogni movimento del prevenuto, presentano un livello di intrusività ben maggiore rispetto a quello caratteristico del monitoraggio domiciliare, che viceversa si limita a controllare la presenza della persona all'interno di un unico spazio predeterminato.

Oltre che per il loro diverso livello di invadenza, le diverse tecnologie impiegate si differenziano anche per difficoltà applicative, efficienza e precisione. La questione è esplosa di recente, e in particolare dopo che gli automatismi inseriti nel 2023 hanno fatto impennare le applicazioni del tracciamento *anti-stalking*: tale meccanismo è molto più sofisticato di quello tradizionalmente deputato al controllo degli arresti domiciliari, consentendo una geolocalizzazione molto precisa; tuttavia, esso è al contempo esposto a falle, dovute a numerose possibili eventualità, fra cui l'interruzione di segnale e l'esaurimento della batteria di cavigliera e telefonini in dotazione di imputato e vittima³²: eventualità, queste, in cui si attiva comunque il sistema di allarme, ancorché mediante *alert* differenziati e ordinati in termini di gravità.

Proprio per questa ragione, il sistema registra una serie di informazioni – tra cui ora, latitudine o longitudine dell'allarme registrato, come pure velocità e direzione di marcia – che permettono di chiarire, *ex post*, se eventuali avvicinamenti possano o meno ritenersi casuali³³.

5. Possibili ricadute probatorie

Stando alle diverse tecnologie oggi in uso, i modi del controllo elettronico presentano livelli di invasività non omologabili fra loro. Ma ancorché in modo differenziato, essi sono tutti forieri di potenziali ricadute probatorie.

La prima fra tali eventuali ricadute è ovvia, poiché strettamente connessa allo scopo del braccialetto elettronico, che è quello di verificare il successo o il fallimento del rapporto fiduciario su cui si regge la misura obbligatoria inizialmente privilegiata rispetto alla cattività carceraria (o ad altra misura, comunque più severa). Essa è a vario titolo regolata innanzitutto dall'art. 276 c.p.p., negli anni reso oggetto di plurime e significative rivisitazioni, intervenute anche molto di recente.

Come noto, il primo comma della disposizione accorda al giudice il

³² Una descrizione tecnica più precisa, maturata sulla base dell'esperienza del circondario della Procura di Tivoli, è riportata in F. MENDITTO, *Ancora sul braccialetto elettronico*, cit., nota 2.

³³ P. REALE, *Il braccialetto elettronico: descrizione del sistema, con approfondimento della funzionalità "anti-stalking"*, in *sicurezzaejustizia.com*, 3 novembre 2025.

potere di disporre la sostituzione o il cumulo della misura originariamente disposta con altra più grave, «tenuto conto dell'entità, dei motivi e delle circostanze della violazione», potendo portare financo alla custodia in carcere indipendentemente dal rispetto dei limiti edittali stabiliti in via generale dall'art. 280 c.p.p. (così il terzo comma di tale ultima disposizione)³⁴. Sennonché, malgrado il primo comma dell'art. 276 sia sostanzialmente rimasto invariato, il relativo ambito operativo si è progressivamente eroso, andando a ridurre la discrezionalità del giudice dinanzi alla constatata trasgressione. Per l'ipotesi in cui ad essere violate siano le prescrizioni degli arresti domiciliari concernenti il divieto di allontanarsi dalla propria abitazione (o da altro luogo di privata dimora), il successivo comma 1-*ter* impone infatti la sostituzione della misura con la custodia cautelare in carcere, «salvo che il fatto sia di lieve entità». Il modo in cui il precetto è formulato lascia spazio a pochi dubbi, di fatto riducendo sensibilmente il perimetro dell'apprezzamento giudiziale.

Per quanto l'automatismo secco introdotto nel 2000³⁵ sia stato poi temperato nel 2015 con la possibile eccezione del fatto di lieve entità, interpolazioni più recenti hanno esteso lo stesso tipo di reazione vincolata anche alle ipotesi di manomissione, come pure di una o più condotte gravi o reiterate che impediscano od ostacolino il regolare funzionamento dei mezzi elettronici e degli altri strumenti tecnici di controllo di cui all'articolo 275-*bis*, anche quando applicati ai sensi degli artt. 282-*bis* e 282-*ter*³⁶. In tutti questi casi, e sempre che il fatto non sia (appunto) di lieve entità, il giudice è inderogabilmente chiamato a disporre l'aggravamento nelle forme obbligate della custodia in carcere. Alla luce dell'attuale fisionomia di questo automatismo, è piuttosto chiara la posta in gioco, in particolare là dove le misure trasgredite siano quelle dell'allontanamento dalla casa familiare e del divieto di avvicinarsi alla persona offesa. Se

³⁴ Il primo comma del 276 c.p.p. altresì stabilisce che quando ad esser trasgredite sono le prescrizioni inerenti a una misura interdittiva, il giudice può disporre la sostituzione o il cumulo anche con una misura coercitiva.

³⁵ Il comma 1-*ter* era stato introdotto con il d.l. n. 341 del 2000, conv. con mod. con l. n. 4 del 2001 (ossia con la medesima novella cui si deve l'ingresso del braccialetto elettronico nel nostro sistema), e, per il caso di trasgressione alle prescrizioni degli arresti domiciliari concernenti il divieto di non allontanarsi dalla propria abitazione o da altro luogo di privata dimora, imponeva al giudice di disporre «la revoca della misura e la sua sostituzione con la custodia cautelare in carcere». Con la legge 16 aprile 2015, n. 47, l'automatismo è stato attenuato con l'inserimento della deroga concernente il «fatto di lieve entità».

³⁶ Il riferimento alla manomissione è stato introdotto con la legge n. 168 del 2023, mentre quello a «una o più condotte gravi o reiterate che impediscono o ostacolano il regolare funzionamento» del dispositivo si deve al d.l. 29 novembre 2024, n. 178, conv. con mod. con l. 23 gennaio 2025, n. 4.

infatti, nell'ideale scala di decrescente afflittività che contraddistingue il ventaglio dei presidi coercitivi, gli arresti domiciliari si collocano subito sotto la custodia in carcere, lo stesso non può dirsi per le due misure normative dagli artt. 282-*bis* e 282-*ter* c.p.p., meno afflittive tanto della cattività carceraria quanto di quella domiciliare. La presunzione di pericolosità associata alla manomissione, nonché a una unica condotta, sia pure «grave», che «impedisca o ostacoli il regolare funzionamento del dispositivo», si rivela dunque gravida di ricadute pesanti, aprendo pressoché inevitabilmente le porte del carcere pure a chi risulti indiziato per un delitto punito con una pena non necessariamente troppo severa. Come già ricordato, infatti, dopo la riforma Roccella del 2023, ove si proceda per uno dei reati per i quali vige il sotto-sistema del “codice rosso”, l'allontanamento dalla casa familiare e il divieto di avvicinamento sono applicabili anche al di fuori dei limiti stabiliti dall'art. 280 c.p.p.

Alla luce di ciò, è chiaro come l'inserimento di vincoli sempre più stringenti alle valutazioni del giudice, insiti nell'imposizione di una risposta automatica e predeterminata alla constatazione della trasgressione, finisca per rendere quest'ultima di per sé decisiva. Decisiva e delicata: specie considerando la difficoltà di distinguere gli allarmi reali da quelli “falsi”, come pure il livello di affidabilità dei dati; e altresì considerando che, oggi, le condotte rilevanti non sono più la sola manomissione, ma anche, appunto, «una o più condotte gravi o reiterate che impediscono o ostacolano il regolare funzionamento».

Come già premesso, l'aggravamento del regime coercitivo individua la ricaduta probatoria più immediata e ovvia, poiché corrispondente alla funzione dell'apparecchio. Non si tratta, tuttavia, della sola, ben potendosene immaginare anche di ulteriori.

Innanzitutto ove l'inottemperanza alle prescrizioni connessa al regime cautelare identifichi essa stessa un fatto-reato. È il caso dell'evasione, dell'inottemperanza all'ordine impartito dal giudice, del danneggiamento del dispositivo. Fattispecie cui negli anni se ne sono andate ad aggiungere di ulteriori, nate proprio per salvaguardare l'integrità del dispositivo o comunque per presidiare (con la forza della generalprevenzione) il rispetto delle prescrizioni connesse a misure di natura obbligatoria: è il caso dell'alterazione del funzionamento dei mezzi elettronici o degli altri strumenti tecnici adottati nei confronti dell'imputato, o comunque di sottrazione fraudolenta alla loro applicazione o al loro funzionamento³⁷; come pure,

³⁷ Le ultime condotte menzionate nel testo sono espressamente previste e punite (con una pena compresa da uno a tre anni) dall'art. 18 del d.l. 24 novembre 2000, n. 341, conv. con mod. con l. 19 gennaio 2001, n. 4.

a partire dal 2019, delle condotte descritte dall'art. 387-*bis* c.p.p., ossia la violazione dei provvedimenti di allontanamento dalla casa familiare e del divieto di avvicinamento ai luoghi frequentati dalla persona offesa, oggi punite con la reclusione da sei mesi a tre anni e sei mesi³⁸.

Non solo. In particolare nel caso di *tracciamento*, per sua natura in grado di guadagnare la maggior mole di informazioni, le conoscenze acquisite tramite il monitoraggio elettronico potrebbero assumere rilevanza probatoria anche rispetto ad ulteriori reati.

In primis – là dove lo scopo di deterrenza in concreto fallisca – in relazione ai reati caratteristici della progressione criminosa ricorrente nei casi di violenza di genere o domestica: quali ad esempio lo *stalking*, le molestie, come pure altre fattispecie penali che spesso (e purtroppo) costituiscono espressione di tali devianze.

Ma più in generale, non limitandosi a registrare l'allontanamento dal domicilio, ed anzi seguendo gli spostamenti del soggetto sottoposto a controllo in modo permanente, il *tracking* è più facilmente in grado di procacciare conoscenze rilevanti anche rispetto a reati sguarniti di qualsiasi nesso con l'originaria decisione di applicare il controllo elettronico³⁹. E ciò – si badi – in ordine alla geolocalizzazione e ai movimenti tanto dell'imputato quanto della persona offesa (che parimenti reca con sé un dispositivo, pur senza indossarlo).

Malgrado la particolare delicatezza di questa categoria di dati (che, registrando i luoghi frequentati, permettono di inferire abitudini, relazioni sociali, condizioni di salute e molti altri aspetti della vita quotidiana)⁴⁰, il

³⁸ Il vigente trattamento sanzionatorio è stato oggetto di inasprimento con la legge 24 novembre 2023, n. 168 (c.d. "legge Roccella"), la quale, in relazione a tale ipotesi di reato, ha stabilito un regime processuale speciale, descritto dall'art. 382-*bis* c.p.p., che contempla un'ipotesi di arresto in flagranza differita per chi, «sulla base di documentazione videofotografica o di altra comunicazione legittimamente ottenuta da dispositivi di comunicazione informatica o telematica», risulti aver commesso, fra l'altro, proprio il reato di cui all'art. 387-*bis* c.p.p.

Con la recentissima legge 2 dicembre 2025, n. 181, la fattispecie di cui all'art. 387-*bis* c.p.p. è stata inserita nel catalogo di reati per i quali non vige il divieto di applicare la custodia in carcere là dove il giudice ritenga che, all'esito del giudizio, la pena detentiva irrogata non sarà superiore a tre anni.

³⁹ In ambito estero, questa medesima considerazione si poteva già riscontrare in A. HUCKLESBY-K. BEYENS-MIRANDA BOONE-F. DÜNKEL- G. MCIVOR-H GRAHAM, *Creativity and effectiveness in the use of electronic monitoring: a case study of five European jurisdictions*: paper assai ricco di informazioni, illustrativo dei risultati di una ricerca (conclusasi nel 2016) che ha messo a confronto l'impiego del braccialetto elettronico in cinque diversi contesti europei (Belgio, Olanda, Germania, Inghilterra e Galles, Scozia) (cfr. files01.core.ac.uk/download/pdf/42545322.pdf, p. 5).

⁴⁰ Proprio per questo, la giurisprudenza della Corte europea (come pure quella della

legislatore italiano non si è mai fatto carico di circoscrivere i loro possibili impieghi. Come pure, ancor prima, i relativi tempi di conservazione. Nel silenzio della legge, è infatti arduo rinvenire un limite tassativo nell'art. 4 comma 3 del decreto 2 febbraio 2001 del Ministero dell'Interno⁴¹, a norma del quale «i dati personali trattati nell'uso dei mezzi elettronici e degli altri strumenti tecnici di controllo sono utilizzati per le finalità di applicazione del capo VII del decreto legge 24 novembre 2000, n. 341 [...]». Il rinvio ai contenuti del capo VII del “decreto anti-scarcerazioni” è infatti molto poco risolutivo, visto che i diversi articoli che compongono tale ristretto *corpus* non esplicitano alcuna finalità, ancorché dando evidentemente per scontato che essa vada individuata nel controllo dell'obbligo di non allontanarsi dal domicilio onde eventualmente aggravare il trattamento coercitivo nel frattempo mostratosi inadeguato per difetto.

Quando il decreto del 2 febbraio 2001 è stato scritto, il monitoraggio poteva essere associato alla sola custodia e alla detenzione domiciliare, e funzionava grazie a una tecnologia assai meno invasiva di quella utilizzata nelle distinte ipotesi di tracciamento (che si nutre del GPS). Tuttavia, nel frattempo il quadro normativo ed empirico si è evoluto. Nel sistema sono infatti state inserite una serie di fattispecie penali (v. art. 387-*bis* c.p.) pensate per sanzionare colui che alteri il corretto funzionamento del dispositivo tecnologico: una novità, questa, cui è difficile non associare il possibile riutilizzo dei dati acquisiti dal braccialetto nel processo volto ad accertare tali condotte penalmente rilevanti. Rispetto al 2001, l'astratta utilità probatoria dei dati offerti dal braccialetto si è dunque arricchita. A fronte di ciò, e quindi anche volendo trascurare l'inidoneità di un decreto ministeriale a colmare il silenzio della legge, l'art. 4 comma 3 del decreto 2 febbraio 2001 comunque non si presta ad impedire che i dati acquisiti grazie alla sorveglianza elettronica possano essere impiegati anche per fini ulteriori rispetto all'aggravamento del regime coercitivo in corso di esecuzione.

Nessuna preclusione sembra potersi inferire neppure dall'art. 3 del

Corte di giustizia: v. *infra*, nota 45) riconduce i dati di geolocalizzazione all'art. 8 CEDU, anche là dove concernente spostamenti in luoghi pubblici. Sul tema, la pronuncia capostipite è Corte e.d.u., Sez. V, 2 settembre 2010, Uzun c. Germania, relativa al monitoraggio mediante GPS.

⁴¹ Il decreto (varato all'indomani dell'ingresso della sorveglianza elettronica nel nostro sistema e rubricato «[m]odalità di installazione ed uso e descrizione dei tipi e delle caratteristiche dei mezzi elettronici e degli altri strumenti tecnici destinati al controllo delle persone sottoposte alla misura cautelare degli arresti domiciliari nei casi previsti dall'art. 275-*bis* del codice di procedura penale e dei condannati nel caso previsto dall'art. 47-*ter*, c. 4-*bis*, della legge 26/7/1975, n. 354») è stato pubblicato sulla G.U. n. 38 del 15 febbraio 2001, ed è tuttora vigente.

d.lgs. 18 maggio 2018, n. 51, con cui il legislatore italiano ha recepito la direttiva (UE)/2016/680 (*Law Enforcement Directive*, o *LED*), relativa al trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. Infatti, dopo aver richiamato, al primo comma, i principi di liceità, minimizzazione, limitazione delle finalità stabiliti dalla direttiva, al capoverso l'art. 3 fa salva la possibilità di un trattamento dei dati personali per uno degli scopi di cui all'art. 1 comma 2, e dunque anche a fini di «prevenzione, indagine, accertamento e perseguimento di reati [...]» «divers[i] da quell[i] per cui i dati sono raccolti»; e ciò «conformemente al diritto dell'Unione europea o dell'ordinamento interno e se il trattamento è necessario e proporzionato a tale diversa finalità, conformemente al diritto dell'Unione europea o dell'ordinamento interno».

Tale disposizione è di per sé sguarnita di un autonomo contenuto precettivo, limitandosi a richiamare l'operatività di meccanismi di circolazione probatoria – e dei relativi limiti – posti da altre discipline, comunitarie o interne.

In forza delle loro caratteristiche, le conoscenze acquisibili grazie al braccialetto elettronico possono essere accostate a quelle considerate dall'art. 132 cod. *privacy*, dedicato alla conservazione, da parte dei *provider*, dei dati di traffico telefonico e telematico. Come noto, infatti, tale disciplina si applica anche ai dati necessari per instradare la comunicazione, tra cui celle di aggancio, dati tecnici che consentono di ricostruire luogo e momento della comunicazione, parametri di rete che individuano l'ubicazione del telefono⁴².

Da un punto di vista morfologico, la conoscenza della posizione e dei movimenti del braccialetto presenta dunque chiari tratti di somiglianza con la determinazione dell'ubicazione dello *smartphone* ottenibile mediante l'acquisizione dei dati esterni del traffico telefonico e telematico. Anzi: la conoscenza potenzialmente guadagnata dal braccialetto elettronico deputato al tracciamento risulta, oltre che continua, anche molto più puntuale, non limitandosi a ricondurre il dispositivo a determinate celle telefoniche⁴³.

⁴² L'art. 2 della direttiva relativa al trattamento dei dati personali (2002/58/CE) qualifica come «dati relativi all'ubicazione» «ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico». Di conseguenza, i dati di geolocalizzazione del dispositivo sono soggetti al rispetto delle regole stabilite in materia di *data retention* sia da tale direttiva (v. Corte giust., sent. 2 marzo 2021, H.K. c. Prokuratuur, C-746/18), sia dalla disciplina interna, stabilita dall'art. 132 cod. *privacy* (v. fra le altre Cass., Sez. VI, 11 gennaio 2023, n. 15836, in *C.e.d.*, n. 284590).

⁴³ La tecnologia mediante GPS fornisce una localizzazione molto più precisa e utile

Facendo leva sulla somiglianza tra i dati registrati dal braccialetto elettronico e quelli nella disponibilità dei *provider*, di primo acchito viene dunque istintivo evocare l'applicabilità dell'art. 132 del codice *privacy*. Anche perché, contrariamente a quanto si può ritenere, i flussi di dati GPS ottenuti tramite il braccialetto non sono nella disponibilità diretta della polizia, ma del fornitore tecnico (oggi *Fastweb/Leonardo*), che gestisce l'avvio delle segnalazioni di allarme diramate alle forze dell'ordine dalla centrale operativa del Ministero dell'Interno.

Sennonché, le due situazioni non sembrano omologabili. Nel caso del braccialetto elettronico, il controllo (operante *in itinere* e non *ex post*) è conosciuto dall'individuo, che ha accettato di rendersi bersaglio dell'autorità giudiziaria penale. Sebbene anche la possibilità dell'autorità giudiziaria penale di attingere ai dati esterni del traffico telefonico e telematico conservati dai fornitori dei relativi servizi sia legalmente nota all'interessato (poiché riconosciuta e regolata in una norma di legge), la differenza tra le due ipotesi messe a confronto resta comunque rilevante. Come vedremo, l'art. 132 cod. *privacy* individua senz'altro un prezioso *tertium comparationis* su cui saggiare la proporzionalità delle diverse soluzioni normative dedicate all'impiego del braccialetto elettronico e su cui tarare il possibile reimpiego dei dati acquisiti da tale congegno; tuttavia, e malgrado quelli acquisibili tramite il dispositivo indossabile si ascrivano a una categoria di dati che l'art. 132 cod. *privacy* circonda di particolari garanzie (tra cui la previsione di soglie di gravità relative al reato da accertare), resta impervio rinvenire i margini per un'applicazione analogica dell'art. 132 cod. *privacy* per regolare la circolazione probatoria dei dati resi disponibili dal braccialetto⁴⁴.

di quella ricavabile dall'analisi delle celle telefoniche agganciate dal *device* (la quale peraltro ha una precisione molto variabile, in funzione della densità della rete, e che si abbassa sensibilmente nelle zone rurali rispetto ai centri densamente abitati). V. i risultati dello studio descritti in A. OGULENKO-I. BENENSON-M. TOGER-J. ÖSTH-A. SIRETSKIY, *The fallacy of the closest antenna: Towards an adequate view of device location in the mobile network*, in *arxiv.org*, 5 settembre 2021.

Oltre che più puntuali, le conoscenze acquisibili mediante braccialetto elettronico sono anche meno facilmente ottenibili altrimenti: si consideri infatti che, a partire da dicembre del 2024, la cronologia delle posizioni (*timeline*) legata all'utilizzo di *Google Maps* non viene più archiviata su *cloud*, ma salvata esclusivamente sul dispositivo in uso.

⁴⁴ Si consideri peraltro che la Cassazione ha ritenuto di ravvisare un'importante differenza tra il fenomeno normato dall'art. 132 cod. *privacy* e l'attività di ricerca della prova attuata mediante pedinamento satellitare, in particolare quando ha affermato che, non postulando il pedinamento satellitare un «un accumulo massivo di dati sensibili da parte del gestore del servizio», non debbano neppure trovare applicazione, per analogia, «né la disciplina di cui all'art. 132 comma 3 d.lgs. 30 giugno 2003, n. 196 e successive modifiche, in tema di tabulati, né i principi affermati dalla sentenza della Corte giust., sent. 5 aprile 2022, C. 140/2020, relativa alla compatibilità di “data retention” con le Direttive 2002/58/CE e

Nel delineare una categoria probatoria inedita e di difficile inquadramento, le caratteristiche sin qui evidenziate rendono impossibile invocare anche la disciplina dell'art. 270 c.p.p., concernente l'uso "ulteriore" dei risultati delle intercettazioni. E ciò non solo perché i dati concernenti l'ubicazione e la geolocalizzazione (sia pure considerati con particolare rigore dalla giurisprudenza della Corte di giustizia⁴⁵) non coinvolgono le libertà inviolabili tutelate dall'art. 15 Cost.; ma anche perché, comunque, tali elementi sono stati acquisiti da un dispositivo consapevolmente accolto dalla persona-bersaglio. In questo caso, il dato non è carpito di soppiatto, ma acquisito alla luce del sole; non è il frutto di una sorveglianza occulta, ma di un controllo noto all'individuo⁴⁶. E infatti, come già osservato, il controllo trova la sua ragion d'essere proprio nell'effetto-deterrenza conseguente al possibile impiego probatorio del dato conoscitivo registrato dal *device*.

Mancando una regola specificamente intesa a normare – e a limitare – la circolazione probatoria dei dati acquisiti grazie alla sorveglianza tecnologica (dell'imputato e del condannato, come pure del prevenuto), l'art. 3 del d.lgs. n. 51 del 2018 impone di domandarsi quale possa essere il canale idoneo a veicolare l'acquisizione del dato probatorio nel procedimento penale *ad quem*.

In prima battuta, la somiglianza con i risultati del pedinamento satellitare (notoriamente considerato, dalla giurisprudenza italiana, quale mezzo d'indagine irripetibile e atipico⁴⁷) potrebbe indurre a considerare il ter-

2009/136/CE, sul trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni» (così Cass., Sez. II, 18 settembre 2024, n. 37395, in *C.e.d.*, n. 286949).

⁴⁵ La giurisprudenza della Corte di giustizia (v. in particolare la nota decisione resa dalla Grande Sezione il 4 ottobre 2024, *Bezirkshauptmannschaft Landeck*, C-548/21) impone per i dati concernenti l'ubicazione del dispositivo elettronico in uso al singolo un livello di tutela analogo a quello da assicurare per i dati esterni delle comunicazioni, che consentono di ottenere notizie in ordine agli «spostamenti quotidiani o di altro tipo, le attività svolte, le relazioni sociali e gli ambienti sociali frequentati dall'interessato» (punto 93 della pronuncia). Il livello di protezione richiesto dal Giudice di Lussemburgo si sostanzia nell'obbligo: di definire in modo sufficientemente preciso la natura o le categorie delle infrazioni per cui tale tecnica d'indagine può operare; di garantire il rispetto del principio di proporzionalità; di subordinare la possibile acquisizione dei dati (salvo in casi di urgenza debitamente giustificati) al controllo preventivo di un giudice o di un organo amministrativo indipendente. V. anche Corte giust., sent. 21 dicembre 2016, *Tele2 Sverige c. Autorità svedese di Sorveglianza Poste e TLC*, C-203/15 e C-698/15, sent. 6 ottobre 2020, *La Quadrature du Net*, C-511/18, C-512/18, C-520/18, sent., 2 marzo 2021, *Prokuratuur*, C-746/18).

⁴⁶ Per una attenta riflessione attorno alla particolare intrusività della natura occulta del controllo v. F. NICOLICCHIA, *I controlli continuativi e occulti come categoria probatoria*, Cedam, Padova, 2020 (in particolare alle pp. 76 ss.).

⁴⁷ Solo fra le ultime, v. Cass., Sez. VI, 9 marzo 2023, n. 15422, in *C.e.d.*, n. 284582 (la quale esclude che al pedinamento satellitare mediante GPS debba applicarsi in via analo-

zo comma dell'art. 238 c.p.p.: sebbene i dati sui movimenti del braccialetto non siano il frutto di un'attività di ricerca della prova del reato per cui si procede nel procedimento *a quo*⁴⁸, in tal senso si potrebbe infatti valorizzare la lettera della norma, che menziona genericamente i verbali di atti «irripetibili». Sennonché, pare a chi scrive che tali conoscenze vadano piuttosto inquadrare nella categoria della prova documentale: una prova documentale – riconducibile talvolta all'art. 235 c.p.p.⁴⁹ e immancabilmente all'art. 237 c.p.p. – confezionata in un diverso procedimento penale, e che, formata nella prospettiva di poter essere utilizzata per inasprire il trattamento cautelare o penitenziario in corso di esecuzione, potrà divenire utile anche come prova di fattispecie di reato sia pure sguarnite di qualsiasi collegamento con le ragioni poste a fondamento del monitoraggio elettronico.

Ora, quale dei due canali acquisitivi – atto irripetibile o mera prova documentale – sia privilegiato dall'interprete, all'atto pratico non dovrebbero discenderne sostanziali differenze. Infatti, anche volendo ricondurre i dati acquisiti dal braccialetto elettronico alla categoria dell'atto irripetibile, l'impossibilità di invocare l'art. 270 c.p.p. non permetterebbe di rinvenire particolari limiti all'uso di tali conoscenze, posta l'incondizionata circolazione probatoria ammessa dall'art. 238 comma 3 c.p.p.⁵⁰.

gica la disciplina in materia di *data retention*, come pure non debbano applicarsi i principi affermati dalla sentenza della Corte di giustizia del 5 aprile 2022, *Garda Síochána*, C. 140/2020). Negli stessi termini, v. Sez. II, 18 settembre 2024, n. 37395, *ivi*, n. 286949. V. anche Sez. IV, 21 aprile 2022, n. 21856, *ivi*, n. 283386, che ha altresì escluso la necessità di dare applicazione agli artt. 244 e 247 comma 1-*bis* c.p.p.

⁴⁸ Sicuramente, la sorveglianza elettronica mediante braccialetto o cavigliera è intesa a produrre dati funzionali al controllo del regime coercitivo in corso di esecuzione e non ad acquisire conoscenze utili ad accertare il reato per il quale si procede.

⁴⁹ L'art. 235 c.p.p. vige in tutte le ipotesi in cui il dato acquisito dal braccialetto costituisca la prova della evasione, della manomissione, o comunque di «una o più condotte gravi o reiterate che impediscano od ostacolino il regolare funzionamento dei mezzi elettronici e degli altri strumenti tecnici di controllo di cui all'articolo 275-*bis*».

⁵⁰ Tuttavia, il discorso cambierebbe rispetto alla possibile circolazione probatoria dei dati procacciati dal *tracking* disposto sulla base della disciplina in materia di prevenzione. In proposito, deve innanzitutto escludersi che possa operare l'art. 226 comma 5 disp. att. c.p.p.: infatti, anche volendo ritenere che il divieto d'uso, nel processo penale, delle conoscenze acquisite mediante le attività preventive stabilito da tale disposizione possa intendersi riferito anche ai dati di traffico telefonico e telematico acquisiti a fini di prevenzione *ex* art. 226 comma 4 disp. att. c.p.p., la già segnalata impossibilità di equiparare i risultati probatori della sorveglianza elettronica a quelli ottenuti con l'acquisizione dei dati di traffico telefonico e telematico finisce anche per escludere l'applicazione dell'art. 226 comma 5 disp. att.

Ciò detto, le conseguenze della scelta definitiva – in ordine alla catalogazione dei dati acquisiti dal braccialetto quale prova documentale o atto irripetibile – potrebbero essere rilevanti. Ove si scegliesse di considerare tali dati una prova documentale, opererebbe

Come torneremo a ribadire nella parte conclusiva di questo lavoro, tale constatazione mostra la necessità di soluzioni normative che, oltre a dover essere precise, risultino anche conformi al principio di proporzionalità. Il consenso dell'interessato non può infatti essere concepito quale fattore in grado di travalicare *in toto* la portata garantistica di tale principio, che resta un ineludibile parametro per determinare l'astratto perimetro operativo della sorveglianza tecnologica, i tempi di conservazione dei dati acquisiti e registrati dal braccialetto, come pure i limiti e i canali in ordine all'ipotetica possibilità dell'uso di tali dati in un distinto procedimento penale.

Questi singoli temi sono con ogni probabilità destinati ad assumere un peso crescente, in particolare ove le tendenze ravvisabili al di fuori dei confini nazionali dovessero attecchire anche da noi.

6. *Uno sguardo al futuro*

Secondo quanto sin qui osservato, già *de iure condito* l'ampliato perimetro del possibile ricorso al braccialetto elettronico tracciato dalle più recenti innovazioni legislative è destinato a ripercuotersi sul possibile reimpiego delle conoscenze acquisite mediante lo strumento digitale, aumentandone la concreta incidenza. Sennonché, in futuro, potrebbero presentarsi ulteriori sviluppi. Il panorama estero offre infatti numerose testimonianze, di cui è bene dar conto.

In generale, le ragioni atte a determinare un ricorso più esteso alla sorveglianza elettronica hanno natura sia quantitativa che qualitativa.

Dal punto di vista quantitativo, va innanzitutto ribadito che oggi in Italia i numeri sono ancora piuttosto contenuti: come già ricordato, la disponibilità di braccialetti si assesta per ora attorno ai 1200 dispositivi attivabili al mese⁵¹. Tuttavia, la situazione potrebbe cambiare, in conseguenza non solo del *trend* espansivo già descritto nelle pagine scorse, ma anche osservando la realtà di altri paesi.

Una possibile dilatazione del ricorso all'istituto – da osservare con diffidenza – potrebbe essere indotta dagli scopi e dai (sedicenti) vantaggi

la disciplina generale di cui agli artt. 234, 235 e 237 c.p.p.; al contrario, ove venissero ricondotti alla categoria dell'atto irripetibile, andrebbe sciolta la questione in ordine all'applicabilità dell'art. 238 comma 3 c.p.p. agli atti irripetibili formati in un procedimento non penale (applicabilità esclusa, fra gli altri, da C. CESARI, *L'irripetibilità sopravvenuta degli atti d'indagine*, Giuffrè, Milano, 1999, p. 433 ss., e viceversa ammessa da R. ORLANDI, *Atti e informazioni della autorità amministrativa nel processo penale. Contributo allo studio delle prove extracostruite*, Giuffrè, Milano, 1992, p. 142 ss.).

⁵¹ V. *supra*, nota 10.

del controllo digitale, dichiaratamente idoneo a rispondere a una pluralità di istanze, quali: il contrasto al sovraffollamento carcerario, il contenimento dei costi connessi al ricorso al carcere e, non ultimo, l'abbattimento dei tassi di recidiva e degli effetti criminogeni indotti dalla detenzione, reso astrattamente possibile da uno strumento che, oltre a mantenere intatti i legami familiari ed evitare le conseguenze stigmatizzanti del carcere, scommette sulla capacità di autodisciplina del prevenuto.

Alla prova dei fatti, il raggiungimento di tali scopi non risulta confermato *ex post*. Studi empirici dimostrano piuttosto, oltre a un'incidenza assai scarsa a ridurre i tassi di recidiva, anche la generalizzata propensione ad affiancare la sorveglianza elettronica a misure alternative alla cattività carceraria che sarebbero state applicate comunque (anche senza l'imposizione del braccialetto).

Cionondimeno, e dunque malgrado l'insussistenza di benefici tangibili, la tendenza all'espansione persiste, favorita dal fatto che, oltre a consentire una profilazione utile anche a fini di giustizia predittiva, questa tecnologia diviene ogni giorno più affidabile⁵², e – soprattutto – più economica⁵³, così com'è dimostrato dall'impiego sempre più diffuso di *smartphone* e *wearable* al posto delle tradizionali cavigliere⁵⁴. La strumentalizzazione di tali tipi di *device* non è ancora approdata in Italia, ma potrebbe farlo molto presto, potendo così aprire le porte a una sorveglianza digitale

⁵² A tale specifico riguardo, si consideri che negli Stati Uniti e in Canada sono già operativi sistemi basati sull'intelligenza artificiale in grado di generare allarmi prima che il soggetto con braccialetto elettronico entri in una zona preclusa o si avvicini troppo alla vittima del reato.

⁵³ V. già, fra gli altri, C. CESARI, *Editoriale: L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, vol. 4, n. 3, 2019, p. 1172. Nello stesso senso, presentando i risultati di una ricerca conclusasi nel 2016, che ha messo a confronto l'impiego del braccialetto elettronico in cinque diversi paesi europei (Belgio, Olanda, Germania, Inghilterra e Galles, Scozia), v. A. HUCKLESBY-K. BEYENS-MIRANDA BOONE-F. DÜNKEL- G. McIVOR-H GRAHAM, *op. cit.*, p. 5.

⁵⁴ Negli Stati Uniti, gli *smartphone* vengono già usati massivamente alla stregua di braccialetti elettronici, in particolare a fronte di soggetti a basso rischio (data la loro minor precisione ed affidabilità, nonché, soprattutto, la facilità con cui il controllo può essere eluso). V. in proposito AMERICAN PROBATION AND PAROLE ASSOCIATION, *Leveraging the power of spartphone applications to enhance community supervision*, 7 aprile 2020. Per una critica a tale pratica v. K. OWENS-A. ALEM.F. ROESNER-T. KOHNO, *Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives*, in *usenix.org*, ottobre 2022, che prende in esame sedici *app* per *smartphone* comunemente usate negli Stati Uniti per il monitoraggio elettronico di persone in *probation*, *parole* o in attesa di giudizio, segnalando come queste raccolgano grandi quantità di dati sensibili (tra cui anche verifiche biometriche), presentino vulnerabilità tecniche e si caratterizzino per una gestione dei dati poco trasparente. Come vedremo nel § 8, negli USA l'uso di applicazioni per *smartphone* è particolarmente *in auge* per il monitoraggio degli stranieri irregolari e dei richiedenti asilo.

numericamente molto più diffusa (oltre che, come vedremo, per certi aspetti anche più invasiva).

In ipotesi, la sorveglianza potrebbe anche oltrepassare le colonne d'Ercole del procedimento e dell'esecuzione penale. Si pensi infatti che, per esempio in Germania, il monitoraggio elettronico mediante GPS può essere applicato a soggetti ritenuti altamente pericolosi anche una volta esaurita l'espiazione della pena⁵⁵.

Oltre che da quello quantitativo, il futuro dischiude nuovi possibili scenari anche dal punto di vista qualitativo. All'estero si possono infatti riscontrare tanto l'impiego a fini penali del braccialetto elettronico volto a procurare dati diversi dalla geolocalizzazione, quanto il ricorso al *device* indossabile per acquisire dati concernenti la geolocalizzazione, ma per scopi diversi da quelli tradizionalmente ascrivibili al sistema penale. Ne daremo conto nei prossimi due paragrafi, onde capire se si tratta di utilizzi ipoteticamente importabili anche nel nostro sistema.

7. Segue: *il controllo a distanza del consumo di alcol*

Innanzitutto, il braccialetto elettronico potrebbe prestarsi ad essere sfruttato per verificare l'eventuale assunzione di alcol, nonché – ma in una prospettiva doppiamente ipotetica – di stupefacenti. Non contemplato nel nostro sistema, il monitoraggio a distanza del consumo di alcolici già opera in altri stati, fra cui gli Usa, e, da qualche anno, la Gran Bretagna. Viceversa, un'analoga tecnica non risulta essere stata ancora messa a punto anche per appurare l'uso di droghe (semmai soggetto a forme di controllo diverse, che passano per l'apposizione di cerotti, denominati *drug sweat patches*⁵⁶)⁵⁷.

⁵⁵ V. § 68b StGB.

⁵⁶ Si tratta di cerotti adesivi da indossare per 7-10 giorni e che assorbono il sudore, e consentono di monitorare l'assunzione di droghe, ancorché non in modo istantaneo. V. la guida *How The Sweat Patch Works*, in *pharmcheck.com*, esplicativa del funzionamento dei cerotti attualmente in uso nel sistema giudiziario statunitense.

⁵⁷ Le ricerche scientifiche evidenziano limiti non ancora superati: la farmacocinetica delle sostanze stupefacenti non consente ancora un monitoraggio transdermico continuo e affidabile come quello già in uso rispetto all'assunzione di alcol. Sebbene i ricercatori riescano a rilevare droghe nel sudore, ciò è possibile solo in condizioni controllate (in laboratorio), a causa della minor sensibilità del sudore all'assunzione di droghe piuttosto che di alcool e dell'elevato rischio di contaminazione esterna. Per tale ragione, nessuna società ha prodotto un *device* forense equivalente a quello in uso per monitorare in modo continuo il consumo di alcol. V. A. M. VINU MOHAN-V. RAJENDRAN-R.K. MISHRA-M. JAYARAMAN, *Recent advances and perspectives in sweat based wearable electrochemical sensors*, in *sciencedirect.com*, ottobre 2020.

In particolare, l'esperienza statunitense vede già da anni operare l'*Alcohol Monitoring Systems* (AMS), che permette e regola il monitoraggio remoto continuo dell'alcol. Tale tecnologia è impiegata in contesti tanto extragiudiziari (in supporto alla cura) quanto giudiziari, ad esempio nei confronti di persone condannate per guida in stato di ebbrezza, o quale misura cautelare (soprattutto in casi di violenza domestica rispetto ai quali è risultata rilevante la dipendenza da alcol).

Lanciato sul mercato nel 2003, il sistema *SCRAM* (acronimo di *Secure Continuous Remote Alcohol Monitoring*) è stato impiegato in ambito giudiziario quasi immediatamente, e, a seguire, ha cominciato ad essere normato dalla legislazione di un numero crescente di stati (sia pure mai a livello federale). Oggi esso opera in tutti e cinquanta gli Stati USA, e funziona grazie all'apposizione di una cavigliera elettronica che misura l'alcol transdermico (*TAC*)⁵⁸.

Già da tempo diffusa oltreoceano, tale forma di monitoraggio ha attecchito anche nel Vecchio continente, in particolare in Gran Bretagna, nell'ambito del programma *Alcohol Abstinence and Monitoring Requirement* (*AAMR*), che consente all'autorità giudiziaria di imporre un periodo di astinenza come parte di una *community order* o *suspended sentence order*, nonché di associare a tale imposizione strumenti di monitoraggio elettronico⁵⁹.

Sebbene, ad oggi, la sorveglianza da remoto del consumo di alcolici sia sconosciuta al nostro sistema, non è da escludere che essa possa, prima o poi, arrivare anche in Italia. Benché, a quanto consta, la relazione tra abuso di alcol e crimine non sia oggetto di specifici studi statistici nel nostro Paese (studi che viceversa si concentrano sulle dipendenze in generale e più che altro su quella da sostanze stupefacenti), è indubbio che esso comporta un aumento del rischio per l'individuo di essere sia il perpe-tratore sia la vittima di un crimine violento⁶⁰.

In Italia, l'amministrazione penitenziaria si fa carico delle dipendenze – complessivamente considerate – mediante percorsi terapeutici che, se

⁵⁸ Un'esaustiva panoramica sulle diverse tecnologie rese disponibili dall'azienda si può ricavare consultando il sito *scramsystems.com*, che descrive anche la storia del monitoraggio transdermico.

⁵⁹ V. part 12, n. 9 del *Sentencing Act* 2020 e la sezione 212A del *Criminal Justice Act* 2003 nella sua formulazione oggi vigente. Sulla scorta di tale base normativa, dopo alcuni progetti pilota già inaugurati negli anni precedenti, l'uso del braccialetto elettronico mediante *SCRAM* è stato dapprima adottato nel Galles (a partire dall'ottobre 2020) e, dal 31 marzo 2021, anche in Inghilterra. V. il *report* del settembre 2025: gov.uk/government/statistics/electronic-monitoring-statistics-publication-september-2025.

⁶⁰ A. DEEHAN, *Alcohol and crime: taking stock*, London, Home Office, 1999.

svolti in carcere, scontano numerose limitazioni; tanto che, onde consentire la prosecuzione o l'inizio dell'attività terapeutica fuori dagli istituti di pena, la legge prevede l'affidamento in prova nei casi particolari di tossicodipendenza o alcol-dipendenza (art. 94 d.P.R. 309 del 1990).

Sebbene non sia normativamente previsto, dunque, anche nel nostro ordinamento sussistono le astratte condizioni per ricorrere all'ausilio del braccialetto in grado di monitorare il consumo di alcol durante l'affidamento in prova a fini terapeutici. Tuttavia, è chiaro come la futuribile importazione di simili tecnologie anche in Italia possa ripercuotersi sul governo del controllo dei comportamenti di chi sia stato ammesso a tale misura alternativa. Stando all'art. 94 del D.P.R. 9 ottobre 1990, n. 309 infatti, la sorveglianza sul rispetto delle prescrizioni di tipo sanitario è rimessa al responsabile della comunità di recupero, che è destinatario di un preciso obbligo di segnalazione all'autorità giudiziaria, stabilito dal comma 6-ter del medesimo testo unico⁶¹. Notoriamente, tale obbligo di segnalazione – la cui «rigidità non si accorda con l'orientamento terapeutico e riabilitativo dell'istituto» – è vissuto con insofferenza dai servizi per le dipendenze, non sempre propensi a segnalare agli uffici di esecuzione penale esterna l'inosservanza delle prescrizioni da parte dell'affidato in prova, onde scongiurare una richiesta di revoca del beneficio ai magistrati di sorveglianza⁶².

A fronte di ciò, se mai dovessero arrivare anche in Italia strumenti di sorveglianza elettronica a fini penali sul consumo di alcol, e la relativa supervisione dovesse essere affidata a personale diverso da quello medico, l'assetto complessivo potrebbe virare verso un approccio più sanzionatorio che terapeutico: determinando, quindi, la prevalenza della “cultura giuridica” su quella “socio-sanitaria”.

In astratto, anche rispetto agli esiti di questo tipo di monitoraggio si potrebbero ipotizzare usi probatori ulteriori rispetto a quelli concernenti l'eventuale revoca dell'affidamento *ex* art. 94 d. P.R. n. 309 del 1990. Il pensiero corre, istintivamente, alla prova della guida in stato di ebbrezza. Sennonché, sul punto è necessario un chiarimento. Infatti, e sebbene la

⁶¹ Così recita la disposizione citata nel testo: «[i]l responsabile della struttura presso cui si svolge il programma terapeutico di recupero e socio-riabilitativo è tenuto a segnalare all'autorità giudiziaria le violazioni commesse dalla persona sottoposta al programma. Qualora tali violazioni integrino un reato, in caso di omissione, l'autorità giudiziaria ne dà comunicazione alle autorità competenti per la sospensione o revoca dell'autorizzazione di cui all'articolo 116 e dell'accreditamento di cui all'articolo 117, ferma restando l'adozione di misure idonee a tutelare i soggetti in trattamento presso la struttura».

⁶² V. in proposito D. BERTACCINI, *Fondamenti di critica della pena e del penitenziario. Rielaborazione aggiornata dell'opera didattica di Massimo Pavarini*, II ed., Bologna, 2021, p. 254 ss.

giurisprudenza statunitense abbia riconosciuto l'affidabilità dell'accertamento (avendo sin dal 2009 acclarato la solidità scientifica di questa tecnologia alla luce dei criteri *Daubert*⁶³), bisogna tener presente come la funzione dello *SCRAM* sia quella di verificare se un individuo ha assunto alcol durante il periodo di monitoraggio, e non anche quella di dimostrare se egli sia troppo alterato per mettersi alla guida in un momento specifico. Proprio per questo, negli USA i dati *SCRAM* vengono considerati utili per una varietà di scopi – ai fini della revoca della *probation* o della *parole*, come pure della libertà su cauzione⁶⁴ – ma non possono costituire una prova idonea a dimostrare la guida in stato d'ebbrezza⁶⁵. Tale aspetto è rilevante, e, in ipotesi, andrebbe tenuto presente nella prospettiva, allo stato non immediata, in cui tale specifica declinazione del monitoraggio mediante *wearable* dovesse arrivare anche nel nostro Paese.

8. Segue: *monitoraggio elettronico e controllo dei migranti*

L'esperienza estera si fa testimone pure di un ulteriore e diverso impiego del braccialetto elettronico, che, applicato per vigilare la posizione della persona-bersaglio (e dunque sempre a fini di localizzazione), agisce tuttavia per uno scopo ancora non contemplato dalla legge italiana, ossia quello di seguire i movimenti degli stranieri irregolari e dei richiedenti asilo, evitando che si rendano irreperibili nella prospettiva di poterli poi effettivamente rimpatriare. Questa “nuova frontiera” della sorveglianza elettronica è tutto fuorché immaginaria, se è vero che, stando a notizie giornalistiche del febbraio 2025, il Governo Meloni avrebbe mostrato di prenderla in considerazione⁶⁶, sul modello di quanto (ancora una volta) già avviene negli Stati Uniti e in Gran Bretagna.

Sebbene sia per ora rimasto isolato, l'annuncio apparso sulla stampa potrebbe tradursi in qualcosa di più concreto, specie considerando i contenuti del Patto europeo su migrazione ed asilo, composto da una copiosa serie di fonti (in prevalenza regolamenti) a breve destinati a diventare con-

⁶³ Particolarmente importante, in tale evoluzione, la pronuncia resa dalla Corte suprema del Dakota del Sud il 16 settembre 2009 nel caso *State v. Lemler*, 774 N.W.2d 272 (S.D. 2009). V. law.justia.com/cases/south-dakota/supreme-court/2009/24815.html.

⁶⁴ E ciò anche in forza del fatto che per assumere tali decisioni, lo *standard* probatorio non è quello del *BARD*, bensì quello della *preponderance of the evidence* (v. *Bail Reform Act*, del 1984, 18 USC Sec. 3148 (b); in giurisprudenza, v. *U.S. v. Gotti*, 794 F.2d 773 (2nd Cir. 1986).

⁶⁵ V. ancora Corte suprema del Dakota del Sud, *State v. Lemler*, cit.

⁶⁶ V. fra gli altri F. MANTI, *Braccialetti elettronici ai migranti. Il Viminale ne ha già presi 100mila*, in ilgiornale.it, 11 febbraio 2025.

cretamente operativi⁶⁷. Onde smaltire le richieste di protezione internazionale e rendere effettivi i rimpatri degli stranieri irregolari, il Patto vincola infatti i singoli Stati membri dell'Unione ad assicurare una «capacità adeguata» di gestire le nuove procedure accelerate di frontiera preposte a esaminare domande di asilo e a eseguire gli allontanamenti dal territorio italiano ed europeo. Per quanto espresso con una formula – quella della «capacità adeguata» – piuttosto sibillina, tale impegno, destinato a farsi progressivamente più oneroso di anno in anno, comporterà per forza di cose il rafforzamento degli strumenti di coercizione e di controllo fisico dei migranti. Oltre ad essere scandite da termini assai celeri, le procedure di frontiera si associano infatti ad un ricorso generalizzato a forme di limitazione della libertà personale o della libertà di circolazione: il che rende assai probabile il futuro ricorso anche alla “gabbia tecnologica”, meno costosa della detenzione amministrativa⁶⁸.

⁶⁷ Secondo la definizione rinvenibile sul sito del *Department for Migration and Home Affairs*, il «Patto sulla migrazione e l'asilo è un insieme di nuove norme per la gestione della migrazione e che istituiscono un sistema Comune di asilo a livello dell'unione europea, orientato ai risultati ma ben ancorato ai nostri valori europei» (v. home-affairs.ec.europa.eu). Il pacchetto si compone di dieci diverse fonti normative, tutte pubblicate nella Gazzetta ufficiale dell'Unione europea del 22 maggio 2024.

⁶⁸ Alla procedura di asilo alla frontiera, normata dal regolamento (UE) 2024/1348, è associata la nozione di «capacità adeguata» (di cui agli artt. 46 e 47 di tale regolamento), ossia la capacità amministrativa e operativa, richiesta al singolo stato membro, di gestire le procedure di frontiera (esaminare domande, effettuare *screening*, garantire risorse, personale, strutture idonee allo scopo). L'obbligo di garantire la concreta operatività di questa nuova procedura di frontiera vige anche, coerentemente, in relazione alla procedura di rimpatrio alla frontiera, di cui al regolamento (UE) 2024/1349.

In particolare, secondo l'art. 47 del Regolamento (UE) 2024/1348 del 14 maggio 2024, sulla base della «capacità adeguata», assegnata a ogni stato, la Commissione calcola il «numero massimo di domande [di protezione internazionale] che lo Stato membro è tenuto a esaminare con procedura di frontiera ogni anno». Tale limite è pari alla «capacità adeguata» moltiplicata per due, nel primo anno di applicazione della riforma, per tre, nel secondo, e per quattro, nel quarto. Stando all'allegato I alla Decisione di esecuzione (UE) 2024/2150 della Commissione europea del 5 agosto 2024 (in GUUE L, 2024/2150, del 9 agosto 2024), per l'Italia, la «capacità adeguata» è pari a 8.016 unità. Si tratta della quota in assoluto più elevata tra quelle previste per i singoli stati, che corrisponde a oltre un quarto della capacità complessiva a livello di UE. Nel biennio successivo all'applicazione della riforma, il numero massimo di domande di protezione che l'Italia dovrà esaminare con procedura di frontiera sarà pari a 16.032 (per il periodo 12 giugno 2026-12 giugno 2027) e a 24.048 (nell'anno di riferimento successivo).

Il concetto di «capacità adeguata» è ambiguo e sfuggente, e probabilmente indotto dalla volontà politica di patrocinare forme di confinamento ibride, non necessariamente corrispondenti a restrizioni o privazioni della libertà personale, e dunque tali da consentire ai singoli stati di optare per soluzioni non sempre onerose come la detenzione amministrativa, che postula la disponibilità di centri chiusi per i migranti e il rispetto delle garanzie dell'*habeas corpus*.

Come anticipato, altrove questo scenario è già realtà.

In USA, il monitoraggio a distanza – gestito da *BI Inc.*, riconducibile a *GEO Group*, ente privato a scopo di lucro (e che ha iniziato la sua attività nel 1978 producendo un dispositivo di tracciamento per bovini)⁶⁹ – opera addirittura su vasta scala, e, con l'avvento della seconda amministrazione Trump, si sta sviluppando nella prospettiva di attingere numeri sempre più imponenti di persone coinvolte nel programma *Expedited Removal* (ER)⁷⁰. Secondo quanto riportato dai media nell'estate del 2025, l'*Immigration and Customs Enforcement* (ICE) punterebbe infatti ad applicare cavigliere elettroniche in modo massiccio, onde monitorare centinaia di migliaia di immigrati⁷¹, andando a sostituire tale forma di sorveglianza a quella, precedentemente in uso, realizzata mediante metodi di controllo diversi, quali il riconoscimento facciale mediante *smartphone* per verificare l'identità e la posizione della persona⁷².

In Australia, il fenomeno si è posto al centro di un braccio di ferro tra il governo federale e la Corte suprema, che, pur non mettendo frontalmente in discussione la legittimità della sorveglianza elettronica a fini di controllo delle migrazioni, ha ritenuto incostituzionale la normativa, introdotta il 16 novembre del 2023, che aveva assegnato al Ministero dell'immigrazione il potere di imporre tale forma di controllo a stranieri la-

⁶⁹ Sugli interessi economici generati dall'investimento politico sulla sorveglianza elettronica a carico dei migranti v. fra gli altri M. SHUHAM, *Private Prison Companies Call Trump's Deportation Plans 'Unprecedented Opportunity'*, in *buffpost.com*, 7 novembre 2024.

⁷⁰ L'Istituto del *Expedited Removal* (rimozione accelerata, ER) è una procedura accelerata di espulsione introdotta negli Stati Uniti nel 1996 con l'*Illegal Immigration Reform and Immigrant Responsibility*, e che, nel corso degli anni, ha visto il proprio raggio applicativo progressivamente rafforzato. A partire dal 2023, tale procedura è stata affiancata dal programma – attivato dalla divisione *Enforcement and Removal Operations* (E.R.O.) dell'*Immigration and Customs Enforcement* (ICE) – denominato *Family Expedited Removal Management*. Il FERM mira a creare un'alternativa alla detenzione amministrativa (*Alternatives to detention: ATD*) destinata ad operare durante l'esame della richiesta di asilo da parte del U.S. Citizenship and Immigration Services e del successivo (eventuale) riesame giudiziario contro il relativo rigetto. Per dettagli sul programma, si può consultare il sito *ice.gov*.

⁷¹ Un articolo del *Washington Post* (pubblicato il 24 luglio 2025 e intitolato *ICE moves to shackle some 180,000 immigrants with GPS ankle monitors*) dà notizia di una nota interna dell'ICE del 9 giugno 2025, con cui l'*Immigration and Customs Enforcement* avrebbe ordinato al personale di applicare – «ove possibile» – cavigliere elettroniche a tutti gli iscritti al programma *Alternatives to Detention* (ATD) dell'agenzia, nella logica di sostituire metodi di monitoraggio fisicamente meno invasivi come l'obbligo di svolgere *check in* virtuali tramite un'app per *smartphone*.

⁷² Il sito dell'ICE riporta dettagliatamente i diversi sistemi di sorveglianza cui gli stranieri possono essere sottoposti nell'ambito del programma *Alternatives to Detention* (ATD), ascrivibili alle alternative della *telephonic reporting*, del *body-worn GPS* e dell'utilizzo della applicazione mobile *SmartLINK*. V. *ice.gov/features/atd*.

sciati a piede libero una volta spirati i termini della detenzione amministrativa (misura di cui la medesima *High Court* aveva nel 2023 riscontrato l'illegittimità per via della mancata previsione di termini di durata massima⁷³)⁷⁴.

L'impiego del braccialetto per controllare i migranti ha già fatto capolino anche in Europa, sia pure fuori dai confini dell'UE. In Inghilterra e nel Galles, la sperimentazione è passata per un progetto sviluppatosi dal dicembre del 2022 al giugno del 2023⁷⁵, forte di due diverse tecnologie: quella che vede entrare in funzione *scanner* per impronte digitali abilitati al GPS (dispositivi non montati)⁷⁶, e quella che opera mediante l'apposizione di una cavigliera (dispositivi montati). Tuttavia, il progetto non ha poi avuto seguito, e non solo perché gli elementi raccolti non hanno dimostrato alcun ridimensionamento del *risk of absconding* in capo alle persone sottoposte a monitoraggio elettronico⁷⁷; determinanti in tal senso sono state infatti due decisioni, rese rispettivamente dall'*Information Commissioner's Office* (omologo del nostro Garante nazionale per la *privacy*) e dalla *High Court* di Londra. La prima ha visto l'ICO riscontrare l'illegittimità dell'esperimento, non avendo l'*Home Office* adeguatamente giustificato la necessità del monitoraggio continuo, valutato l'impatto sui dati personali e definito limiti alla conservazione dei dati raccolti⁷⁸. La seconda decisio-

⁷³ V. la storica sentenza *High Court of Australia*, 8 novembre 2023, *NZYQ v. Minister for Immigration, Citizenship and Multicultural Affairs* [2023] HCA 37, in bcourt.gov.au/sites/default/files/eresources/2023/HCA/37.pdf

⁷⁴ *High Court of Australia*, 6 novembre 2024, *YBFZ v. Minister for Immigration, Citizenship and Multicultural Affairs* [2024] HCA 40. Partendo dalla constatazione che il monitoraggio elettronico e il "coprifuoco" sono misure coercitive e altamente restrittive, il cuore della decisione sta nell'affermazione secondo cui il parlamento e il governo non possono accordare all'esecutivo poteri di natura punitiva analoghi a quelli accordati alla giurisdizione penale. V. bcourt.gov.au/sites/default/files/eresources/2024/HCA/40.pdf.

⁷⁵ Si è trattato del *GPS Expansion Pilot*, la cui base legale era rinvenibile nella *Schedule 10 (Immigration Bail)* dell'*Immigration Act 2016*.

⁷⁶ Gli scanner GPS inviano un segnale alle persone fino a cinque volte al giorno a orari casuali, con l'invito a scansionare le proprie impronte digitali onde verificare che stiano effettivamente indossando il localizzatore. In questo caso, all'obbligo di indossare si sostituisce l'obbligo di recare con sé un dispositivo cui si collega la lettura di un dato biometrico: lo scopo è simile ma il livello di controllo è meno continuativo. Trattandosi di un dispositivo non montato, lo straniero potrebbe più facilmente far perdere le proprie tracce disfacendosi del *device*; tuttavia, quantomeno per i richiedenti asilo, l'impatto di un simile comportamento sugli esiti della propria domanda di protezione internazionale costituisce un significativo deterrente, idoneo a scongiurare condotte non collaborative.

⁷⁷ HOME OFFICE, *GPS expansion pilot evaluation*, in gov.uk, 13 gennaio 2025.

⁷⁸ V. i documenti, del 28 febbraio 2024, pubblicati in ico.org.uk, 1° marzo 2024, alla notizia *ICO finds the Home Office's pilot of GPS electronic monitoring of migrants breached UK data protection law*.

ne, di natura giurisdizionale, ha invece visto scendere in campo la *High Court*, che nei casi sottoposti al suo vaglio ha ravvisato nell'imposizione del *GPS-tag* su alcuni migranti una misura sproporzionata e illegittima, poiché in contrasto con l'art. 8 della Conv. e.d.u.⁷⁹.

Malgrado la (almeno momentanea) battuta d'arresto britannica, altri paesi vicini al nostro sembrano guardare con attenzione alle potenzialità offerte dalla sorveglianza elettronica a fini di controllo delle migrazioni. È ad esempio il caso della Grecia, il cui governo, nell'agosto del 2025, ha annunciato di voler ricorrere a tale tecnologia nei confronti dei richiedenti asilo che abbiano visto rigettata la propria istanza, per la durata di trenta giorni e nelle more della decisione giudiziaria sull'impugnazione del diniego disposto in prima battuta⁸⁰.

In generale, l'esperienza estera ha messo in risalto elementi critici che suggeriscono estrema cautela in prospettiva *de iure condendo*. Alle perplessità riguardanti il monitoraggio elettronico in sé e per sé considerato, si sommano infatti preoccupazioni specificamente riferite all'utilizzo di braccialetti o cavigliere nei confronti degli stranieri, stigmatizzati per il fatto stesso di indossare un dispositivo istintivamente associato alla sorveglianza penale (e dunque a persone percepite dalla collettività come delinquenti proprio perché portatrici del dispositivo)⁸¹.

Le soluzioni adottate in altri sistemi dimostrano poi che l'impiego di braccialetti o cavigliere volte a prevenire l'irreperibilità degli stranieri (e i loro "movimenti secondari" verso altri paesi) tende ad essere affiancato da tecnologie diverse, in grado di servirsi degli *smartphone*. All'apparenza sconfessato dall'esperienza riscontrabile sotto l'attuale amministrazione Trump, propensione a privilegiare comunque i dispositivi indossabili, tale *trend* non è innocuo. Da un lato, infatti, l'uso di queste nuove tecniche di controllo in genere non soppianta il ricorso al braccialetto, andando semplicemente a sommarvisi, così estendendo lo sguardo dell'autorità a una platea più popolosa di persone. Dall'altro lato, la "strumentalizzazione" degli *smartphone* a fini di sorveglianza non è comunque più rassicurante in termini di proporzionalità: infatti, queste applicazioni per *device* portabili (e non da indossare) si presta a trarre una serie di dati e conoscenze

⁷⁹ *High Court of Justice, ADL & Ors v. Secretary of State for the Home Department*, EWHC 994 (Admin), 15 maggio 2024, che si può leggere in caselaw.nationalarchives.gov.uk.

⁸⁰ V. *Migrants on deportation list to wear ankle monitors, Greek government says* in ekathimerini.com, 11 agosto 2025.

⁸¹ Questo tipo di critica, rinvenibile ad esempio in PRIVACY INTERNATIONAL, *Privacy International files complaints against GPS tagging of migrants in the UK*, in privacyinternational.org, 17 agosto 2022, replica quelle tipicamente mosse al trattenimento, tacciato di costituire una pena senza reato.

più ricca di quelli ottenibili con il braccialetto: posizione continua, *selfie* biometrici, controlli vocali, metadati telefonici, reti *Wi-Fi*, *logs* di attività del *device*⁸².

A fronte di tale possibilità, proviamo ora a ragionare in una prospettiva interna, *de iure condendo*.

Se davvero un simile impiego della sorveglianza elettronica dovesse approdare anche in Italia, la *ratio* sarebbe presumibilmente la stessa già dichiarata nei sistemi che già hanno sposato tale soluzione, ossia quella di propiziare l'applicazione di una misura meno severa (e più economica) rispetto alla detenzione amministrativa.

Proprio per questo, nel tentativo di ragionare sul possibile impatto sistematico di una simile innovazione, vanno considerati i criteri che, quantomeno oggi, orientano l'applicazione del trattenimento nei centri di preparazione al rimpatrio. Stando alla disciplina positiva, tale restrizione della libertà personale dovrebbe attingere un numero molto consistente di stranieri (sia irregolari sia richiedenti asilo); in concreto, però, nei C.P.R. finisce una porzione ancora piuttosto contenuta di coloro che, stando alla *law in the books*, ne dovrebbero costituire i potenziali ospiti. La scarsità dei posti disponibili nei centri chiusi ha addirittura indotto il legislatore del 2020 a mettere nero su bianco alcuni criteri di priorità volti a regolare la scelta degli individui da destinare a tali luoghi. Stabiliti dall'art. 14 comma 1.1. d.lgs. 25 luglio 1998, n. 286 in relazione ai destinatari di provvedimenti espulsivi, tali parametri sono richiamati anche dalle regole valevoli per il trattenimento dei richiedenti asilo⁸³, e impongono di avviare con precedenza ai centri detentivi non solo le persone da rimpatriare in paesi con i quali vigono accordi di "riammissione", ma anche coloro che costituiscano una minaccia per l'ordine o la sicurezza pubblica, come pure chi sia già stato condannato, anche in via non definitiva, per un reato ostativo al rilascio del visto d'ingresso e del permesso di soggiorno.

Ora, se davvero il legislatore italiano dovesse decidere di puntare sulla sorveglianza elettronica per vigilare sui movimenti degli stranieri irregolari e dei richiedenti asilo, è facile presagire che la cernita delle persone da sottoporre al monitoraggio potrebbe improntarsi a una logica simile a quella esplicitata dall'art. 14 comma 1.1 del Testo unico in materia di im-

⁸² V. OWENS-F. ROESNER-T. KOHNO, *Electronic Monitoring Smartphone Apps*, Usenix Security, cit., e K. OAKLEY, *The limit does not exist: how smartphone technology expands electronic and proposed limitation*, in *Harvard Journal of Law & Technology*, v. 36, n. 1, Fall 2022, p. 263 ss.

⁸³ V. in proposito il rinvio operato dal comma 1 dell'art. 6-*bis* d.lgs. 18 agosto 2015, n. 142.

migrazione. Se così fosse, il ricorso al braccialetto elettronico consentirebbe un monitoraggio potenzialmente costante dei movimenti dei migranti considerati pericolosi (oltretutto etichettati come tali sulla scorta di valutazioni operate dall'autorità di polizia e non necessariamente condivise da un giudice): il che, nei fatti, avvicinerebbe questa futuribile forma di sorveglianza a un'atipica misura di prevenzione, esattamente come già avviene per il trattenimento.

Malgrado lo scopo di un ipotetico ricorso al braccialetto elettronico sia quello di rendere possibile l'esecuzione del rimpatrio evitando l'irreperibilità del non cittadino, è chiaro come i dati resi disponibili dal dispositivo possano prestarsi ad offrire elementi utili anche ad altri fini: ad esempio nell'ambito della procedura innescata con la richiesta di asilo; e, evidentemente, anche in seno a un processo penale (in particolare, ma non solo, onde dimostrare la commissione di reati propri dello straniero irregolare⁸⁴).

In questo caso, ci si troverebbe davanti a dati probatori identici a quelli acquisiti mediante i braccialetti già in uso in Italia, ma raccolti in un procedimento amministrativo e per scopi estranei al sistema penale. Lungi dal riguardare la sola geolocalizzazione continua tramite cavigliera, la questione si porrebbe in termini simili anche là dove il legislatore dovesse optare per strumenti diversi (come l'obbligo di recare con sé un dispositivo cui si collega la lettura di un dato biometrico) che potrebbero rivelarsi parimenti forieri di conoscenze spendibili nel processo penale.

In tale prospettiva, i compilatori dovrebbero prevedere dei rigidi paletti alla circolazione probatoria, onde evitare di replicare la lacuna già rilevata a proposito degli usi ulteriori dei risultati della sorveglianza elettronica per come disciplinata dal legislatore italiano, e cercando di esprimersi in termini più chiari rispetto a quelli adoperati a proposito dell'ispezione

⁸⁴ Negli USA, la questione è già riscontrabile in concreto. Nel *Privacy Impact Assessment DHS/ICE sull'Alternatives to Detention (ATD) Program*, programma statunitense che include l'applicazione di *ankle monitor* o *app* per *smartphone*, (alla pagina 6) ICE esplicita che, se il partecipante viola volontariamente gli obblighi di rilascio o non ottempera alla partenza, ERO (*Enforcement and Removal Operations*, ossia la divisione di ICE incaricata dell'esecuzione amministrativa delle misure di rimpatrio e della supervisione degli stranieri sottoposti a programmi di monitoraggio non detentivo) può deferire i casi al *Department of Justice* per il perseguimento delle condotte di *failure to depart* e *willfull failure to comply*. Ciò dimostra che dati originati dal monitoraggio applicato in sede amministrativa – come geolocalizzazione e mancati *check-in* – possono costituire l'*input* per il procedimento penale. Sebbene non consti che questa specifica questione sia stata affrontata a livello giurisprudenziale, è da ritenere che, per poter essere impiegati come prova nel processo penale, vada emesso un *warrant*. In proposito, v. anche *infra*, nota 99.

degli *smartphone* in uso a trattenuti e richiedenti asilo: ispezione resa possibile da una problematica novella del dicembre 2024⁸⁵.

Ove dovesse mancare un'espressa e perentoria previsione di inutilizzabilità nel processo penale (la quale peraltro non riuscirebbe comunque a evitare che le conoscenze apprese tramite tale forma di sorveglianza possano fungere da spunto per avviare delle indagini, preventive o anche penali), è facile attendersi che il diritto vivente possa incasellare i dati acquisiti dal braccialetto nella nozione di documento *ex art.* 234 c.p.p., così come avviene rispetto alle conoscenze apprese da organi amministrativi o di vigilanza prima che insorgano gli estremi per l'applicazione della disciplina processualpenalistica (prescritta dall'*art.* 220 disp. att. c.p.p.)⁸⁶. Sen-

⁸⁵ L'*art.* 12 d.l. 11 ottobre 2024, n. 145, convertito con l. 9 dicembre 2024, n. 187, ha visto l'interpolazione del primo comma dell'*art.* 11 d.lgs. 28 gennaio 2008, n. 25 e l'inserimento dei commi 2-*bis* e 2-*ter* nell'*art.* 10-*ter* d.lgs. n. 286 del 1998. Tale disciplina impone, sia per il richiedente asilo che per lo straniero irregolare, un «obbligo di cooperare ai fini dell'accertamento dell'identità e di esibire o produrre gli elementi in suo possesso relativi all'età, all'identità e alla cittadinanza, nonché ai Paesi in cui ha soggiornato o è transitato [...]»; nel caso di inosservanza di tale obbligo di cooperazione, il questore può disporre l'ispezione dei *device* in uso allo straniero, «al solo fine di acquisire [tal]i elementi». È in ogni caso vietato l'accesso alla corrispondenza e a qualunque altra forma di comunicazione. Lo scopo è quello di ricostruire, oltre appunto all'età, anche il percorso migratorio dello straniero, e dunque di ricavare, dall'analisi dello *smartphone*, conoscenze in grado di suffragare o di smentire quanto da lui dichiarato in ordine alla propria provenienza. Sebbene essa sia tale da incidere sulla libertà e segretezza delle comunicazioni, la disciplina non rispetta l'*art.* 15 Cost. (e forse per questo ancora non risulta che sia stata formalmente applicata): l'istituto assegna infatti il potere di disporre e attuare l'ispezione dei *device* direttamente all'autorità di polizia, salva la necessità di una successiva convalida da parte del giudice di pace, replicando uno schema – quello di cui all'*art.* 13 comma 3 Cost. – del quale tuttavia l'*art.* 15 Cost. non reca traccia. Tra le tante criticità di questa disciplina (sulle quali ci si è soffermati in E. VALENTINI, *L'ispezione per finalità identificative dello smartphone in uso allo straniero, tra "persuasione" e coazione senza garanzie*, in *dirittimmigrazione cittadinanza.it*, 2025, f. 1), si deve segnalare quella indicata nel testo: il comma 2-*ter* dell'*art.* 10-*ter* T.U.I. si limita a stabilire l'inutilizzabilità e il conseguente obbligo di cancellazione dei soli dati di cui il giudice, in sede di mancata convalida (o convalida parziale), abbia riscontrato l'illegittimo controllo. Ma nulla dice rispetto all'ipotetica circolazione probatoria dei dati legittimamente acquisiti, che non risulta dunque esplicitamente preclusa.

⁸⁶ Senza limiti espressamente prescritti alla circolazione probatoria, resterebbe infatti difficile immaginare l'applicazione analogica dell'*art.* 226 comma 5 disp. att. c.p.p., che vieta l'uso nel rito penale «in ogni caso», e «fatti salvi i fini investigativi», degli elementi acquisiti attraverso le attività preventive regolate dai commi precedenti.

L'inapplicabilità di tale divieto di utilizzo nel processo penale discende da più ragioni. La prima è che, in questo caso, il controllo *in itinere* è noto al diretto interessato, a differenza di quello (*ex post*) conseguente all'acquisizione retrospettiva dei dati a disposizione dei *provider ex art.* 226 comma 4 disp. att. c.p.p. Infatti, anche là dove si ritenesse il divieto *ex art.* 226 comma 5 disp. att. applicabile anche ai dati esterni del traffico telefonico e telematico acquisiti ai sensi dell'*art.* 226 comma 4 disp. att. c.p.p. (e dunque non solo alle

nonché, in questo caso ci troveremmo di fronte a una *function creep* ben più marcata rispetto a quella conseguente a un'ipotetica circolazione probatoria dei dati acquisiti mediante la sorveglianza digitale disposta da un giudice penale⁸⁷.

9. Gli "altri" braccialetti elettronici

In esordio, abbiamo dato conto dell'esistenza anche di *altri* braccialetti elettronici, per tali intendendo quelli indossati – ancorché in modo non libero e incondizionato – per scopi estranei a processo e esecuzione penale, e non riconducibili neppure al sistema della prevenzione. Come abbiamo constatato, dispositivi sottoposti al controllo in tempo reale di soggetti o enti terzi (pubblici come pure privati) possono infatti essere indossati per ragioni le più varie: per monitorare parametri sanitari di persone sottoposte a cure mediche⁸⁸; per tener d'occhio minorenni o persone non cognitivamente autosufficienti⁸⁹; per garantire la

intercettazioni preventive), resta il fatto che, al pari del trattenimento, anche la futuribile applicazione del braccialetto elettronico ai migranti non sarebbe comunque formalmente ascrivibile alla categoria delle misure di prevenzione. I dati acquisiti dal braccialetto non sarebbero dunque inutilizzabili *ex art.* 226 comma disp. att., prestandosi a essere incasellati nella categoria della prova documentale e conseguentemente impiegati anche in sede penale, in linea con la giurisprudenza maturata in relazione all'art. 220 disp. att. c.p.p. (v. ad esempio Cass., Sez. III, 11 aprile 2024, n. 26527, in *C.e.d.*, n. 286792).

⁸⁷ Con l'espressione *function creep* ci si riferisce al fenomeno per cui dati acquisiti o tecnologie impiegate per finalità circoscritte vengono riutilizzati per scopi ulteriori e più invasivi, in assenza di una rinnovata legittimazione giuridica e con la conseguente erosione delle garanzie a tutela dei diritti fondamentali. Il termine è stato sistematizzato da Roger Clarke, informatico e studioso australiano di *privacy*, in particolare nel testo *Tax File Number Scheme: A Case Study of Political Assurances and Function Creep* (1991) 7(4) *Policy*. Per una storia sull'uso del termine v. B.J. KOOPS, *The concept of function creep*, in *Law, Innovation and Technology*, 2021, vol. 13, n. 1, p. 29 ss.

⁸⁸ Si pensi agli *smartwatch* medicali per monitoraggio cardiaco o neurologico, come pure ai sensori glicemici continui, o ai medesimi dispositivi impiegati per verificare l'assunzione di alcol (di cui già abbiamo detto *supra*, al § 7), ove applicati solo per ragioni terapeutiche e non di monitoraggio penale.

⁸⁹ La questione è stata fatto oggetto di un primo parere del Garante della *privacy* del 25 gennaio 2018 (doc. 7810766, consultabile in *garanteprivacy.it*), sollecitato da una fondazione che gestiva una struttura per anziani a Mantova, con una richiesta motivata dalle difficoltà di controllare simultaneamente i pazienti bisognosi di un monitoraggio continuo, e avente lo scopo di prevenire cadute, vagabondaggio incontrollato, episodi di disorientamento, così da consentire agli operatori di intervenire tempestivamente. Riguardando persone fragili e dati sanitari (tra cui il controllo del battito cardiaco), il sistema ha ricevuto parere positivo perché si prefiggeva di rilevare solo i dati indispensabili, raccolti entro il perimetro della struttura, da conservare per il tempo strettamente necessario. Intuitivamente, la questione centrale coinvolge il tema del consenso: che dovrebbe essere consapevole,

sicurezza⁹⁰ o agevolare il compimento di determinate mansioni nel mondo del lavoro⁹¹.

La messe di informazioni potenzialmente custodite da questi dispositivi non si limita alla sola geolocalizzazione, ma si estende anche ad altre conoscenze, anche più sensibili, quali dati biometrici, “di movimento”, stato di veglia o sonno: informazioni che in determinate circostanze potrebbero rivelarsi preziose per saggiare la coerenza di prove dichiarative, come pure, più in generale, supportare o confutare determinate versioni dei fatti.

Premessa l'indubbia riconducibilità dei dati registrati da questi dispositivi alla categoria della prova documentale, va detto innanzitutto che la relativa raccolta è chiamata a rispettare la disciplina in materia di *privacy*, dalla quale dovrebbero coerentemente discendere tempi di conservazione dei dati improntati a una logica di minimizzazione oltre che di limitazione delle finalità.

Ciò premesso, si tratterà di comprendere, di volta in volta, se la relativa acquisizione al processo penale possa o meno scontrarsi con un divieto probatorio. La galleria di ipotesi appena abbozzata è assai varia, per diversità di situazioni, interessi e diritti volta a volta coinvolti; essa è tuttavia resa in qualche modo omogenea da un tratto comune, riconducibile alla definizione di *braccialetto elettronico* sposata nelle prime pagine di questo contributo: quando, anche sulla scorta del linguaggio frequentemente in uso, abbiamo dato atto di come tale espressione, nata per indicare i dispositivi usati a fini di sorveglianza digitale penale, venga spesso adoperata per alludere anche ad altri *wearable*, ove questi vengano indossati in conseguenza di una scelta non libera ma indotta, in modo più o meno stringente, da fattori esterni.

Nel caso di dispositivi finalizzati a monitorare a distanza determinati parametri (come livello di saturazione di ossigeno nel sangue, tasso glicemico, e soprattutto ECG, frequenza cardiaca, parametri neurologici, assunzione di alcolici), la scelta è infatti spesso imposta da esigenze connes-

e che rispetto a persone non in grado di rilasciarlo vede entrare in campo soggetti terzi, tra cui il responsabile della struttura sanitaria in cui il soggetto medesimo è ospitato. Tale parere conserva tuttora rilevanza perché ha costituito la prima occasione di pronuncia sul tema da parte del Garante, ed esprime principi che poi sono stati estesi anche alla sorveglianza domiciliare.

⁹⁰ Per rilevare cadute o incidenti, così assicurando l'invio di un allarme in tempo reale; per localizzare rapidamente i dipendenti in aree rischiose (ne sono un esempio i prodotti pubblicizzati sul sito safe-engineering.it/wearable-per-la-sicurezza-i-dispositivi-indossabili-che-proteggono-i-lavoratori); per tracciare segnali fisiologici utili a prevenire *stress* e infortuni, così da scongiurare incidenti o gestire meglio i carichi di lavoro (v. fatiguescience.com).

⁹¹ V. la casistica riportata in A. INGRAO, *Il braccialetto elettronico tra privacy e sicurezza del lavoratore*, cit.

se al diritto alla cura. Nel contesto lavorativo, essa potrebbe invece essere imposta per assicurare massime condizioni di sicurezza; e anche là dove non riconducibile a una funzione antinfortunistica, essa potrebbe essere dovuta alla necessità di ottemperare a stringenti direttive del datore di lavoro, difficili da declinare per via dell'assenza di una reale possibilità di scelta.

Sebbene la forza persuasiva caratteristica delle situazioni appena descritte non possa essere equiparata a quella in cui ad imporre il bracciale elettronico sia l'autorità giudiziaria penale, il fatto che il dispositivo sia anche in questi casi attivato in forza di una scelta coatta interroga in ordine alla esistenza di limiti alla possibilità di acquisire le conoscenze offerte dal dispositivo in seno a un processo penale. Tanto più che, per quanto egli abbia consapevolmente scelto di sottoporsi al monitoraggio, in questo caso l'interessato non si è consegnato al controllo delle agenzie penali, ma a quello di altri attori, nei confronti dei quali nutre una ragionevole aspettativa di riservatezza⁹²: garantire una piena circolazione probatoria implicherebbe qui un'eclatante ipotesi di *function creep*.

Pur non riguardando conoscenze acquisite mediante un dispositivo indossabile, la giurisprudenza maturata su questioni in qualche misura limitrofe lascia pronosticare un'altamente probabile risposta riduttiva, quantomeno con riferimento a dati di geolocalizzazione, che non dovrebbero offrire conoscenze tali da coinvolgere gli artt. 14 e 15 Cost. Si allude qui alle conseguenze della violazione dell'art. 4 dello statuto dei lavoratori, che sanziona il controllo a distanza della prestazione lavorativa⁹³: violazione che, malgrado integri una fattispecie di reato, il diritto vivente ha sempre ritenuto priva di ricadute processuali⁹⁴. Si allude, poi, alle violazioni della disciplina in materia di *privacy*⁹⁵, le cui conseguenze sul piano della utilizzabilità in un (qualsiasi) «procedimento giudiziario» sono rimesse alla disciplina «delle pertinenti disposizioni processuali» (secondo quanto stabilito dall'art. 160-*bis* del d.lgs. 30 giugno 2003, n. 196, introdotto nel 2018).

⁹² L'elaborazione del principio della *reasonable expectation of privacy* si deve alla Corte suprema degli Stati Uniti, a partire da caso *Katz v. United States* 18 dicembre 1967 (389 U.S. 347).

⁹³ Anche nella versione edulcorata dal *Jobs act*, che ha circoscritto la portata del divieto, tale disciplina continua a punire a titolo penale il datore di lavoro che vi trasgredisca. Ma sebbene essa costituisca il frutto di una condotta penalmente rilevante (e dunque di una prova illecita), la giurisprudenza ha sempre escluso l'inutilizzabilità della conoscenza acquisita in spregio all'art. 4 della l. 20 maggio 1970, n. 300 (v. ad esempio Cass., Sez. II, 4 aprile 2019, n. 23172, in *C.e.d.*, n. 276966).

⁹⁴ V. però, recentemente, Cass., Sez. I, 5 novembre 2025, n. 37457.

⁹⁵ V. ad esempio Cass., Sez. II, 22 aprile 2017, n. 28367, in *C.e.d.*, n. 270362, o Sez. V, 28 novembre 2014, n. 2304, *in*, n. 262686.

Senonché, il ricorso generalizzato, indiscriminato, privo di limiti alla categoria della prova documentale (per di più attraverso la strada privilegiata dell'art. 237 c.p.p.) lascia insoddisfatti.

Ciò vale – soprattutto – per i dati acquisiti mediante dispositivi di monitoraggio medico, in grado di registrare informazioni particolarmente sensibili, come tali soggette alla rigorosa disciplina di cui agli artt. 4 e 9 GDPR, che implicano un'aspettativa di riservatezza massima, e coinvolgono direttamente l'art. 32 Cost. In proposito, si consideri che, ove a conoscenza o nella disponibilità del personale sanitario, tali informazioni ricadrebbero nel raggio operativo degli artt. 200 e 256 comma 1 c.p.p., in materia di segreto professionale⁹⁶.

Malgrado tale disciplina accordi al sanitario una mera facoltà (di non deporre come pure di non consegnare i documenti posseduti per ragioni professionali), la relativa *ratio* depone nel senso di un'interpretazione rigorosamente improntata al principio di limitazione della finalità della raccolta dei dati registrati mediante il telemonitoraggio medico.

È vero: se i dati fossero conservati nel *wearables* nella disponibilità dell'imputato o dell'imputato, il *device* potrebbe essere acquisito mediante sequestro probatorio; tuttavia, se per accedere al contenuto del dispositivo fosse necessaria la collaborazione del personale sanitario (ad esempio per fornire la relativa chiave di accesso), ci troveremmo comunque di fronte a una situazione in cui il segreto professionale potrebbe essere comunque opposto.

Tale constatazione dovrebbe suggerire al legislatore una regolamentazione sostenibile dal punto di vista sistematico, da attuarsi attraverso l'introduzione di una clausola di inutilizzabilità nel processo penale riferibile a dati sensibili acquisiti mediante un consenso che sia stato circoscritto a finalità di cura.

10. Conclusioni

La rassegna sin qui svolta ha descritto la proliferazione di dispositivi tecnologici idonei ad assicurare il controllo a distanza, rispondenti a scopi

⁹⁶ È peraltro doveroso segnalare che l'art. 256 c.p.p. è stato interpretato in maniera riduttiva dalla giurisprudenza: v. Cass., Sez. IV, 16 gennaio 1998, n. 2270, in *C.e.d.*, n. 210262 (pronuncia cui mostra di aderire anche Sez. IV, 6 luglio 2006, n. 32300, *ivi*, n. 235183), che ha ritenuto utilizzabile il referto medico relativo ad un ricovero in ospedale a seguito di incidente stradale benché fosse stato acquisito dalla polizia giudiziaria senza il rispetto delle formalità previste dall'art. 256 c.p.p.

diversi ma spesso indicati con la comune espressione *braccialetto elettronico*, nata per alludere al controllo digitale attuato in sede penale.

Paradossalmente, tale locuzione è poco adatta a indicare gli strumenti preposti ad assicurare la sorveglianza operante in tale contesto (dove si ricorre a cavigliere), prestandosi piuttosto a raffigurare *wearable* e *device* impiegati per ragioni diverse, in particolare nel mondo della cura sanitaria e in quello del lavoro.

La matrice di tutti gli strumenti di cui ci siamo occupati si presenta comune. Infatti, i moderni dispositivi indossabili e i sistemi di telemonitoraggio utilizzati per scopi diversi da quelli propri del sistema penale si inseriscono in una traiettoria storica unitaria di controllo sul corpo, che affonda le proprie radici nelle sperimentazioni di telemetria degli anni '60 e che ha trovato la sua prima applicazione, in ambito penale, negli anni '80, quando è stata inaugurata una modalità di governo del comportamento fondata non sull'intervento umano (inevitabilmente episodico), ma sulla sorveglianza continua e mediata tecnicamente.

Riguardo al monitoraggio disposto a fini penali, i numeri in Italia sono decisamente contenuti rispetto a quelli riscontrabili in alcuni paesi di *common law*, e testimoniano la propensione a impiegare il braccialetto elettronico per tre diversi ordini di ragioni. Se nel 2000 l'introduzione dell'istituto nel nostro sistema giuridico intendeva rendere più effettive le prescrizioni connesse alla detenzione extracarceraria (disposta a titolo cautelare come pure in sede di esecuzione della pena), con le novelle del 2013-2015 il potenziamento dell'istituto è stato concepito soprattutto per alleviare il sovraffollamento che endemicamente affligge gli istituti di pena del nostro Paese. Negli ultimi anni, la crescente fiducia mostrata verso questa tecnologia ha inteso sfruttare i suoi progressi, così propiziandone la valorizzazione normativa onde contrastare la violenza di genere e domestica. Ciò è avvenuto nell'ambito non solo della disciplina cautelare personale (peraltro investita da una recentissima controtendenza, volta a incentivare il ricorso alle misure custodiali rispetto a quelle di minore impatto sulla libertà personale), ma anche di quella dedicata alle misure di prevenzione.

Parallelamente, la proliferazione del controllo a distanza mediante *wearable* sta interessando contesti i più disparati della vita reale (per tale intendendo quella esterna al processo). Con l'evoluzione tecnologica, la logica di controllo inaugurata a fini penali è stata infatti traslata e ampliata al di fuori del suo perimetro iniziale. Il monitoraggio a distanza del corpo interessa oggi anche altri rapporti asimmetrici, come quelli che legano il lavoratore al datore di lavoro o il paziente alla struttura sanitaria che lo ha preso in carico. In determinati contesti, infatti, indossare il sensore diviene spesso condizione di accesso a un servizio, a una prestazione lavo-

rativa o a un percorso di cura, di fatto comprimendo drasticamente lo spazio di autodeterminazione del singolo. In questa chiave, i dispositivi indossabili e il telemonitoraggio costituiscono l'espressione più avanzata di un controllo che si esercita attraverso il corpo e sta assumendo un'incidenza sempre più penetrante.

Se questo vale già per il presente, la constatazione di quanto accade fuori dai confini nazionali ci ha sollecitato a immaginare, sia pure in via ipotetica, l'approdo anche in Italia del controllo elettronico statale per scopi da noi finora inediti: in ordine al governo del consumo di alcol come argine alla possibile ricaduta in condotte violente, nonché, soprattutto, in ordine alla sorveglianza degli stranieri nella prospettiva di agevolarne il rimpatrio.

Se il primo tra questi due impieghi ancora sconosciuti al nostro ordinamento non pare di prossima importazione, il secondo identifica invece un'ipotesi tutt'altro che irrealistica, tanto da essere guardata con interesse dal governo in carica, impegnato ad affrontare le sfide del Patto europeo su migrazione e asilo.

A tale specifico proposito, le più recenti evoluzioni del diritto dell'immigrazione fanno presagire un futuro marcato da forme di sorveglianza digitale rese possibili grazie ad *app* da installare su *smartphone*, che potrebbero affiancare e anche soppiantare il ricorso a *device* indossabili, non foss'altro perché più economiche e facili da gestire. Dove si è già verificata, tale dinamica ha segnato un passaggio decisivo nell'evoluzione della sorveglianza: mentre braccialetti e cavigliere, basati su tecnologie RF o GPS, permettono la verifica della presenza domiciliare o la ricostruzione degli spostamenti, le *app* per *smartphone* si prestano a estendere in modo significativo la capacità di raccolta, analisi e trasmissione dei dati, basandosi sulla geolocalizzazione ma anche sulla biometria, sulla registrazione dei metadati del telefono e su *check-in* da soddisfare fotografandosi o registrando la propria voce in momenti non prevedibili. La conseguenza sta nell'espansione del controllo, che va a sommarsi al rischio di una gestione poco trasparente del trattamento di dati personali nella disponibilità di aziende private potenzialmente interessate a sfruttarli anche per scopi diversi rispetto a quelli sotesi alla loro raccolta⁹⁷.

⁹⁷ Stando ad alcuni studi (v. in particolare OWENS-F. ROESNER-T. KOHNO, *Electronic Monitoring Smartphone Apps*, cit.), le *app* di *electronic monitoring* raccolgono e trasmettono metadati del dispositivo, informazioni di rete e coordinate di geolocalizzazione con frequenza superiore a quanto dichiarato nelle *privacy policy*, che risultano spesso vaghe o incoerenti con il comportamento effettivo delle applicazioni. Inoltre, queste *app* si prestano a raccogliere dati non necessari agli scopi del monitoraggio (v. la p. 4086 del pdf).

Alla luce di ciò, la sorveglianza muta la propria fisionomia rispetto a quella resa possibile dai dispositivi indossabili tradizionali, rendendosi meno visibile ma al contempo più intensa; e quindi, al contrario delle apparenze, non necessariamente più conforme al principio di proporzionalità.

Questa proliferazione tecnologica porta con sé anche la conseguenziale crescita di informazioni potenzialmente utili a fini di accertamento penale.

Negli Stati Uniti, dove il numero di braccialetti elettronici in circolazione è enorme, il tema della circolazione probatoria ha già impegnato il diritto vivente, in particolare rispetto ai dati acquisiti grazie alla sorveglianza disposta in fase di rilascio o di esecuzione della pena. Accanto ad alcune questioni non suscettibili di investire il giurista italiano⁹⁸, la casistica americana ha fatto emergere interrogativi che potrebbero porsi pure da noi, visto che coinvolgono il ruolo dell'autorità giudiziaria rispetto all'ammissione dei dati digitali come prove in un procedimento diverso da quello in cui la sorveglianza è stata disposta⁹⁹.

⁹⁸ La giurisprudenza si è in parte concentrata sul possibile contrasto tra l'uso dei dati GPS del braccialetto con la *bearsay rule*: e ciò non perché il dato GPS sia in sé *bearsay*, ma perché i *report* che contengono quei dati spesso incorporano dichiarazioni umane, quali interpretazioni, riassunti, classificazioni: v. ad esempio quanto riportato da E. SHELEY, *Pennsylvania Supreme Court holds GPS Data is not Hearsay*, in *fedsoc.org*, 26 luglio 2023.

⁹⁹ Negli USA, la grande questione ruota attorno ai rapporti con il IV emendamento. Infatti, in quel sistema la decisione di applicare il braccialetto elettronico raramente promana dal giudice, che si limita a stabilire condizioni molto generiche, di fatto delegando la scelta in ordine alle modalità di controllo ad altri attori: i *probation officers* nel caso di *probation* o di *parole* (libertà condizionale, che peraltro non è disposta dal giudice ma da un organo amministrativo, la *parole board*), i *pretrial services agency* nel caso di *pretrial release*: ed è proprio questo a determinare l'attrito con il IV emendamento. Un attrito che si ripropone poi anche rispetto all'interrogativo ulteriore, molto rilevante ai nostri fini, concernente la necessità o meno di un *warrant* per consentire alle forze dell'ordine di recuperare i dati registrati grazie alla cavigliera. Sul tema v. l'importante saggio di K. WEISBURD, *Sentenced to Surveillance: Fourth Amendment Limits on Electronic Monitoring*, 98 *North Carolina Law Review* 717 (2020). Per una rassegna più recente di decisioni, v. D. SPIEGEL, *Can Law Enforcement Review Ankle Monitor Location Without a Warrant?*, *forensicsource.org*, 3 marzo 2025. In tale contesto, merita di essere qui segnalato il caso – davvero “estremo” – che ha visto numerose persone cui era stato applicato il braccialetto elettronico in fase di *pretrial-release* ricorrere contro il *Pre-Trial Electronic Monitoring* della Contea di San Francisco. Inizialmente, tale programma accordava allo sceriffo il potere di imporre il monitoraggio elettronico, nonché di raccogliere e conservare indefinitamente i dati di geolocalizzazione, nella prospettiva di condividerli con altre agenzie di *law enforcement*; in un secondo momento, il programma è stato modificato prevedendo che l'imposizione della sorveglianza elettronica fosse disposta dall'autorità giudiziaria. Dinanzi a questa importante variazione, con decisione del 23 aprile 2025, la Corte d'appel-

Viceversa, a quanto consta la giurisprudenza domestica ed estera non si sono ancora occupate dell'uso a fini di accertamento penale dei dati acquisiti dai *wearable* indossati in modo “coatto”, ancorché per ragioni estranee al controllo penale (e dunque a fini sanitari o acquisiti nell'ambito del contesto lavorativo)¹⁰⁰. Il tema tuttavia esiste, e potrebbe presentarsi anche in concreto.

Sulla scorta della disciplina italiana, abbiamo concluso come, *de iure condito*, le conoscenze procacciate grazie a tutti questi dispositivi si prestano a essere ricondotte alla categoria della prova documentale; e ciò indipendentemente dal fatto che la sorveglianza digitale sia stata decisa dall'autorità giudiziaria (penale) o da altri attori, pubblici o privati, come avviene in relazione ai pazienti monitorati a distanza e ai *connected worker*.

Con specifico riferimento alla sorveglianza penale, allo scenario complessivamente illustrato nelle scorse pagine non corrisponde ancora, in Italia, una diffusa consapevolezza di questioni e rischi che, già denunciati oltreoceano (dove le dimensioni ormai abnormi del fenomeno hanno indotto valutazioni e censure assai allarmate), potranno manifestarsi anche nel nostro Paese. Limitandosi ai principali fra gli aspetti critici, si possono menzionare: la totale assenza di impatto del ricorso alla sorveglianza digitale sui tassi di carcerizzazione (che in genere, anziché calare, aumentano parallelamente alle dimensioni della “gabbia digitale”); il difetto di proporzionalità in ordine all'impiego della sorveglianza digitale; la scarsa trasparenza nei rapporti con il singolo interessato, il cui consenso non sempre è adeguatamente informato; l'assenza di regole tassative in ordine ai tempi e alle modalità di conservazione dei dati; il ruolo significativo di aziende private coinvolte nella gestione del monitoraggio e che si muovono in una logica di lucro¹⁰¹; il livello non sempre indiscutibile di affidabilità dei dati tecnici acquisiti mediante il *device*.

Malgrado quelle appena accennate siano questioni note e dibattute, il

lo degli Stati Uniti, IX Circuito (causa *Simon v. City and County of San Francisco*, 135 F, 4th 784, 9th Cir. 2025: [v. caselaw.findlaw.com/court/us-9th-circuit/117200568.html](https://www.caselaw.findlaw.com/court/us-9th-circuit/117200568.html)), ha stabilito che il programma potesse rimanere in vigore e che la condivisione dei dati GPS fosse compatibile con il IV emendamento, ove effettivamente imposta da un'autorità giudiziaria nell'ordinanza di rilascio. Senza, dunque, che sia necessario un successivo mandato.

¹⁰⁰ La questione si è invece notoriamente presentata in relazione a dati acquisiti da *wearable* indossati in modo non coatto. Ciò è avvenuto anche in Italia, in almeno un caso, relativo a un processo per duplice omicidio celebratosi davanti alla Corte d'assise di Bologna, nell'ambito del quale i movimenti registrati dall'app Salute dello *smartwatch* in uso all'imputato nelle notti in cui si sono verificati i due decessi sono stati utilizzati per smentire la versione dei fatti resa dall'imputato.

¹⁰¹ A tale proposito, si consideri che negli USA i costi della sorveglianza elettronica sono posti a carico della persona sottoposta a monitoraggio.

legislatore italiano non se ne è ancora fatto carico, con una latitanza che si fa via via più grave man mano che si allarga lo spazio operativo accordato a questi strumenti e, al contempo, si modificano i connotati della sorveglianza, passati dal semplice controllo della permanenza in casa alla geolocalizzazione continua mediante GPS.

In Italia, l'estensione dell'ambito operativo del braccialetto elettronico impiegato a scopi penali intrapresa negli ultimi anni è per ora rimasta circoscritta al settore della criminalità contro le donne e in ambito domestico, le cui peculiarità e gravità riescono a giustificarla solo in parte. Tale estensione denota infatti un allontanamento dal principio di proporzionalità insito nel ricorso a una tecnologia – quella del tracciamento – quale presidio di controllo *immancabilmente* destinato ad affiancare l'allontanamento dalla casa familiare e il divieto di avvicinarsi alla persona offesa e ai “suoi” luoghi.

Come giustamente osservato anche dalla dottrina italiana, pur lasciando intatta la possibilità di circolare al di fuori della propria abitazione, il tracciamento è più intrusivo del monitoraggio domiciliare; tuttavia, visto che le due misure di cui agli artt. 282-*bis* e 282-*ter* c.p.p. possono trovare applicazione anche al di fuori dei limiti edittali prescritti in via generale dall'art. 280 c.p.p., ne consegue che pure il braccialetto potrà operare oltre quei limiti: e dunque nei confronti di soggetti indiziati di fattispecie penali contrassegnate da soglie di gravità non necessariamente elevate, oltretutto nell'ambito di procedimenti improntati a uno spiccato *favor* normativo per l'applicazione dei presidi cautelari. A tale specifico riguardo, il *net widening* è dunque evidente, visto che la custodia cautelare in carcere non sarebbe normativamente applicabile.

Riflettendoci, il laboratorio rappresentato dal doppio binario cautelare freneticamente edificato a protezione della vittima di violenza di genere e domestica individua una declinazione specifica ma potenzialmente pervasiva, pronta ad estendersi anche al contrasto di altre forme di criminalità, come pure ad approdare anche in contesti extrapenal, come quello migratorio, secondo una dinamica già osservata in altri sistemi.

Da qui l'esigenza di sollecitare il legislatore a svolgere almeno una riflessione, nonché, soprattutto, a colmare alcune lacune, *in primis*, ma non solo, in relazione alla sorveglianza disposta dal giudice penale.

La riflessione attiene innanzitutto alla determinazione dello spazio applicativo della sorveglianza tecnologica da remoto, la quale, anche ove dovesse essere declinata sfruttando le potenzialità offerte dagli *smartphone*, andrebbe comunque modulata nella piena consapevolezza della forza intrusiva di tale alternativa al braccialetto.

L'affidamento mostrato dal legislatore degli ultimi anni verso il monitoraggio elettronico non si è infatti accompagnato a un'adeguata valuta-

zione di impatto in ordine al rispetto del principio di proporzionalità. Ne deriva l'esigenza di un ripensamento; un ripensamento ben diverso, però, da quello operato dall'ultima riforma intervenuta sulla materia cautelare, che, introducendo il comma 3.1 nel corpo dell'art. 275 c.p.p., si è posta in antitesi con le novelle di poco precedenti, tornando a puntare sulle misure custodiali e così dando prova di un'inedita diffidenza per lo strumento tecnologico. Infatti, tale sfiducia si deve evidentemente non all'eccessiva intrusività del mezzo, quanto piuttosto alle difficoltà di assicurarne una gestione che sia davvero in grado di contrastare determinate forme di devianza.

La riflessione deve coinvolgere il significato e i confini del consenso richiesto all'individuo da sottoporre a monitoraggio: un consenso cui il sistema mostra di attribuire un ruolo sovradimensionato, quasi esso fosse in grado di travalicare l'esigenza di un impiego proporzionato del mezzo, e quasi esso fosse realmente libero e non il frutto di una costrizione generata dalla prospettiva di una più gravosa restrizione della libertà personale. Da tale riflessione scaturisce la presa d'atto dell'esigenza di calibrare in modo prudente lo spazio applicativo del braccialetto elettronico, così da scongiurarne un uso eccessivo, come pure la tentazione di sostituirlo con le applicazioni per *smartphone*, che, per quanto visivamente non stigmatizzanti, sono in grado di raccogliere più dati personali rispetto alla sola geolocalizzazione.

Ne consegue, poi, l'esigenza di un'attenta definizione di requisiti e perimetro del consenso richiesto a imputato, condannato o prevenuto, come pure alla persona offesa coinvolta dal tracciamento (e, un domani, allo straniero irregolare o al richiedente asilo): malgrado ne postuli il rilascio per far operare il dispositivo tecnologico, la legge infatti non spende una parola in ordine ai contenuti di tale consenso, destinato a essere raccolto e documentato dalla polizia giudiziaria ma senza che siano prescritti particolari requisiti sul piano informativo.

Quanto alle lacune, l'*excursus* che abbiamo svolto ne ha segnalate almeno due, concernenti l'assenza di limiti alla circolazione probatoria e, ancor prima, di regole puntuali dedicate ai tempi di conservazione dei dati, la cui esistenza sarebbe in grado di incidere a monte sul possibile riutilizzo delle conoscenze acquisite grazie al monitoraggio.

In proposito, abbiamo escluso la possibilità di un'applicazione analogica della disciplina racchiusa nell'art. 132 cod. *privacy* ai dati raccolti a fini di sorveglianza penale. Tuttavia, la circostanza che tale disciplina sia riferita anche ai dati di geolocalizzazione dei *device* porta a caldeggiare regole che stabiliscano tempi di conservazione e requisiti per il possibile futuro impiego dei dati ottenuti, nel rispetto dei principi di proporzionalità e di minimizzazione. Regole, va da sé, che, oltre a dover essere chiare, andreb-

bero anche rese note al diretto interessato, onde farle rientrare nello spettro del consenso.

Le soluzioni in rapporto alle diverse declinazioni della sorveglianza digitale a distanza passate in rassegna nelle scorse pagine non necessariamente dovranno essere unitarie; anzi, difficilmente potrebbero esserlo. Per quanto affrontate qui in un unico contesto descrittivo a causa dei loro tratti comuni – *in primis* la natura non libera della sottoposizione a controllo da remoto – tali diverse declinazioni riguardano contesti e coinvolgono interessi differenti, come pure dati personali non omogenei (e dunque, come tali, non sempre sottoposti alla medesima disciplina in materia di *privacy*). Soprattutto, tali distinte declinazioni implicano livelli di *creep function* non equiparabili, ma ordinabili fra loro in modo crescente: ove il *device* preposto al monitoraggio sia applicato nell'ambito di un procedimento penale, l'eventuale circolazione probatoria in un diverso rito penale è più prevedibile da parte del sorvegliato; all'opposto, la prevedibilità si abbassa drasticamente nei casi di dati acquisiti tramite gli “*altri*” braccialetti elettronici, per tali intendendo quelli che l'individuo indossa in modo non libero ma condizionato da situazioni di necessità (l'esempio è quello delle cure mediche) o da rapporti di potere asimmetrico (come avviene al *connected worker*). In questi ultimi casi, trattandosi di dati acquisiti in un contesto extragiudiziario, non solo il dispositivo è stato applicato senza alcun intervento di un giudice, ma il consenso iniziale a indossare il *device* riguarda usi assai distanti da quelli di accertamento penale: il che rende il rischio di *creep function* particolarmente marcato¹⁰².

Queste constatazioni inducono a ipotizzare due diverse strategie che potrebbero prestarsi ad entrare in campo *de iure condendo*.

Rispetto alla sorveglianza elettronica disposta in ambito penale e preventivo, il legislatore dovrebbe adottare soluzioni conformi al principio di proporzionalità: *in primis* (e come già osservato), limitando già sul piano astratto il perimetro applicativo della sorveglianza elettronica; in secondo luogo, stabilendo tempi di conservazione dei dati non superiori a quelli di durata della misura cui è associato il monitoraggio¹⁰³;

¹⁰² In mezzo a questi due poli opposti si collocherebbe il monitoraggio disposto a fini di controllo dei migranti, che, per quanto finalizzato a scopi non penali, verrebbe comunque presumibilmente gestito dall'autorità di pubblica sicurezza (sia pure con il supporto di un operatore tecnico), secondo quanto stabilito dalla disciplina in ordine all'esecuzione dei provvedimenti espulsivi e alla gestione dei richiedenti asilo.

¹⁰³ Per quanto un'indicazione in tal senso possa inferirsi dal tenore dell'art. 4 comma 3 del decreto 2 febbraio 2001 del Ministero dell'Interno (secondo cui, come già ricordato al § 5, «i dati personali trattati nell'uso dei mezzi elettronici e degli altri strumenti tecnici di

infine, prescrivendo limiti alla circolazione probatoria, in considerazione della gravità del reato per cui si procede nel processo *ad quem* ed ivi altresì prevedendo un parametro di ammissibilità della prova che sia più stringente rispetto a quello, a maglie larghe, stabilito dall'articolo 190 c.p.p.¹⁰⁴. Ove, come di regola avviene, i dati di monitoraggio si trovassero nella disponibilità non dell'autorità giudiziaria ma del fornitore tecnico (*Fastweb*), per la loro acquisizione andrebbe prescritta un'autorizzazione del giudice sulla falsariga di quanto prescritto dall'art. 132 comma 3 cod. *privacy*.

Con riferimento agli *altri* braccialetti elettronici, l'attenzione del legislatore penale andrebbe invece giocoforza focalizzata sulla previsione di limiti stringenti alla possibile circolazione probatoria, diversamente modulabili in considerazione del tipo di dato da acquisire e comunque condizionata a un intervento giudiziale motivato sulla scorta di requisiti improntati al principio di proporzionalità, anche qui secondo uno schema simile a quello rinvenibile nell'art. 132 comma 3 d.lgs. 196 del 2003.

Limiti stringenti andrebbero estesi anche all'eventualità, tutt'altro che immaginaria, in cui forme di sorveglianza elettronica dovessero essere introdotte a scopo di controllo dei migranti. Come abbiamo rilevato, consentire un monitoraggio pervasivo e continuativo dei movimenti di persone neppure sospettate di aver commesso un reato è una scelta controversa¹⁰⁵; ove venisse davvero intrapresa, per controbilanciare gli effetti di una sorveglianza massiva giustificata da finalità amministrative sarebbe doveroso introdurre un divieto radicale di reimpiego dei dati acquisiti per fini diversi da quelli sottostanti al ricorso alla sorveglianza elettronica (o quantomeno condizionarne l'eventuale riutilizzo in un processo penale solo nella prospettiva di accertare delitti di elevatissima gravità).

In ogni caso, le singole questioni qui segnalate andrebbero comun-

controllo sono utilizzati per le finalità di applicazione del capo VII del decreto legge 24 novembre 2000, n. 341 [...]), in proposito sarebbe opportuna una prescrizione più puntuale, oltre che racchiusa in una norma di legge.

¹⁰⁴ *Mutatis mutandis*, lo schema potrebbe essere quello di cui all'art. 270 c.p.p., che, oltre a condizionare l'acquisizione dei risultati delle intercettazioni nel processo *ad quem* alla gravità del delitto per il quale si procede, stabilisce anche requisiti di ammissione della prova – la rilevanza e la indispensabilità – più restrittivi di quelli, generali, *ex art. 190 c.p.p.*

¹⁰⁵ V. quanto affermato dalla *High Court* di Londra in ordine al progetto pilota svoltosi recentemente in Gran Bretagna (con una pronuncia di cui s'è fatta menzione *supra*, alla nota 79).

que regolate in modo preciso e tassativo, sull'onda della crescente attenzione riservata al tema della *data retention*¹⁰⁶.

¹⁰⁶ Il tema è interessato dalle evoluzioni sfociate nella novella del 2021 (d.l. 30 settembre 2021, n. 132, conv. con mod. con l. 23 novembre 2021, n. 178), che ha imposto il necessario intervento del giudice per acquisire i dati (tra cui quelli di geolocalizzazione) nella disponibilità dei *provider*, e dovrebbe a breve vedere l'inserimento di alcuni commi aggiuntivi (3-*bis*.1 ss.) nel corpo dell'art. 132 cod. *privacy*, nell'ottica di dare attuazione al regolamento (UE) 2023/1543, relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali. In proposito, v. lo Schema di decreto legislativo recante individuazione delle autorità competenti di cui all'articolo 31 del regolamento (UE) 2023/1543, relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali, nonché delle procedure per l'emissione, ricezione, esecuzione e riesame degli ordini europei di produzione e di conservazione (Parere ai sensi degli articoli 1 e 19 della l. 13 giugno 2025, n. 91), trasmesso alla Presidenza del Senato il 6 ottobre 2025. Il disegno di riforma dovrebbe portare anche all'inserimento di un nuovo art. 263-*bis* c.p.p.

ACCESSO AI DISPOSITIVI ELETTRONICI E PRINCIPIO
NEMO TENETUR SE DETEGERE: PASSWORDS BIOMETRICHE
ED ALFANUMERICHE, ORDINI DI DECRITTAZIONE
E DI PRODUZIONE

GIACOMO COTTI

SOMMARIO: 1. L'accesso ai dispositivi elettronici: una sfida per la giustizia penale. – 2. Il versante sovranazionale... – 3. Segue. Uno sguardo comparato. – 4. Obbligo di rivelazione della password e diritto al silenzio: codici alfanumerici... – 5. Segue. Chiavi d'accesso biometriche. – 6. Obblighi di decrittazione e di produzione. – 7. Collaborazione “spontanea” e valutazione del “silenzio”. – 8. Cooperazione “fittizia” e attacchi a “forza bruta”. – 9. Obbligo di rivelazione della password e privilegio contro l'autoincriminazione. – 10. Conclusioni.

1. *L'accesso ai dispositivi elettronici: una sfida per la giustizia penale*

L'evoluzione tecnologica ha modificato la maniera di intendere il procedimento e il processo penale. La quantità di informazioni disponibili su fatti e persone è accresciuta vertiginosamente dall'onnipresenza di dispositivi quali cellulari, *tablet* e *computer*; le indagini condotte su tali apparecchi sono divenute ordinaria amministrazione; la valutazione delle prove da essi estratte è ormai appannaggio di esperti (periti e consulenti tecnici), rispetto alle cui conoscenze specialistiche giudici e parti appaiono sempre più ridotti al rango di discenti.

Questo stato di cose apre notevoli problemi giuridici, a partire da quello che si colloca *in apicibus*, ossia l'individuazione dei valori – costituzionali, internazionali, convenzionali – in grado di governare l'indagine condotta su questi apparecchi: molti di essi possono infatti costituire, ad un tempo, vere e proprie “estensioni” del corpo umano (art. 13 Cost.), in quanto appendici ormai inseparabili dall'utente¹; “luoghi” meritevoli di

¹ M. TORRE, *Privacy e indagini penali*, Giuffrè, Milano, 2020, p. 27; L. PARLATO, *Libertà*

tutela, in quanto proiezioni dell'individuo nello spazio virtuale (art. 14 Cost.)²; “mezzi di comunicazione”, data la loro diffusa idoneità ad inviare, ricevere e conservare messaggi (art. 15 Cost.)³; manifestazioni d'una «libertà informatica» di nuovo conio, discendente dal catalogo aperto dei diritti inviolabili (artt. 2 Cost. – 8 CEDU) ed idonea a proteggere l'uso riservato delle tecnologie dell'informazione (ICT)⁴, a tutelare la *privacy*⁵, ovvero a preservare la «intangibilità della vita digitale»⁶.

A questo tema di fondo se ne aggiungono ulteriori, più specifici. Si pensi alla scarsa consapevolezza da parte degli utenti circa il fatto che i dati raccolti potrebbero venir scoperti, o che talune funzionalità dei dispositivi potrebbero esser sfruttate a scopo investigativo (con possibile apertura di spazi alle indagini atipiche o ad attività meramente esplorative); alla difficoltà di tracciare una linea di demarcazione fra dati ostensibili e dati privilegiati (con possibile lesione della disciplina dei segreti); al rischio di elusione dei limiti posti dalla legge a tutela delle corrispondenti prove nel mondo “fisico” (con potenziale aggiramento dei divieti probatori); nonché all'incertezza circa la affidabilità dei dati estratti dai dispositi-

della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale, in *Proc. pen. giust.*, 2020, n. 2, p. 295-298. Tale assetto è particolarmente evidente nel caso degli *smartphone*: cfr. Corte cost., 31 marzo 1987, n. 88, punto 2 del *Considerato in diritto*. In dottrina, A. CAMON, *Cavalli di Troia in Cassazione*, in *Arch. n. proc. pen.*, 2017, n. 1, p. 95.

² Per tutti, G. PICA, *Diritto penale delle tecnologie informatiche*, Utet, Torino, 1999, p. 38.

³ Vista anche la nozione ampia di “comunicazione” da ultimo sposata da Corte cost., 27 luglio 2023, n. 170. A favore della parificazione fra intercettazioni e sequestri di *smartphone*, *tablet*, *computer*, o di «device dalle funzioni similari» si veda ad esempio K. LA REGINA, *Il sequestro dei dispositivi di archiviazione digitale*, in *Penale. Diritto e procedura (web)*, 12 ottobre 2023, p. 3.

⁴ Così R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv. it. dir. proc. pen.*, 2018, p. 540 ss., il quale opera una comparazione con la giurisprudenza costituzionale tedesca, che in una celebre decisione (*Bundesverfassungsgericht*, 27 febbraio 2008, in *Riv. trim. dir. pen. ec.*, 2009, p. 679 ss., con nota di R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona*) ha riconosciuto l'esistenza di un “nuovo” diritto all'uso riservato dei sistemi informatici, in grado di comprendere e superare nell'ambiente digitale sia la classica libertà di domicilio, sia la protezione delle comunicazioni.

⁵ Nella Costituzione non è presente una tutela esplicita del diritto alla *privacy*, ma quest'ultima è stata ricondotta, da alcuni studiosi, alla manifestazione di uno (o più) diritti inviolabili, quali gli artt. 13, 14, 15, 21 Cost., oppure direttamente all'art. 2 Cost., come affermato pure dalla Corte costituzionale (Corte cost., 4 dicembre 2009, n. 320). Per una ricostruzione del sottostante dibattito, si veda S. CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in D. NEGRI (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Aracne, Aprilia, 2007, p. 9 ss.

⁶ S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 69-71.

tivi e dei metodi acquisitivi impiegati (con i relativi problemi in ordine alla valutazione giudiziale della prova scientifica/tecnologica).

Tutti questi aspetti meriterebbero un separato approfondimento. Oggetto della presente trattazione sarà, invece, un punto ulteriore, in un certo senso prodromico rispetto a quelli elencati, riassumibile nel seguente quesito: è legittimo – ed eventualmente, a quali condizioni – forzare l'utente a far accedere gli investigatori al proprio dispositivo?

Gli apparecchi in parola presentano infatti un rapporto conflittuale con i sistemi di sicurezza.

Da una parte, è facoltà dell'utente, nella maggior parte dei modelli, inserire una misura di blocco in modo da favorire la protezione dei dati personali e al fine di prevenire l'uso del *device* da parte di terzi. Ciò può avvenire nelle forme di una *password* alfanumerica (combinazione di lettere, numeri e/o altri caratteri)⁷ o, sempre più spesso, biometrica (scansione della retina, dell'iride, delle impronte digitali, dei tratti somatici, del padiglione auricolare, o ancora riconoscimento di un campione vocale, dell'andatura, finanche della battitura o della firma, solo per fare alcuni esempi)⁸.

Dall'altra, la lecita barriera posta dal privato a tutela di ingressi non desiderati rischia di scontrarsi con l'altrettanto legittimo interesse pubblico alla repressione degli illeciti penali. Se è vero che tra i doveri di carattere "sociale" richiamati dall'art. 2 Cost. ed esigibili dai consociati va annoverato anche il contributo all'accertamento del fatto⁹, è doveroso chiedersi come tale obbligo vada modulato in ragione della veste processuale assunta dal destinatario della richiesta della *password* e in virtù del tipo di prestazione domandata.

Lo studio va quindi impostato tenendo presente che a chiavi diverse possono corrispondere comportamenti diversi: quelle alfanumeriche permettono infatti una autenticazione basata su qualcosa che l'utente "ha" o "conosce" – vale a dire una parola d'ordine o un codice PIN; quelle biometriche, al contrario, valorizzano qualcosa che l'utente "è" – ossia, verificano la dichiarazione d'identità tramite il confronto fra la caratteristica

⁷ In questa categoria ci si sente di includere pure la *password* grafica, la quale permette di sbloccare il dispositivo tracciando un certo segno sullo schermo, visto che pare suscettibile di venir immessa materialmente o comunicata alla stessa stregua di un codice tradizionale.

⁸ Per questa ultima elencazione, si veda G.L. MARCIALIS, *La sicurezza informatica di frontiera*, in G. COLAIACOVO (a cura di), *Sicurezza, informazioni e giustizia penale*, Pacini Editore, Pisa, 2023, p. 394.

⁹ Per tutti, T. ALESCI, *Il corpo umano come fonte di prova*, Cedam, Padova, 2017, p. 22.

soggettiva (*feature*) rilevata dal sensore e un campione comparativo (*template*) in precedenza memorizzato dal *device*¹⁰.

Non stupisce che proprio queste ultime misure di sblocco siano arrivate a diffondersi rapidamente nel campo degli apparecchi elettronici, in quanto appaiono in grado di offrire, rispetto ai tradizionali codici, molteplici vantaggi: risultano infatti più difficili da compromettere o da rubare, e sono quindi più sicure; velocizzano l'accesso al dispositivo, non richiedendo alcuno sforzo mnemonico; non ammettono condivisione, poiché basate su caratteri fisionomici o comportamentali esclusivi dell'utente. In virtù di questi punti di forza, le *password* biometriche appaiono sempre più appetibili anche nel caso degli apparecchi elettronici di nuova generazione, ossia i c.d. dispositivi indossabili (es. i *fitness trackers*), viste le ridotte dimensioni di questi ultimi e la loro fisiologica capacità di raccogliere e conservare proprio i dati biometrici¹¹.

Il problema non è però di carattere settoriale, essendo un quesito che ha parimenti modo di porsi per la generalità degli *electronic devices* (soprattutto *computer*, *smartphone* e *tablet*) recanti contenuti appetibili a fini di giustizia. Si cercherà perciò di tematizzare l'argomento in un'ottica di ampio respiro.

2. Il versante sovranazionale...

Prima di esaminare la normativa primaria italiana occorre chiedersi se una soluzione non si possa trovare già sul piano delle fonti sovranazionali. La ubiquità della tecnologia e le conseguenti sfide impongono infatti di provar a dare una risposta che trascenda le scelte del singolo ordinamento.

In quest'ottica, significativo pare l'art. 19 § 4 della Convenzione di Budapest sulla criminalità informatica, che impone agli Stati parte di introdurre misure volte a «consentire alle proprie competenti autorità di ordinare ad ogni soggetto che abbia conoscenza del funzionamento del sistema informatico o delle misure utilizzate per proteggere i dati [...] in esso contenuti, di mettere a disposizione tutte le informazioni ragionevolmente necessarie [...]» al sequestro e alla perquisizione di supporti o sistemi. La platea di potenziali destinatari individuata da un così generico riferimento permette di sorreggere la scelta, compiuta da numerosi stati

¹⁰ G.L. MARCIALIS, *La sicurezza informatica di frontiera*, cit., p. 392 ss.

¹¹ Cfr. A. BIANCHI - I. OAKLEY, *Wearable authentication: trends and opportunities*, in *Information Technology*, p. 255 ss.

aderenti, di introdurre veri e propri *decryption orders* la cui inottemperanza talvolta è penalmente sanzionata, attivando così un rischio di contrasto con il *nemo tenetur* dei destinatari di simili provvedimenti.

Tuttavia, il riferimento dell'articolo (§ 5) alle condizioni e tutele di cui all'art. 15 del medesimo documento – il quale a sua volta richiama espressamente la Convenzione europea dei diritti dell'uomo quale base inderogabile per l'instaurazione, implementazione e applicazione dei poteri e delle procedure previste dal trattato¹² – potrebbe implicare che una simile richiesta non possa venir rivolta ad un indagato, in quanto potenzialmente lesiva del suo diritto a non autoincriminarsi¹³.

Ciò sposta inevitabilmente l'attenzione sulla norma di rinvio, vale a dire la garanzia euro-convenzionale del diritto al silenzio. La Corte di Strasburgo ha infatti da tempo ricavato in via implicita questa cautela dal diritto ad un processo equo (art. 6 § 1 Conv. e.d.u.)¹⁴ e dalla presunzione di innocenza (art. 6 § 2), ritenendola funzionale ad evitare errori giudiziari e a mantenere l'onere della prova in capo all'accusa¹⁵.

Il diritto in parola, se pur talvolta è stato esteso fino a coprire anche la consegna di documenti¹⁶, va comunque incontro a diversi limiti. Innanzi tutto, non risulta in grado di impedire l'uso nei procedimenti penali di evidenze ottenute coattivamente e al di fuori della volontà dell'accusato¹⁷; inoltre, anche una volta che una compressione sia stata riscontrata, non è detto che questa risulti "impropria"¹⁸, cioè in grado di condurre all'an-

¹² Convenzione del Consiglio d'Europa sulla criminalità informatica, Budapest, 23 novembre 2001, art. 15 § 1 secondo cui «[o]gni Parte deve assicurarsi che l'instaurazione, implementazione e applicazione dei poteri e delle procedure previste in questa sezione siano soggette alle condizioni e alle tutele previste dal proprio diritto interno, che deve assicurare un'adeguata tutela dei diritti umani e delle libertà, in particolare dei diritti derivanti da obblighi assunti in base alla Convenzione del Consiglio d'Europa del 1950 per la tutela dei diritti umani e delle libertà fondamentali, alla Convenzione Internazionale delle Nazioni Unite del 1966 sui diritti civili e politici, e agli altri strumenti internazionali applicabili in materia di diritti umani, e che deve considerare il principio di proporzionalità».

¹³ M. HILDEBRANDT, *Law for computer scientists and other folk*, Oxford University Press, Oxford, 2020, p. 180-181; J.J. OERLEMANS - M. GALIĆ, *Cybercrime investigations*, in W. VAN DER WAGEN - J.J. OERLEMANS - M.W. KRANENBARG (eds.), *Essentials in cybercrime. A criminological overview for education and practice*, Eleven, Utrecht, 2022, p. 238; M. HILDEBRANDT, *Law for computer scientists and other folk*, Oxford University Press, Oxford, 2020, p. 180-181.

¹⁴ Corte e.d.u., 25 febbraio 1993, Funke c. Francia, § 44.

¹⁵ Corte e.d.u., Gr. Ch., 17 dicembre 1996, Saunders c. Regno Unito, § 68.

¹⁶ Corte e.d.u., 5 aprile 2012, Chambaz c. Svizzera, § 50-58; Corte e.d.u., 3 maggio 2001, J.B. c. Svizzera, § 63-71.

¹⁷ Corte e.d.u., Saunders c. Regno Unito, cit., § 69.

¹⁸ Corte e.d.u., Gr. Ch., 8 aprile 1996, John Murray c. Regno Unito, § 45.

nientamento dell'essenza stessa della garanzia¹⁹. Difatti, a giustificare la costrizione potranno esser sufficienti, oltre all'esame della natura e del grado dell'interferenza, l'efficacia delle cautele procedurali apprestate e l'uso fatto delle informazioni così ottenute²⁰.

Non è quindi chiaro come potrà orientarsi la Corte europea sul punto, anche se la questione già è stata proposta²¹. Da un lato, i giudici alsaziani potrebbero accettare la distinzione – già menzionata, e che sarà approfondita con più calma nel prosieguo – fra *passwords* alfanumeriche e chiavi d'accesso biometriche, proteggendo le prime in quanto prove dipendenti dalla volontà dell'accusato (*will-dependent*), poiché veicolate tramite dichiarazioni, e non le seconde, per la ragione opposta (*will-independent*), giacché trattasi di dati corporei; dall'altro, potrebbero ritenere che in entrambi i casi una coercizione possa venir ammessa quando opportunamente salvaguardata (tramite efficaci garanzie procedurali e nel rispetto del principio di proporzionalità)²².

Non è nemmeno escluso che la Corte europea opti per una tutela massimalistica delle *passwords* biometriche, ritenendole incoercibili al pari delle informazioni orali. Questa soluzione sembra invero più difficile, in quanto tali chiavi d'accesso paiono comunque costituite da elementi ottenibili senza la collaborazione dell'accusato, occorrendo al limite un modesto uso della forza – fermo restando il divieto di dar luogo a trattamenti inumani e degradanti (art. 3 Conv. e.d.u.). Tuttavia, l'art. 6 Conv. e.d.u., proprio perché non menziona il *nemo tenetur*, non prevede alcuna esplicita

¹⁹ Secondo Corte e.d.u., Gr. Ch., 13 settembre 2016, Ibrahim e altri c. Regno Unito, § 267, questa situazione potrebbe verificarsi, ad esempio, ove il sospettato venga spinto a testimoniare a fronte della minaccia di subire una sanzione, oppure venga punito proprio per via del rifiuto opposto; laddove venga assoggettato a pressioni fisiche o psicologiche implicanti la lesione dell'art. 3 Conv. e.d.u.; o ancora ove le autorità abbiano impiegato sotterfugi per acquisire da lui informazioni, poiché non in grado di ottenerle nelle sedi a ciò deputate.

²⁰ Corte e.d.u., Gr. Ch., 11 luglio 2006, Jalloh c. Germania, § 101. La Corte, nella stessa decisione, indica anche l'esistenza di un ulteriore criterio valutativo (§ 117), ossia *«the weight of the public interest in the investigation and punishment of the offence in issue»*, il quale, tuttavia, non è stato ripreso dalla giurisprudenza successiva.

²¹ Lamin Minteh c. Francia, richiesta n. 23624/20, presentata il 10 giugno 2020, comunicata il 31 maggio 2021. Il ricorso interroga la Corte sulla compatibilità con il diritto all'equo processo (art. 6 § 1 Conv. e.d.u.) e con il rispetto della vita privata e della corrispondenza (art. 8 Conv. e.d.u.) di una condanna penale inflitta ad un soggetto sottoposto a custodia (*garde à vue*) che si sia rifiutato di rivelare la *password* del proprio *smartphone* agli inquirenti.

²² Con riferimento a quest'ultima ipotesi, pare possibilista M. HILDEBRANDT, *Law for computer scientists and other folk*, cit., p. 181.

barriera, lasciando così la porta aperta anche ad una lettura estensiva della garanzia²³.

Indicazioni più solide non sembrano poi provenire dall'ordinamento euro-unitario, se si osserva come la stessa Direttiva 343/2016/UE, art. 7, pur riconoscendo ad indagati ed imputati il diritto a restare in silenzio (§ 1) e a non autoincriminarsi (§ 2), escluda la incompatibilità dello *ius tacendi* con la raccolta di «prove che possono essere ottenute lecitamente ricorrendo a poteri coercitivi legali e che esistono indipendentemente dalla volontà» del prevenuto (§ 3), tra le quali si annoverano i materiali acquisibili in forza di un mandato, o per cui sussista un obbligo legale di conservazione e di produzione, ovvero le analisi dell'aria alveolare espirata, del sangue, delle urine o dei tessuti corporei necessari ad eseguire la prova del DNA (*Considerando* n. 29). Non è chiaro se la elencazione delle evidenze coercibili sia tassativa o meramente esemplificativa, e perciò suscettibile di integrazione: in quest'ultimo caso, non può escludersi che gli Stati Membri impieghino questo inciso come base legale per costringere l'imputato a rivelare la chiave di accesso al proprio dispositivo²⁴.

La giurisprudenza della Corte di Giustizia dell'Unione Europea, dal canto suo, non sembra aver affrontato espressamente la questione. In un recente arresto, relativo alle garanzie applicabili durante l'accesso ai dati contenuti nel cellulare dell'indagato²⁵, la facoltà di opporre il diritto al silenzio è stata infatti estromessa dal *thema decidendum*, poiché già rispettata nel procedimento *a quo*²⁶.

Insomma, se e come la disciplina europea (convenzionale e comunitaria) arriverà ad abbracciare la tutela delle chiavi d'accesso è materia controversa. Quel che appare chiaro dalle note che precedono è però la dif-

²³ In questo senso si veda W. ZONTEK, *Biometric Encryption of Smart Devices and the Prohibition against Self-incrimination in Criminal Procedure. Old Guarantees in the New World*, in *Eur. Journ. Crime, Crim. Law Crim. Justice*, 32 (2024), p. 170 ss.

²⁴ A. PIVATY, *Opening Pandora's box: The Right to Silence in Police Interrogations and the Directive 2016/343/EU*, in *New Journ. Eur. Crim. Law*, 12 (2021), p. 339.

²⁵ Corte giust., Gr. Ch., 4 ottobre 2024, C-548/21, C.G. v Bezirkshauptmannschaft Landeck, § 81 ss. In particolare, la Direttiva 2016/680, letta alla luce degli artt. 47 e 52, § 1, della Carta di Nizza, è stata ritenuta ostativa ad una disciplina nazionale che consenta alle autorità procedenti di accedere ai dati contenuti in un cellulare, in assenza di una informazione agli interessati in ordine ai motivi sui quali l'autorizzazione, rilasciata da un giudice o da un'autorità amministrativa indipendente, si basa. Tale incombenza, finalizzato a tutelare il diritto ad un ricorso effettivo, opera a partire momento in cui l'informazione non rischi più di compromettere le indagini condotte da tali autorità.

²⁶ *Ivi*, § 21. In questa pronuncia, infatti, i vani tentativi della polizia austriaca di introdursi nel cellulare sequestrato scaturivano proprio dal legittimo rifiuto del ricorrente di consentire l'accesso ai propri dati.

fusa tendenza a operare un discrimine fra il “nucleo duro” del diritto al silenzio, basato su richieste di informazioni, e una sua “periferia” più flessibile, incentrata sulla acquisizione di *material evidence* – inidonea, in quanto tale, a costringere il prevenuto ad attivarsi.

3. Segue. *Uno sguardo comparato*

Una volta delineato il quadro sovranazionale, occorre chiarire come i diversi ordinamenti si pongano dinanzi alla sfida comune posta dall'accesso ai dispositivi elettronici.

Volendo schematizzare, emerge un duplice approccio seguito nei Paesi dell'Europa continentale e nelle isole britanniche.

Innanzitutto, si possono individuare Stati che, non operando alcuna distinzione in base al tipo di chiave d'accesso, pongono un obbligo generalizzato di collaborazione in capo al titolare del dispositivo o, in generale, ad ogni soggetto che abbia le conoscenze necessarie ad operare lo sblocco. In questa schiera si annoverano, ad esempio, ordinamenti quali Inghilterra e Galles²⁷, Irlanda²⁸, Belgio e Francia.

Questi due ultimi appaiono particolarmente didascalici, vista la radicalità delle scelte effettuate. In Belgio, infatti, l'art. 88-*quater* del *code d'instruction criminelle* prevede un obbligo di cooperazione (introdotto proprio in virtù dell'art. 19 § 4 della Convenzione di Budapest)²⁹ in capo a coloro che si presume abbiano una conoscenza particolare di un sistema informatico o dei servizi utilizzati per proteggere i dati ivi memorizzati, elaborati o trasferiti. Ad essi può venir ordinato di fornire, in forma comprensibile, informazioni circa le modalità di accesso al sistema o ai dati (§ 1) ovvero di eseguire operazioni sul *computer* oggetto d'indagine, quali l'accesso, la copia, la rimozione, la crittazione o la decrittazione dei dati contenuti (§ 2). A tal fine è necessaria un'ordinanza del giudice istruttore, il mancato rispetto della quale costituisce reato punibile con la reclusione fino a tre anni e/o con sanzione pecuniaria; se, tuttavia, la collaborazione

²⁷ In base al *Regulation of Investigatory Powers Act* (RIPA 2000), la polizia può richiedere l'accesso ai dati contenuti in dispositivi elettronici (sequestrati durante le indagini) protetti da crittografia. Ove l'imputato/indagato rifiuti di fornire il codice, la polizia ha la facoltà di chiedere al giudice l'emissione di un *notice requiring disclosure* ai sensi dell'articolo 49 RIPA. In caso di mancata ottemperanza a tale avviso, potrà essere inflitta una pena massima di 5 anni, qualora il procedimento riguardi casi di “*national security*” o “*child indecency*”; di 2 anni, nelle altre situazioni (art. 53 RIPA).

²⁸ *Section 48 Criminal Justice Theft and Fraud Offences Act* (2001); *Section 7 Criminal Justice Offences Relating to Information Systems Act* (2017).

²⁹ Cfr. *supra*, § 2.

rifiutata avrebbe potuto ridurre e/o attenuare le conseguenze di un reato grave, la pena si può spingere sino a 5 anni di reclusione e alla irrogazione di un'ammenda compresa tra 50.000 e 500.000 euro (§ 3).

Le condotte di cui al secondo paragrafo, per espressa indicazione normativa, non possono venir imposte all'imputato. Non è chiaro invece se tale esenzione riguardi anche l'obbligo cooperativo indicato nel primo paragrafo. In effetti, è lecito presumere che i prevenuti siano dotati di una "conoscenza particolare" dei sistemi informatici nella loro disponibilità³⁰. In tal senso sembra muoversi la giurisprudenza maggioritaria: smentendo un orientamento prima adottato da taluni tribunali inferiori³¹, la Corte di cassazione belga ha di recente ritenuto che il privilegio contro l'autoincriminatione e la presunzione di innocenza non siano diritti assoluti, e che un giudice istruttore possa perciò ordinare all'indagato – a pena di reclusione – di fornire il codice di accesso al suo telefono cellulare quando la decrittazione risulti fondamentale per scoprire la verità³². Il tribunale supremo ha quindi qualificato l'ordine in parola come un obbligo di carattere meramente "informativo", non implicante una cooperazione con le indagini: secondo la Corte, in breve, il codice di accesso integrerebbe di per sé un dato "neutro", privo di valenza autoincriminante³³. Un simile assetto è stato peraltro accolto, nello stesso torno di tempo, pure dal locale giudice delle leggi³⁴.

In maniera ancor più diretta, in Francia, la Cassazione ha avuto di recente modo di ribadire che indagati e imputati possono esser obbligati a comunicare agli inquirenti le *passwords* del telefono cellulare (*passcode*)³⁵. Secondo la motivazione addotta, il codice d'accesso costituirebbe infatti una *convention de déchiffrement*, ossia un mezzo di crittografia, una chiave volta a sbloccare lo schermo del telefono: dimodoché la garanzia contro l'autoincriminatione e il diritto di rimanere in silenzio non avrebbero modo di es-

³⁰ S. ROYER-W. YPERMAN, *You have the right to remain silent... until we want your smartphone password*, in *CiTiP blog*, 13 febbraio 2020, disponibile al sito law.kuleuven.be/citip/blog/you-have-the-right-to-remain-silent-until-we-want-your-smartphone-password/.

³¹ Cfr. anche per i richiami giurisprudenziali A. BEAZLEY, *Silence with caution: the right to silence in police investigations in Belgium*, in *New Jour. Eur. Crim. Law*, 12 (2021), p. 422-423.

³² Corte di cassazione belga, II Ch., 4 febbraio 2020, Hof c. Belgio, P.19.1086.N.

³³ *Ibidem*.

³⁴ Corte costituzionale del Belgio, 20 febbraio 2020, n. 28, § B.6.2. Secondo questa decisione, tale assetto normativo non violerebbe né il principio di uguaglianza, né il diritto ad un equo processo, né il diritto alla riservatezza.

³⁵ Corte di cassazione francese, assemblea plenaria, 7 novembre 2022, ric. n. 21-83.146; nello stesso senso si vedano Corte di cassazione francese, Ch. crim., 12 gennaio 2021, ric. n. 20-84.045; Corte di cassazione francese, Ch. crim., 10 dicembre 2019, ric. n. 18-86.878.

sere invocati, alla luce dell'art. 434-15-2 *code pénal*. Quest'ultimo punisce infatti il rifiuto di fornire la *password* con un'ammenda fino a 270.000 euro o 3 anni di reclusione (la pena è aumentata fino a 450.000 euro o a 5 anni di reclusione quando lo sblocco avrebbe potuto impedire un reato o ridurne i danni). Secondo la logica seguita (anche) dai giudici francesi, dunque, l'esame del telefono cellulare risulterebbe equiparabile ad una perquisizione, dal momento che il mezzo in parola corrisponderebbe ad uno spazio privato, non già ad un surrogato della persona indagata³⁶.

Un esito parzialmente diverso si può invece ravvisare presso un altro gruppo di Paesi, in cui il discrimine corre lungo la linea che divide *passwords* alfanumeriche e dati biometrici: ne fanno parte, ad esempio, Paesi Bassi³⁷ e Germania.

Particolarmente esplicativo appare l'approccio seguito in quest'ultimo ordinamento. Sebbene non sia possibile rinvenire un obbligo di *disclosure* della chiave d'accesso, il § 81b (1) StPO, relativo all'identificazione dell'indagato, è stato considerato in grado di legittimare le autorità a procedere allo sblocco dello *smartphone* mediante l'impiego di matrici biometriche³⁸. La ragione di questa esegesi è intuibile, e risiede nell'assenza d'una richiesta di cooperazione attiva rivolta al prevenuto³⁹.

³⁶ Così R. PARIZOT, *Qu'est-ce qu'un téléphone portable?*, in *Rev. science crim. dr. comparé*, 2021, n. 1, p. 129.

³⁷ È infatti vero che l'art. 125k del codice di procedura penale olandese esclude testualmente che un ordine di decrittazione possa venir impartito alla persona sottoposta ad indagini: nonostante ciò, questi può comunque venir fisicamente costretto a fornire dati biometrici per sbloccare il telefono. Il limite menzionato sembra infatti operare solo ove venga richiesta all'indagato una cooperazione attiva, non quando la chiave di accesso risulti indipendente dalla sua volontà e sia ottenibile mediante un uso proporzionato della forza.

Così Corte suprema olandese, 9 febbraio 2021, n. 19/05471 CW. Cfr. anche il testo attuale dell'art. 558 del codice di procedura penale olandese, a seguito delle modifiche in vigore dall'1 ottobre 2022 (valide fino all'1 ottobre 2025): «If a seized automated work is biometrically secured or the data are biometrically encrypted in the form of a fingerprint or an iris or facial image, the public prosecutor may order the investigating officer to undo this security or encryption. In order to execute this order, the investigating officer may take the measures that are reasonably necessary to do so, against the will of anyone who may reasonably be suspected of being able to undo this security or encryption» (traduzione dall'olandese).

Per un approfondimento, si veda P. TER VRUGT, *A pragmatic attitude: the right to silence in the Netherlands*, in *New Journ. Eur. Crim. Law*, 12 (2021), p. 394-395, la quale sottolinea che in taluni casi le corti inferiori sono arrivate a riconoscere un tale obbligo anche in caso di *passwords* "tradizionali", ove la situazione era risultata connotata da particolare urgenza.

³⁸ In tal senso si veda LG Ravensburg (2023) 11 Gs 69/23 (*Regional Court of Ravensburg*), secondo cui il § 81 cit. consentirebbe la raccolta delle impronte finalizzata a sbloccare il cellulare.

³⁹ Non a caso, la Corte territoriale ha anche specificato che la medesima conclusione sarebbe stata raggiungibile pure nel caso in cui la polizia avesse proceduto a porre forza-

All'esito di questa sommaria indagine, il cui scopo è di esemplificare un *trend* e non già di fornire analisi esaustive, emerge chiaramente come gli ordinamenti europei oscillino fra l'assenza di copertura delle chiavi d'accesso da parte del *nemo tenetur* e l'applicazione di tale garanzia (quantomeno) con riferimento al codice alfanumerico.

Una posizione simile a quest'ultima si registra anche oltreoceano, negli Stati Uniti d'America, dove la maggior parte delle corti statali e federali aderisce alla tesi secondo cui il Quinto Emendamento – a mente del quale «[n]o person [...] shall be compelled in any criminal case to be a witness against himself [...]» – troverebbe applicazione solo dinanzi alla richiesta d'una testimonianza, orale o scritta, *contra se*⁴⁰. Pertanto, il *privilege against self-incrimination* sarebbe in grado, in linea di principio, di coprire solo la rivelazione della *password* alfanumerica, non lo sblocco biometrico⁴¹.

Questa prima impressione va però temperata alla luce della teoria giurisprudenziale nota come *act of production doctrine*, secondo cui atti di carattere “testimoniale” sarebbero tutti quelli in grado di veicolare, in maniera non dissimile da una dichiarazione, notizie circa l'esistenza, il possesso e l'autenticità dei contenuti cercati⁴².

Una simile lettura solleva il dubbio che anche l'impiego della chiave d'accesso biometrica, non diversamente dall'esecuzione coattiva di altri comportamenti materiali – quali la decrittazione e la produzione – possa

tamente il polpastrello a contatto con lo schermo. La decisione non è comunque andata esente da critiche in dottrina, dal momento che la norma invocata non farebbe menzione alcuna della possibilità di impiegare dati biometrici a fini di sblocco, essendo volta a disciplinare solo la raccolta di dati a scopo identificativo. Così F. NICOLAI-M.H. MARAS-J. TRAUTMANN-J. SCHNEIDER, *When objects betray you: the Internet of Things and the privilege against self-incrimination*, in *Information & Communications Technology Law*, 33 (2024), p. 255 ss.

⁴⁰ Perché sia invocabile il Quinto Emendamento occorre che si verifichino tre condizioni: l'individuo deve esser costretto per legge a collaborare con il Governo; la condotta obbligata deve essere di carattere testimoniale, ossia idonea a costringere una persona a rivelare il contenuto della propria mente; l'informazione veicolata deve essere incriminante. Cfr. es. *Hiibel v. Sixth Judicial Dist. Court*, 542 U.S. 177, 189-190 (2004).

⁴¹ *United States v. Doe (In re Grand Jury Subpoena)*, 670 F.3d 1335, 1341 (11th Cir. 2012); *United States v. Kirschner*, 823 F. Supp. 2d 665 (E.D. Mich. 2010); *Commonwealth v. Baust*, 89 Va. Cir. 267 (2014). Di regola, infatti, il privilegio contro l'autoincrimination non opera con riferimento alla raccolta di campioni corporei. Cfr. es. *Schmerber v. California*, 384 U.S. 757, 760-765 (1966).

Metaforicamente, occorre perciò distinguere la consegna della “chiave per una cassaforte” (*key to a strongbox*) dalla rivelazione di una “combinazione” (*combination to a wall safe*). Pur avendo il medesimo scopo, la prima appare neutra sul piano del diritto a tacere, risolvendosi in una operazione dal carattere prettamente materiale, mentre la seconda appare potenzialmente lesiva del *privilege against self-incrimination*, in quanto impone al prevenuto di svelare il contenuto della propria mente. Cfr. *Doe v. United States*, 487 U.S. 201, 210, n. 9, 219 (1988) (Stevens, J., dissenting); *United States v. Hubbell*, 530 U.S. 27, 43 (2000).

⁴² *Fisher v. United States*, 425 U.S. 391, 410 (1976).

apparire un'attività gravida di significato, e risultare perciò meritevole di tutela. Sul punto non si registrano indirizzi univoci. Alcune corti hanno infatti ritenuto che costringere l'imputato a fornire un dato fisionomico come l'impronta digitale non lo porti, di per sé, ad autoincriminarsi⁴³; altre hanno optato per la tesi contraria, affermando che essere obbligati a sbloccare il dispositivo equivarrebbe a dover fornire l'ubicazione e i contenuti (indizianti) d'un "archivio"⁴⁴.

Tuttavia, anche volendo optare per quest'ultima esegesi estensiva, una eccezione si può in ogni caso rinvenire quando si sia al cospetto di una *foregone conclusion*. Secondo questa lettura, anch'essa d'origine pretoria⁴⁵, quando l'autorità che procede è in grado di indicare con un ragionevole grado di precisione (*reasonable particularity*) che l'elemento incriminato esiste, è autentico ed è sotto il controllo dell'interessato, l'atto di produzione forzata non assume più natura testimoniale, poiché non in grado di aggiungere nulla alle informazioni a disposizione dell'accusa⁴⁶. Quando tale esito si verifica, il valore dichiarativo dell'atto viene azzerato, e la cooperazione può conseguentemente venir imposta⁴⁷.

4. Obbligo di rivelazione della password e diritto al silenzio: codici alfanumerici

Per quanto riguarda invece l'ordinamento italiano, occorre partire dall'inesistenza, allo stato, di un obbligo di collaborazione in capo all'indagato/imputato relativo alla consegna della *password* alfanumerica.

⁴³ *In Matter of Search Warrant Application for [redacted text]* 279 F. Supp. 3d 800 (N. D. Ill. 2017). Più di recente, si veda *United States v. Payne*, 99 F.4th 495, 508-513 (9th Cir. 2024), che, pur rigettando nel caso di specie il valore testimoniale dello sblocco biometrico, arriva ad affermare come ciò dipenda in gran parte dalle dinamiche fattuali.

⁴⁴ *In re Search of a Residence in Oakland* 354 F. Supp. 3d 1010 (N. D. Cal. 2019). Più di recente, si veda *United States v. Brown*, No. 23-3074, 23 ss. (D.C. Cir. Jan. 17, 2025). In dottrina, favorevoli a questa visione sono Z.E. JACOBSON, *Face Off: Overcoming the Fifth Amendment Conflict Between Cybersecurity and Self-Incrimination*, in *Journal of Law and Health*, 36 (2023), p. 201; B.A. CARNES, *Face ID and Fingerprints: Modernizing Fifth Amendment Protections for Cell Phones*, in *Loy. L. Rev.*, 66 (2020), p. 202 ss.; H. METZ, *Your Device Is Disabled: How and Why Compulsion of Biometrics to Unlock Devices Should Be Protected by the Fifth Amendment Privilege*, in *Val. U. L. Rev.*, 53 (2019), p. 460 ss.

⁴⁵ Risalente a *Fisher v. United States*, cit., 411.

⁴⁶ Cfr. es. *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718, 3-4 (D. Vt. Feb. 19, 2009).

⁴⁷ È controverso se la *foregone conclusion* permetta anche la rivelazione diretta della *password* alfanumerica, e non solo la sua materiale immissione nel dispositivo. Alcune pronunce si sono espresse in senso favorevole, mentre altre hanno dissentito. Per un esempio delle prime, si veda *State v. Andrews*, 234 A.3d 1254 (N.J. 2020); per le seconde, invece, *Commonwealth v. Davis*, 220 A.3d 534, 548 ss. (Pa. 2019).

L'unica disposizione rassomigliante ad un *decryption order* sembra essere l'art. 248 c.p.p., ossia l'invito a consegnare la cosa cercata tramite perquisizione – la quale però non rappresenta un obbligo per l'indagato, ed è comunque volta ad ottenere la *res*, più che la chiave per accedere ad essa⁴⁸.

Tuttavia, scorrendo il codice è possibile imbattersi anche in alcuni punti deboli, suscettibili di aprire spiragli coercitivi.

Si pensi innanzi tutto alla perquisizione dei dispositivi elettronici (artt. 247 comma 1-*bis*; 352 comma 1-*bis* c.p.p.)⁴⁹. Se è vero infatti che l'autorità procedente è tenuta, anche in queste circostanze, ad avvertire l'indagato della facoltà di nominare un difensore di fiducia (artt. 356 c.p.p. - 114 disp. att. c.p.p.), lo stesso non può dirsi per quanto riguarda il diritto a tacere, del quale non viene fatta menzione⁵⁰.

Si pensi poi alla facoltà della polizia giudiziaria di richiedere alla persona sottoposta ad indagini, anche in assenza del difensore, «notizie e indicazioni» (art. 350, commi 5 e 6, c.p.p.), ovvero di ricevere da essa dichiarazioni spontanee (art. 350 comma 7 c.p.p.), senza alcun previo avviso circa il diritto a restare in silenzio⁵¹. Le notizie così ottenute dagli operanti risultano certo inutilizzabili (comma 6) o al più spendibili in dibattimento

⁴⁸ Un simile pensiero è stato espresso da A. ZAMPINI, nell'intervento alla conferenza *Dimensione giudiziaria e dimensione mediatica della presunzione d'innocenza*, EmpRiSe Project, Roma, 14 ottobre 2021. Attualmente non sono disponibili pubblicazioni o registrazioni in merito.

⁴⁹ Per l'osservazione secondo cui la distinzione tra perquisizione ed ispezione “informatica” si basa sulla presenza o meno di misure di sicurezza, si veda ad esempio P. FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, in A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA (diretto da), *Cybercrime*, 2^a ed., Utet Giuridica, Milano, 2023, p. 1603. In senso contrario si pone chi invece ritiene che tale distinzione dovrebbe venir superata nel caso delle indagini digitali, in quanto ogni perlustrazione del contenuto del dispositivo consisterebbe necessariamente in una ricerca della prova e non in una mera constatazione dello stato delle cose. Così ad esempio O. MURRO, *Lo smartphone come fonte di prova. Dal sequestro del dispositivo all'analisi dei dati*, Wolters Kluwer-Cedam, Milano, 2024, p. 124-125; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 210.

⁵⁰ A. LARONGA, *Sul valore probatorio del contegno non collaborativo dell'imputato nell'accertamento del fatto proprio*, in *Quest. giust. (web)*, 17 aprile 2014, p. 6. Cfr. anche A. MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici ... e non solo*, in *Proc. pen. giust.*, 2021, n. 4, p. 736-737.

⁵¹ *Ibidem*. Si segnala che oggi, a seguito della riforma operata con art. 3 comma 1 lettera b d.l. 16 settembre 2024, n. 131, convertito con modificazioni dalla legge 14 novembre 2024, n. 166, il comma 5 consente la richiesta di informazioni all'indagato sul luogo o nell'immediatezza del fatto «quando ciò è imposto dalla necessità di evitare un imminente pericolo per la libertà, l'integrità fisica o la vita di una persona oppure dalla necessità di compiere attività indispensabili al fine di evitare una grave compromissione delle indagini».

mediante le contestazioni (comma 7, che richiama l'art. 503 comma 3 c.p.p.)⁵². La lacuna informativa, tuttavia, rischia di mascherare una surrettizia elusione dello *ius tacendi* ove tali conoscenze rappresentino lo spunto investigativo che porti ad acquisire ulteriori elementi di prova, dei quali non sarà poi possibile lamentare l'invalidità⁵³. In altre parole, il contrappeso apprestato dal legislatore attraverso la comminatoria dell'inutilizzabilità – totale (comma 6) o parziale (comma 7) – pare pressoché inutile nel nostro caso, perché la *password* risulta comunque in grado di schiudere l'accesso ad una ricchissima platea di dati immuni da sanzioni processuali.

In termini concreti, ove gli inquirenti si trovino dinanzi alla difficoltà o all'impossibilità di superare le barriere poste all'ingresso nel dispositivo, potranno facilmente esser tentati di aggirare l'ostacolo stimolando il prevenuto a rilasciare le suddette "indicazioni" volte a proseguire l'indagine, o a fornirle "spontaneamente" – informazioni che, nel caso di specie, sarebbero rappresentate proprio dalla *password* o da un altro mezzo di decrittazione⁵⁴.

A fronte di quanto esposto, è facile comprendere come mai si rinvenga in dottrina, in un'ottica ricostruttiva, un diffuso consenso circa la necessità di ricondurre la richiesta della *password* all'area del diritto al silenzio in senso stretto – tanto che, si afferma, anche in caso di atti "a sorpresa" quali sono le perquisizioni (pure di dispositivi elettronici), la polizia giudiziaria e il pubblico ministero dovrebbero avvisare l'indagato della facoltà di non rispondere (artt. 64 comma 3 lett. b - 350 comma 1 c.p.p.) prima di domandargli la rivelazione della chiave di accesso⁵⁵. Solo in tale

⁵² Le dichiarazioni spontanee possono però venir impiegate nella fase procedimentale, ossia in sede di incidente cautelare e nei riti a prova contratta. Cfr. es. Cass., Sez. II, 13 marzo 2018, Basso, in *C.e.d.*, n. 272541 – 01.

⁵³ A. LARONGA, *Sul valore probatorio del contegno non collaborativo dell'imputato nell'accertamento del fatto proprio*, cit., p. 6. Nello stesso senso si esprimeva già MARAFIOTI, *Digital evidence e processo penale*, in *Cass. pen.*, 2011, n. 12, p. 4516.

⁵⁴ *Ibidem*.

⁵⁵ L. LUPARIA, *Computer crimes e procedimento penale*, in G. GARUTI (a cura di), *Trattato di procedura penale*, vol. VII, t. I, Utet Giuridica, Torino, 2001, p. 387-388; ID., *Processo penale e tecnologia informatica*, in *Diritto dell'internet*, 2008, n. 3, p. 227-228; ID., *Disciplina processuale e garanzie difensive*, in AA.VV., *Investigazione penale e tecnologia informatica: l'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè, Milano, 2007, p. 159-160. Nello stesso senso si vedano N. ROMBI, *Mentire sui propri precedenti penali equivale a difendersi? La soluzione della Corte costituzionale a tutela del diritto al silenzio*, in *Proc. pen. giust.*, 2024, n. 1, p. 70-71, che osserva come «[i]n queste situazioni, il mancato avvertimento, laddove accompagnato dal possibile impiego di quanto dichiarato, magari anche solo a fini orientativi delle indagini, permette che si realizzi una censurabile rinuncia inconsapevole al diritto al silenzio»; A. DEL GIUDICE, *The principle of nemo tenetur se detegere in the age of data*, in *Revista "Curentul Juridic"*, 98 (2024), p. 84; F.N. RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella*

maniera potrebbe dirsi tutelato lo *ius tacendi*, a sua volta baluardo della libertà di autodeterminare le opzioni difensive nei confronti degli organi di giustizia penale. La mancata somministrazione dell'avvertimento dovrebbe pertanto comportare la inutilizzabilità del dato carpito (art. 64 comma 3-*bis* c.p.p.) e, «secondo l'orientamento più rigoroso, di tutti i risultati investigativi ottenuti [...] a seguito della violazione del divieto»⁵⁶.

Non potrebbe in senso contrario invocarsi l'art. 66 comma 1 c.p.p., che pone quale eccezione al diritto al silenzio dell'imputato l'esplicitazione delle sue generalità e di «quant'altro [possa] valere a identificarlo», dato che le *password* «più che riguardare l'identità di un soggetto, sembrano finalizzate alla protezione delle informazioni elettroniche trasmesse o conservate [...]»⁵⁷.

decrittazione dei dispositivi informatici e privilegio contro l'autoincriminazione, in *Cass. pen.*, 2022, n. 2, p. 889; I. SFORZA, *Il nemo tenetur se detegere nelle audizioni Consob e Banca d'Italia: uno statuto ancora da costruire*, in *Sistema penale*, 2022, n. 2, p. 100; A. MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici ... e non solo*, cit., p. 737; F. CAJANI, *Le "nuove frontiere" dell'investigazione digitale alla luce della legge n. 48/2008, ovvero: quello che le norme (ancora) non dicono*, in S. ATERNO-F. CAJANI-G. COSTABILE-D. CURTOTTI (a cura di), *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Giappichelli, Torino, 2021, p. 551; L. PARLATO, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, cit., p. 295-296; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 33-34; M. PITTIRUTI, *Digital evidence e procedimento penale*, Giappichelli, Torino, 2017, p. 103; P.P. RIVELLO, *Tecniche scientifiche e processo penale*, in *Cass. pen.*, 2013, n. 4, p. 1718; S. VENTURINI, *Sequestro probatorio e fornitori di servizi telematici*, in L. LUPARIA (a cura di), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Giuffrè, Milano, 2012, p. 133-134; L. MARAFIOTI, *Digital evidence e processo penale*, cit., p. 4515-4516.

In senso parzialmente contrario si veda P. FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, cit., p. 1629, nota 218, secondo cui il problema risiederebbe tutt'al più negli eventuali abusi commessi in fase investigativa, ove la cooperazione dell'interessato venisse coartata di fatto. D'altronde, se «è vero [...] che la collaborazione non può essere imposta, [...] è altrettanto vero che l'avvertimento del diritto al silenzio è garanzia delineata con riferimento agli atti di indagine in cui l'indagato interviene, non per propria scelta, come dichiarante. Appare significativo, d'altro canto, che l'avvertimento in questione non sia previsto per l'ipotesi delle dichiarazioni spontanee rese dall'indagato alla polizia giudiziaria ai sensi dell'ultimo comma dell'art. 350 c.p.p.».

⁵⁶ L. LUPARIA, *Computer crimes e procedimento penale*, cit., p. 159-160.

⁵⁷ S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 34.

Questione ulteriore è la riconducibilità del *nickname* o dell'*avatar* – ossia rispettivamente del nome e dell'immagine con cui l'imputato si presenta e agisce nel *web* – al citato obbligo di identificazione.

La dottrina domestica sul punto pare divisa. Da una parte si è sostenuto che una lettura aggiornata all'evoluzione tecnologica imporrebbe di interpretare estensivamente il dettato dell'art. 66 comma 1 c.p.p., ricomprendendo nell'obbligo ostensivo, accanto alle identità fisica e anagrafica, pura quella "virtuale", costituita da *nickname* e *avatar* (*ivi*, p. 35); dall'altra, si è obiettato che la disposizione in parola, concepita avendo riguardo alla sola identità fisica e anagrafica, dovrebbe essere oggetto di stretta esegesi in quanto norma ec-

La giurisprudenza della Cassazione, dal canto suo, sembra accogliere soluzioni non dissimili. Pur essendosi sinora occupata solo di rado della compatibilità di tali richieste collaborative con il principio del *nemo tenetur*, ha già avuto modo di affermare come il rifiuto di fornire le chiavi di accesso al dispositivo elettronico da parte dell'indagato rappresenti una legittima manifestazione del diritto di difesa⁵⁸. Emblematico pare un recente caso, in cui la rivelazione del codice d'accesso ai documenti celati nel

cezionale. Un diverso esito non potrebbe quindi prescindere dall'intervento del legislatore (così C. CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. bras. de direito processual penal*, 5 (2019), n. 3, p. 1180-1181; infine, vi è chi ha negato recisamente tale possibilità sottolineando come, nel caso di reati commessi tramite mezzi informatici, pretendere il disvelamento del *nickname* o dell'*avatar* equivarrebbe di fatto a costringere l'indagato ad ammettere l'addebito (A. MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici ... e non solo*, cit., p. 736).

La seconda impostazione citata si lascia preferire, poiché maggiormente in linea con gli ordinari canoni interpretativi (art. 14 Preleggi): se il rapporto tra diritto al silenzio e obbligo *ex* art. 66 c.p.p. è un rapporto tra regola ed eccezione, occorre evitare che una lettura largheggiante della disciplina processuale possa comprimere lo *ius tacendi* al di fuori dei casi tassativamente indicati.

Naturalmente, tale conclusione non deve far presumere l'irrelevanza del contributo informativo in parola, che potrà comunque legittimamente venir richiesto dagli inquirenti ai sensi dell'art. 21 disp. att. c.p.p., ossia quando, in occasione del primo atto in cui è presente l'indagato o l'imputato, quest'ultimo viene invitato a rivelare ulteriori informazioni personali, tra cui, per quanto qui interessa, l'esistenza di un "soprannome" o di uno "pseudonimo". Se la disposizione eccezionale di cui all'art. 66 c.p.p. non può essere interpretata fino al punto di comprendere una "identità digitale" non ravvisata (allo stato) dal legislatore, lo stesso non potrebbe dirsi per i due concetti appena menzionati, la cui indeterminatezza anzi ben si attaglierebbe al *nickname* – che a tutti gli effetti è un "altro nome", non anagrafico, con cui l'individuo è conosciuto in una più o meno ampia comunità virtuale. Se si accetta di ricondurre il *nick* alla norma di attuazione, allora anche la richiesta all'indagato di rivelare lo stesso dovrebbe venir preceduta, come ha chiarito di recente la Consulta (Corte cost., 5 giugno 2023, n. 111), dall'avviso circa la facoltà di non rispondere, finendo perciò tutelata dal diritto al silenzio (sul punto pare possibilista A. DEL GIUDICE, *The principle of nemo tenetur se detegere in the age of data*, cit. p. 81-82).

Ad ogni modo, anche qualora si volesse ricondurre il *nickname* alla fattispecie aperta dell'art. 66 c.p.p. (secondo cui l'indagato è tenuto a rivelare, oltre alle generalità, pure «quant'altro può valere a identificarlo»), ciò potrebbe non bastare a ritenere del tutto inoperante il diritto al silenzio. È qui utile infatti richiamare quella visione dottrinale che da tempo auspica l'allargamento dello *ius tacendi* e del mendacio anche alla domanda sulle mere generalità, ove ciò sia imposto da una stretta necessità difensiva, come avverrebbe ad esempio nei casi di sostituzione di persona (art. 494 c.p.) (O. MAZZA, *L'interrogatorio e l'esame dell'imputato nel suo procedimento*, in G. UBERTIS-G.P. VOENA (diretto da), *Trattato di procedura penale*, vol. VII.1, Giuffrè, Milano, 2004, p. 112 ss.).

⁵⁸ Cass., sez. V, 30 maggio 2017, Occhionero, in *C.e.d.*, n. 271412. Nel caso di specie, la Cassazione osserva come i provvedimenti di perquisizione e sequestro avevano sortito effetti limitati proprio per via della condotta impeditiva degli imputati, che erano riusciti a bloccare tempestivamente i propri apparecchi elettronici per poi rifiutarsi, invocando il diritto di difesa, di rivelare le chiavi d'accesso ai medesimi.

cellulare era stata sollecitata dalla polizia a seguito di perquisizione preventiva *ex art.* 103 d.P.R. 9 ottobre 1990, n. 309, la quale aveva portato a rinvenire una certa quantità di droga occultata sulla persona dell'utente⁵⁹. Secondo i giudici supremi, ferma restando la impossibilità di supplire tramite il consenso dell'indagato alla mancanza di una previa autorizzazione o di una convalida successiva dell'atto di indagine da parte dell'autorità giudiziaria, appariva chiaro che, a seguito dell'emersione di indizi di reato, «ogni ulteriore attività di indagine [...] richiede[nte] la collaborazione della persona indagata [avrebbe dovuto venir] espletata dopo la formale comunicazione degli avvisi di tutte le facoltà difensive ad essa spettanti, ivi compresa quella della facoltà di rifiutare tale collaborazione ed il diritto ad essere assistito da un difensore [...]»⁶⁰.

5. Segue. *Chiavi d'accesso biometriche*

Maggiori spazi per la collaborazione coartata potrebbero invece aprirsi nel caso in cui il dispositivo risultasse protetto non dalle tradizionali *password* alfanumeriche, ma da chiavi d'accesso biometriche.

Dinanzi a queste ultime, si è infatti osservato, l'imputato verrebbe in considerazione non quale “organo di prova”, a cui viene richiesto di prestare un contributo attivo alle indagini, bensì come “oggetto di prova”⁶¹, che deve semplicemente soggiacere all'acquisizione conoscitiva, senza che la sua volontà venga in alcun modo sollecitata⁶².

L'argomento è semplice e lineare: a differenza di quanto accade per le *password* alfanumeriche, l'impiego di chiavi biometriche per sbloccare il dispositivo non imporrebbe all'indagato un *facere*, bensì un mero *pati*, il che escluderebbe la possibilità di invocare il diritto al silenzio⁶³. Peraltro, dal momento che si renderebbe necessario esercitare una coazione – modica ma non insignificante – sul titolare (immobilizzarlo temporaneamente; forzarlo ad appoggiare il polpastrello sul rilevatore di impronte digitali; e così via) un simile assetto sarebbe legittimo, in forza dell'art. 13 Cost., soltanto in presenza di una previsione legislativa espressa, al momento as-

⁵⁹ Cass., sez. VI, 20 novembre 2024, Lato, in *DeJure*.

⁶⁰ *Ibidem*.

⁶¹ La distinzione fra imputato quale organo ed oggetto di prova si fa tradizionalmente risalire a E. FLORIAN, *Delle prove penali*, vol. II, Vallardi, Milano, 1924, p. 9.

⁶² F.N. RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'autoincriminazione*, cit., p. 890.

⁶³ *Ibidem*. Nello stesso senso si veda A. DEL GIUDICE, *The principle of nemo tenetur se detegere in the age of data*, cit., 87-89.

sente. L'attività di identificazione dell'indagato a cui procede la polizia giudiziaria ai sensi dell'art. 349 comma 2 c.p.p. – mediante «rilievi dattiloscopici, fotografici e antropometrici nonché altri accertamenti» – non potrebbe infatti essere piegata ad altri fini in via interpretativa⁶⁴.

S'aprirebbe così uno scenario per certi versi paradossale: le *passwords* biometriche, più forti delle controparti tradizionali dal punto di vista tecnico-informatico, risulterebbero più deboli dal punto di vista giuridico.

Questa visione, per quanto plausibile, non può dirsi pacifica. Diversi sono in effetti gli argomenti addotti in senso contrario.

È stata innanzi tutto prospettata una violazione del principio di uguaglianza (art. 3 Cost.), dal momento che pare irragionevole discriminare il livello di tutela del *nemo tenetur* in relazione alle diverse tipologie di chiave di accesso al dispositivo, visto che *passwords* biometriche e alfanumeriche svolgono la stessa funzione, e che in entrambi i casi la rivelazione del dato integra l'antecedente necessario della ricerca della prova a proprio danno⁶⁵; inoltre, la stessa qualifica dei dati biometrici quali elementi esistenti indipendentemente dalla volontà del prevenuto è stata messa in discussione, poiché gli stessi, «a differenza del campione sanguineo, sono stati “creati” *ad hoc* proprio da quest'ultimo, con il fine di proteggere informazioni a carattere riservato»⁶⁶. Per l'effetto, non dovrebbe esserci una differenza di tutela per ciò che concerne il *nemo tenetur* fra *passwords* biometriche e alfanumeriche⁶⁷.

Entrambe le tesi indicate colgono qualche aspetto; forse, però, la verità sta nel mezzo.

La prima impostazione va infatti in parte rimeditata alla luce dell'ampiezza del diritto di difesa *ex* art. 24 comma 2 Cost., e in particolare del suo corollario, il principio *nemo tenetur se detegere*, la cui portata non può esser confinata alla sola dimensione dichiarativa (lo *ius tacendi* in senso stretto), ma deve includere anche il diritto di rifiutare una collaborazione attiva alla ricostruzione del fatto storico⁶⁸. Se infatti il dettato codicistico

⁶⁴ A. MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici ... e non solo*, cit., p. 739.

⁶⁵ A. MALACARNE, *Social network e giustizia penale. Nuovi scenari investigativi e probatori*, Tesi di dottorato, Università degli Studi di Genova, 2024, p. 232, iris.unige.it/retrieve/d1775cdc-8644-4d1f-9856-eda125205dd4/pbdunige_4969484.pdf.

⁶⁶ *Ibidem*.

⁶⁷ A favore dell'irrelevanza fra le distinzioni tra tipi di chiavi sembra porsi anche A. MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici ... e non solo*, cit., p. 740.

⁶⁸ A. CAMON, *La disciplina costituzionale*, in AA.VV. *Fondamenti di Procedura penale*, 4^a ed.,

richiama solo la mancata risposta alle domande dell'autorità inquirente (art. 64 comma 3 lett. *b* c.p.p.), la disciplina costituzionale – a mente della quale la difesa è “inviolabile in ogni stato e grado del procedimento” – permette invece di individuare un più vasto «diritto di “resistenza”»⁶⁹ che sorregge sia il contegno silenzioso, sia la facoltà di astenersi dal compiere quei movimenti corporei imposti dall'attività istruttoria (ad es., indossare vestiti o adottare una certa posa a fini ricognitivi, fornire al perito un campione vocale o un saggio grafico, etc.)⁷⁰.

Per quanto qui interessa, quindi, se la garanzia contro l'autoincriminazione esclude l'esistenza di un dovere in capo al prevenuto di fornire prove a proprio carico, siano esse materiali o dichiarative, pare doveroso rileggere il concetto di collaborazione alla luce degli influssi che scienza e tecnica esercitano sull'accertamento penale, attesa la sempre maggiore capacità degli inquirenti di “interrogare” il corpo, prima ancora che l'intelletto⁷¹. In questi casi, infatti, la persona sottoposta ad indagini viene in rilievo quale «fonte di dati», prima ancora che di dichiarazioni⁷².

In altre parole, ciò che consente di determinare il livello di protezione del *nemo tenetur* non dovrebbe esser tanto la natura della *password* (alfanumerica o biometrica), quanto piuttosto il tipo di condotta richiesta per mettere quest'ultima a disposizione degli inquirenti (attiva o passiva). Le chiavi d'accesso biometriche non dovrebbero quindi essere per ciò solo ricondotte allo schema dell'imputato quale “oggetto di prova”, poiché ciò dipenderebbe essenzialmente dal contegno domandato. Qualora sia l'inserimento della *password* a richiedere un *facere*, il prevenuto diverrà soggetto di prova pure quando la chiave sia costituita da una parte del suo

Giuffrè, Milano, 2023, p. 150. Nello stesso senso R. DEL MONACO, *L'accertamento dei reati di guida in stato di ebbrezza e alterazione da droghe*, Tesi di dottorato, Alma Mater Studiorum - Università di Bologna, 2012, p. 61, amsdottorato.unibo.it/4510/1/del_monaco_roberta_tesi.pdf; più di recente, in tema di accertamenti medici coattivi, l'orientamento viene citato anche da P. SPAGNOLO, *Gli accertamenti medici coattivi e le tecniche corporali intrusive*, in *Cass. pen.*, 2024, n. 1, p. 25.

⁶⁹ A. CAMON, *La disciplina costituzionale*, cit., p. 150.

⁷⁰ *Ibidem*. Si vedano, per un simile approccio, anche M. BIRAL, *L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Riv. it. dir. proc. pen.*, 2015, n. 4, p. 1872-1873; P. FELICIONI, *Accertamenti sulla persona e processo penale*, IPSOA, Assago (MI), 2007, p. 35; M. SCAPARONE, *Elementi di procedura penale. I principi costituzionali*, Giuffrè, Milano, 1999, p. 123.

⁷¹ S. RODOTÀ, *Ipotesi sul corpo «giuridificato»*, in *Tecnologie e diritti*, Il Mulino, Bologna, 1995, p. 204, secondo cui la dimensione corporea, elevata ad «oggetto giuridico nuovo», imporrebbe il riconoscimento al titolare di diritti volti a tutelarla dalle intromissioni dell'autorità; M. GIALUZ, *Radiologia e accertamenti medici coattivi: il difficile equilibrio tra libertà della persona ed esigenze di prova*, in *Riv. it. dir. proc. pen.*, 2012, n. 2, p. 559 ss.

⁷² M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisprudenza penale, intelligenza artificiale ed etica del giudizio*, Giuffrè, Milano, 2021, p. 57.

corpo o da un suo tratto fisionomico (es. campione vocale, compimento di specifici gesti)⁷³; al contrario, la valorizzazione di tratti puramente esteriori, osservabili ad occhio nudo, non esigerà alcuna postura attiva dall'imputato, che sarà chiamato solo ad un *patti* del tutto compatibile con il *nemo tenetur* (si pensi al caso della scansione facciale o della retina, o all'impiego della funzione *TouchID*)⁷⁴.

La seconda impostazione, a sua volta, intuisce in maniera condivisibile una comunanza di scopo fra le diverse possibili tipologie di accesso al dispositivo protetto. Tuttavia, gli argomenti suggeriti non paiono insuperabili. Se è vero che ragioni di giustizia sostanziale rendono eccentrica una distinzione fra livelli di tutela basata sul tipo di chiave di sicurezza impiegata (e magari configurata *by design* nel dispositivo), tale scelta potrebbe non essere del tutto irragionevole, atteso che la stessa situazione ha modo di verificarsi rispetto alle *password* alfanumeriche. Queste ultime, infatti, restano incoercibili finché esistono nella mente dell'imputato; una volta tradotte nel mondo esterno, possono invece essere oggetto di apprensione unilaterale da parte degli inquirenti come prove documentali (si pensi al codice di accesso che l'imputato lascia incautamente scritto nella propria agenda poi sequestrata). In un certo senso, dunque, il prevenuto che, per scelta o per negligenza, utilizza un dato biometrico come chiave di sblocco del proprio dispositivo, accetta che quest'ultima esista all'infuori di lui, e che possa perciò venir raccolta indipendentemente dalla sua volontà.

È chiaro poi che la natura *will-dependent* o meno di un certo elemento di prova, in questo caso la chiave, vada esaminata avendo riguardo alla richiesta di cooperazione, non già alla sua origine: a ragionar diversamente, pure ogni documento formato dall'imputato dovrebbe dirsi, per ciò solo, coperto dal diritto al silenzio.

Ancora una volta, dunque, l'attenzione si sposta sul comportamento richiesto all'imputato, più che sulla natura della chiave impiegata. In breve, le matrici biometriche dovrebbero poter vantare un livello di protezione

⁷³ Cfr., con riguardo a quest'ultima eventualità, il metodo di autenticazione basato sul movimento del braccio proposto per gli *smartwatches* da Y. ZHAO-R. GAO-H. TU, *Smartwatch User Authentication Based on the Arm-Raising Gesture*, in *Interacting with Computers*, 32 (2020), p. 569 ss.

⁷⁴ Quest'ultima matrice biometrica, a ben vedere, potrebbe astrattamente rientrare anche nella prima categoria, ove fossero gli inquirenti a richiedere al prevenuto di sbloccare il *device* tramite l'impronta digitale. La distinzione pare pressoché scolastica, nel senso che, in concreto, nessuna difficoltà avrà la polizia giudiziaria ad applicare quella modica forza necessaria a porre il polpastrello dell'utente a contatto col *display*; tuttavia, sul piano dogmatico, è bene non tralasciare questa eventualità.

uguale a quello delle *password* tradizionali ove gli inquirenti non possano ottenerle senza l'attiva cooperazione dell'imputato. In caso contrario, essendo richiesto un contegno puramente passivo, il *nemo tenetur* non dovrebbe poter operare.

6. *Obblighi di decrittazione e di produzione*

Occorre a questo punto chiedersi se fra i due estremi sopra considerati, ossia fra la richiesta di rivelare una *password* alfanumerica e l'obbligo di "sopportare" l'utilizzo di una chiave biometrica, non si possa scorgere una terza via, in cui la richiesta investigativa cada su qualcosa di diverso rispetto al codice di protezione: vale a dire, sull'accesso diretto al dispositivo o sulla consegna del suo contenuto⁷⁵.

In entrambi i casi infatti la *password*, sia essa alfanumerica o biometrica, rimarrebbe impregiudicata e nella disponibilità esclusiva dell'utente; nondimeno, l'autorità penale riuscirebbe ad ottenere ciò che vuole mediante la cooperazione del prevenuto.

In altre parole, occorre domandarsi se siano compatibili con il *nemo tenetur* ordini di decrittazione o di produzione.

Gli ordinamenti che tendono a circoscrivere al diritto al silenzio il problema della collaborazione con l'autorità si mostrano, al riguardo, possibilisti. In tali ipotesi non verrebbe in effetti domandato alla persona sottoposta ad indagine di rivelare il contenuto della propria mente, non intaccandosi quindi il "nucleo duro" (dichiarativo) dello *ius tacendi*.

Si potrebbe perciò sostenere che la decrittazione di un dispositivo riesca a comunicare un unico fatto, cioè la conoscenza della *password*⁷⁶. Per l'effetto, ulteriori inferenze, quali il controllo esercitato sul dispositivo o il possesso dei *files* in esso conservati, costituirebbero semplici deduzioni, in quanto tali prive di valore testimoniale⁷⁷.

⁷⁵ Doveri di tal genere si stanno facendo strada in territori limitrofi al processo penale. È il caso dell'ispezione, prevista a fini identificativi, dei dispositivi o dei supporti elettronici o digitali in possesso dei migranti. L'art. 12 d.l. 11 ottobre 2024, n. 145, convertito con legge 9 dicembre 2024, n. 187, ha infatti previsto, sia per il richiedente asilo che per il migrante irregolare, così come per colui che richiede la protezione internazionale, un «obbligo di cooperare ai fini dell'accertamento dell'identità e di esibire o produrre gli elementi in suo possesso relativi all'età, all'identità e alla cittadinanza, nonché ai Paesi in cui ha soggiornato o è transitato [...]», che comprende, «quando è necessario per acquisire i predetti elementi, l'accesso ai dispositivi o supporti elettronici o digitali in suo possesso».

⁷⁶ O.S. KERR, *Compelled Decryption and the Privilege against Self-Incrimination*, in *Tex. L. Rev.*, 97 (2019), p. 779.

⁷⁷ *Ivi*, p. 780.

Tale impostazione non è però pacifica, e viene contrastata rilevando come la conoscenza del codice non sarebbe l'unico fatto rivelato dall'apertura del dispositivo⁷⁸. L'impiego di un codice comunicherebbe infatti anche che il *device* probabilmente appartiene alla persona a cui lo sblocco è stato richiesto, e che la medesima, consapevolmente o meno, possiede i *files* ivi conservati⁷⁹ – informazioni la cui pregnanza sarà suscettibile di esser apprezzata in concreto dal giudice.

Soprattutto, l'approccio nordamericano rischia di mostrarsi debole in quanto potenzialmente esposto allo stesso limite a cui la giurisprudenza d'oltreoceano assoggetta la protezione del Quinto Emendamento, ossia alla già citata *foregone conclusion doctrine*⁸⁰. Se l'ottemperanza all'ordine conoscitivo poco o nulla aggiunge alle informazioni a disposizione dell'autorità procedente, si argomenta, il privilegio contro l'autoincriminazione non dovrebbe poter venire opposto, in quanto l'attività di ricerca della prova raggiungerebbe un esito, per l'appunto, "scontato"⁸¹.

Occorre perciò domandarsi se una simile eccezione sia ravvisabile nell'ordinamento domestico. Un inaspettato avallo potrebbe provenire dall'interpretazione offerta dalla Corte europea dei diritti dell'uomo nel recente caso *De Legé c. Paesi Bassi*⁸², in cui i giudici strasburghesi hanno affermato che non viola il diritto all'equo processo, nel suo corollario del diritto a non autoincriminarsi, l'obbligo imposto all'interessato di fornire documenti a pena d'una sanzione tributaria – "punitiva" secondo i criteri *Engel* – «where the authorities are able to show that the compulsion is aimed at obtaining specific pre-existing documents – thus, documents that have not been created as a result of the very compulsion for the purpose of the criminal proceedings – which documents are relevant for the investigation in question and of whose existence those authorities are aware»⁸³.

È chiaro, dunque, il parallelismo con la citata teoria statunitense⁸⁴:

⁷⁸ L. SACHAROFF, *What Am I Really Saying When I Open My Smartphone?: A Response to Professor Kerr*, in *Tex. L. Rev.*, 97 (2019), p. 67.

⁷⁹ *Ibidem*.

⁸⁰ Cfr. *supra*, § 3.

⁸¹ Naturalmente la richiesta dovrebbe venir diversamente articolata nel caso in cui venga domandata l'apertura del dispositivo e nel caso in cui venga chiesta la produzione di elementi in esso contenuti. Nella prima ipotesi, infatti, basterebbe dimostrare la conoscenza della *password* da parte del prevenuto; nella seconda, invece, occorrerebbe descrivere specificamente le prove cercate. Cfr. O.S. KERR, *Compelled Decryption and the Privilege against Self-Incrimination*, cit., 786-787.

⁸² Corte e.d.u., 4 ottobre 2022, *De Legé c. Paesi Bassi*.

⁸³ *Ivi*, § 76.

⁸⁴ Come osservato da J. ESCOBAR VEAS, *De Legé v. the Netherlands: The ECtHR*

quando gli inquirenti sono in grado di indicare specificamente di quali prove reali sono alla ricerca, il diritto al silenzio non opera.

Si potrebbe perciò ammettere nel nostro ordinamento un'eccezione basata sulla regola *De Legé*, tale per cui l'indagato possa essere costretto, a certe condizioni, a consegnare dati contenuti nel suo dispositivo elettronico, ovvero a sbloccare il dispositivo?

Al riguardo si possono avanzare alcune perplessità.

Innanzitutto, l'interpretazione formulata dai giudici alsaziani sembra lacunosa, in quanto non spiega perché il grado di conoscenza che l'autorità possiede riguardo una specifica prova dovrebbe rilevare nel determinare se l'imputato sia stato o meno illegittimamente costretto a contribuire alla propria condanna⁸⁵. In particolare, non viene specificato quale sia lo *standard* di giudizio che l'autorità dovrebbe rispettare per potersi dire effettivamente a conoscenza dell'esistenza delle prove reali⁸⁶, né quale sia la logica in grado di sorreggere quest'esegesi⁸⁷. Al contrario, se è vero che il diritto all'autoincriminazione è legato alla presunzione d'innocenza, nel senso che l'accusa dovrebbe riuscire a dimostrare il suo caso senza ricorrere a evidenze ottenute mediante coercizione, come pacificamente affermato nella giurisprudenza della Corte di Strasburgo, allora non dovrebbe esservi spazio alcuno per la regola *De Legé*: in effetti, indipendentemente dal fatto che sia stata o meno consapevole della loro esistenza, ogni volta che l'autorità pubblica costringe l'imputato a produrre attivamente prove reali altro non fa che renderlo partecipe della costruzione dell'accusa nei propri confronti⁸⁸.

D'altronde, anche volendo ammettere la correttezza dell'interpretazione seguita dalla Corte europea, dubbi permarrebbero circa la sua effettiva applicabilità nell'ordinamento italiano. Le garanzie previste dalla Convenzione e.d.u. sono infatti cautele minime, che non ostacolano l'introduzione di un maggior livello di tutela ad opera degli Stati Parte: se il diritto

adopts a line of reasoning similar to that of the United States Supreme Court on compelled production of real or physical evidence, in *Maastricht Journal of European and Comparative Law*, 30 (2023), p. 653 ss.

⁸⁵ *Ibidem*.

⁸⁶ *Ibidem*.

⁸⁷ *Ibidem*. L'Autore sottolinea in particolare come, a differenza del Quinto Emendamento della Costituzione degli Stati Uniti, che circoscrive la sua portata ad un diritto a non essere costretti a testimoniare contro sé stessi, l'art. 6 CEDU non prevede esplicitamente alcuna limitazione di tal genere, né la Corte europea si è mai espressa apertamente in favore di una simile opzione. Una teoria come la *foregone conclusion* assume perciò senz'altro significato ove la protezione offerta dal *nemo tenetur* coincida con il contenuto comunicativo dell'atto; ove si scinda questa endiadi, invece, tale teoria può apparire priva di una *ratio* giustificatrice.

⁸⁸ *Ibidem*.

a non collaborare è da considerare un corollario del diritto di difesa costituzionalmente riconosciuto all'imputato, allora il nostro sistema penale pare già ammettere, su questo punto, un livello di protezione superiore rispetto ai minimi *standard* convenzionali. Inoltre, la Consulta, pur confermando di non poter sindacare l'interpretazione offerta dalla Corte di Strasburgo, ha da tempo asserito che l'esegesi convenzionale diviene vincolante per il giudice comune, al fine di precisare e specificare il contenuto della norma pattizia, solo quando risulti indice d'un "diritto consolidato"⁸⁹.

Elementi idonei ad orientare il magistrato penale in questa valutazione sarebbero, per quanto qui interessa, «la creatività del principio affermato, rispetto al solco tradizionale della giurisprudenza europea» e «la circostanza che quanto deciso proman[*i*] da una sezione semplice, e non [abbia] ricevuto l'avallo della Grande camera»⁹⁰. La sentenza *De Legé* parrebbe rispondere ad entrambi i criteri proposti, essendo stata pronunciata da una sezione semplice, la Quarta, e presentando profili innovativi: la situazione di "*fishing expedition*" infatti, nonostante qualche opinione favorevole in dottrina⁹¹, mai era stata additata in via esplicita dalla Corte e.d.u. quale presupposto necessario a legittimare la mancata consegna di prove reali da parte dell'accusato⁹².

Relativizzata così la portata del precedente, ci si sente di concludere negativamente circa la applicabilità di una "eccezione di conoscenza" in ordine alla possibilità di avvalersi del *nemo tenetur* nel processo penale tradizionale⁹³.

⁸⁹ Corte cost., 26 marzo 2015, n. 49, punto 7 del *Considerato in diritto*.

⁹⁰ *Ibidem*.

⁹¹ In questo senso, ad esempio, G. STESENS, *The obligation to produce documents versus the privilege against self-incrimination: human rights protection extended too far?*, in *European Law Review - Checklist no. 1*, 22 (1997), p. 61, che tenta di riconciliare così i contrastanti precedenti *Funke* e *Saunders*.

⁹² Alcune decisioni, in cui le richieste dell'autorità pubblica erano state ritenute lesive del *nemo tenetur*, sembravano in effetti alludere ad un tale contesto di incertezza, senza però indicarlo testualmente come unico o principale criterio risolutivo. Cfr. es. Corte e.d.u., *Funke* c. Francia, cit., § 44; Corte e.d.u., J.B. c. Svizzera, cit., § 69.

⁹³ Una soluzione diversa potrebbe valere per il procedimento amministrativo "punitivo", ossia "penale" nell'ottica della giurisprudenza di Strasburgo. Qui la facoltà di tacere si porrebbe come eccezione alla regola, altrimenti generale, di cooperazione con autorità amministrative indipendenti, comportando perciò un effettivo innalzamento di tutela.

7. Collaborazione “spontanea” e valutazione del “silenzio”

Ad un diverso esito rispetto alle ricostruzioni offerte fin qui si deve giungere ove il prevenuto si determini spontaneamente a rivelare la *passsword* o ad immetterla lui stesso, trattandosi di una forma di abdicazione al diritto a non collaborare⁹⁴. Il problema che qui si pone, piuttosto, è quello di verificare l'effettiva assenza di costrizioni o di pressioni indebite, visto l'incerto confine di un'effettiva spontaneità⁹⁵.

Il tema non è puramente teorico, dato che il ricorso a forme oblique di “*moral suasion*” ben può rappresentare un utile viatico per persuadere l'indagato a dismettere il proprio diritto senza che l'attività investigativa vada incontro ad alcuna formale sanzione⁹⁶. Il comportamento collaborativo, se non può essere imposto dagli inquirenti, può infatti esser oggetto di una larvata “negoziiazione” volta, nell'ottica dell'imputato, a conseguire vantaggi (o ad evitare mali) e, nell'ottica dell'organo dell'indagine, a prevenire diseconomie processuali.

In primo luogo, l'interesse perseguito dal soggetto passivo dell'accertamento penale potrebbe essere quello di evitare il rischio di alterazione dei dati contenuti nel dispositivo – non escludibile a priori in caso di accesso *brute force* –, o, ancora, il desiderio di conseguire una pronta restituzione del bene oggetto di sequestro⁹⁷. È facile perciò immaginare come i codici di accesso potrebbero venir rivelati, o lo sblocco del *device* venir eseguito, proprio al fine di favorire i predetti esiti.

Questo stato di cose sembra trovare una implicita conferma nella giurisprudenza di legittimità, la quale, pur riconducendo la mancata collaborazione dell'indagato nel rilascio dei codici di accesso all'esercizio di una facoltà difensiva – ossia, al “diritto al silenzio” –, ha già avuto modo di specificare che «si tratta [...] di comportamento che influisce sulla valutazione della legittimità della protrazione del vincolo, che trova giustificazione nella accresciuta difficoltà di accesso ai dati di interesse investigativo»⁹⁸. In altre parole, se è vero che nell'ambito del sequestro probatorio di dispositivi informatici – prodromico ad identificare ed estrarre i dati rilevanti per le in-

⁹⁴ A. MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici ... e non solo*, cit., p. 737.

⁹⁵ *Ibidem*.

⁹⁶ F.N. RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'autoincriminação*, cit., p. 889.

⁹⁷ A. ZAMPINI, intervento alla conferenza *Dimensione giudiziaria e dimensione mediatica della presunzione d'innocenza*, cit.

⁹⁸ Cass., Sez. II, 23 marzo 2023, Casale, in *C.e.d.*, n. 284393 – 01. Più di recente, nello stesso senso, si veda Cass., Sez. III, 4 luglio 2024, Ferrero, in *C.e.d.*, n. 286923 – 01.

dagini – la finalizzazione dell’ablazione alla successiva analisi implica che la protrazione del vincolo (nel rispetto dei principi di proporzionalità e di adeguatezza) debba essere limitata al tempo necessario all’espletamento delle operazioni tecniche, la ragionevolezza della durata dovrà esser valutata in rapporto alle difficoltà tecniche di apprensione dei dati, le quali debbono ritenersi aumentate ove l’indagato non cooperi fornendo le chiavi di accesso alle banche dati contenute nei supporti sequestrati⁹⁹.

Non meno insidioso pare poi l’effetto che, *a latere* o prima del giudizio di cognizione, può avere l’inerzia dell’imputato nel rivelare le proprie *passwords*. Il procedimento cautelare rappresenta infatti uno snodo delicato per ciò che concerne la tutela del *nemo tenetur*, essendo facilmente impieghabile da parte del pubblico ministero per sollecitare la collaborazione materiale o la confessione del prevenuto, “scambiandole” con una domanda di revoca o di attenuazione della misura¹⁰⁰.

Proprio al fine di scongiurare tali pratiche, la legge esclude testualmente che il silenzio e la mancata ammissione degli addebiti possano rientrare nel novero delle situazioni da cui dedurre l’esistenza di un pericolo per l’acquisizione e la genuinità della prova (*ex* art. 274 comma 1 lett. a, c.p.p.)¹⁰¹. Eppure, in senso contrario si è in anni recenti pronunciata la Suprema Corte, arrivando a desumere tale rischio di inquinamento proprio dal rifiuto dell’indagato di fornire le chiavi di accesso ai dispositivi informatici a lui sequestrati¹⁰². Il pericolo ravvisato è stato evidentemente quello di una cancellazione a distanza dei dati da parte del prevenuto non ristretto; seguendo quest’esegesi, un esito favorevole della vicenda cautelare ben potrebbe rappresentare il “premio” offerto a colui che rivela le *passwords* dei sistemi controllati. La soluzione appare tuttavia censurabile, perché il diritto a tacere, anche nella sua appendice elettronica, non dovrebbe costituire di per sé un elemento idoneo a giustificare la compressione della libertà individuale, pena l’elusione dello specifico divieto posto dal legislatore¹⁰³.

In quest’ottica, un approccio incoraggiante si rinviene in tema di ripa-

⁹⁹ *Ibidem*.

¹⁰⁰ Cfr. es. G. ILLUMINATI, *Carcere e custodia cautelare*, in *Cass. pen.*, 2012, n. 7-8, p. 2373.

¹⁰¹ La scelta di limitare tale divieto ad uno solo dei *pericula libertatis* è stata peraltro oggetto di critiche in dottrina poiché, letta al contrario, tale clausola rischia di legittimare l’inferenza censurata in relazione alle altre esigenze cautelari. Cfr. es. G. GIOSTRA, *Per una migliore disciplina della custodia cautelare*, in *Dir. pen. proc.*, 1995, n. 3, p. 305.

¹⁰² Cass., Sez. II, 26 febbraio 2021, M.M., in *Diritto di internet*, 12 marzo 2021, con nota di M. PITTIRUTI, *Rifiuto di fornire i codici di sblocco della strumentazione informatica in sequestro e pericolo di inquinamento probatorio: addio al nemo tenetur se detegere?*.

¹⁰³ M. PITTIRUTI, *Rifiuto di fornire i codici di sblocco*, cit., il quale sottolinea che tale pratica risulterebbe evidentemente propedeutica a fungere da pungolo per la collaborazione.

razione per la ingiusta detenzione subita dall'imputato, ove si è escluso che la mancata indicazione alla polizia giudiziaria dei codici di accesso al cellulare possa risultare ostativa al rimedio (art. 314 comma 1 c.p.p., così come modificato dal d.lgs. 8 novembre 2021, n. 188), stante la riconducibilità di tale comportamento, in senso lato, all'alveo del diritto al silenzio¹⁰⁴.

In ultimo, non può tacersi il rischio che il sindacato sul contegno non collaborativo possa penetrare anche sul piano decisionale. Come tradizionalmente sottolineato, il comportamento meramente passivo rappresenta di per sé un dato neutro sul piano probatorio¹⁰⁵; tuttavia, scorrendo il diritto vivente ci si accorge che la possibilità di trarre inferenze negative o positive – rispettivamente dall'esercizio o dal mancato esercizio dello *ius tacendi* – fatica a scomparire.

La mancata cooperazione, infatti, pur non potendo portare ad una inversione dell'onere della prova¹⁰⁶, viene talvolta valorizzata quale “argomento”¹⁰⁷ o “elemento” probatorio¹⁰⁸: ciò, ad esempio, al fine di corroborare ulteriori evidenze¹⁰⁹, o per decidere tra la concessione o il diniego di circostanze attenuanti (specie generiche)¹¹⁰, ovvero in sede di applicazione dei “doppi benefici” (sospensione condizionale della pena e non menzione della condanna nel certificato del casellario giudiziale)¹¹¹.

In dottrina, nonostante l'opinione contraria di buona parte degli studiosi, secondo cui consentire al giudice di trarre inferenze negative dal silenzio equivarrebbe a sanzionare l'esercizio di un diritto costituzionalmente tutelato¹¹², vi è chi assume una posizione più blanda, ammettendo quella indiretta valutazione “negativa” del silenzio nel momento in cui il

¹⁰⁴ Cass., Sez. IV, 14 marzo 2023, I.A.C.S., in *DeJure*.

¹⁰⁵ Per tutti si veda F. CORDERO, *Procedura penale*, 9ª edizione, Milano, 2012, p. 255.

¹⁰⁶ Cfr., *ex multis*, Cass., Sez. III, 19 settembre 2019, C.F., in *DeJure*.

¹⁰⁷ Cfr., *ex multis*, Cass., Sez. II, 12 febbraio 2020, P.M., in *DeJure*.

¹⁰⁸ Cfr., *ex multis*, Cass., Sez. IV, 6 novembre 2019, Ascone, in *C.e.d.*, n. 279246 – 02; in senso contrario Cass., Sez. VI, 27 gennaio 2015, Scarpa, in *C.e.d.*, n. 262499 – 01.

¹⁰⁹ Cass., Sez. VI, 19 giugno 2019, Arena, in *C.e.d.*, n. 276381 – 01.

¹¹⁰ Cass., Sez. Un., 24 maggio 2012, P.G., in *C.e.d.*, n. 253152 – 01. In senso parzialmente contrario, si vedano invece Cass., Sez. V, 24 settembre 2020, Barzaghi, in *C.e.d.*, n. 279778 – 01; Cass., Sez. VI, 17 ottobre 2013, Faga, in *C.e.d.*, n. 256963 – 01.

¹¹¹ Cass., Sez. VI, 16 febbraio 1984, Rampuglia, in *C.e.d.*, n. 164489 – 01. La giurisprudenza di legittimità sembra però ormai tendere ad allinearsi alla protezione del *nemo tenetur* su questo punto. Cfr. Cass., Sez. III, 25 novembre 2015, Tonti Donaggio, in *C.e.d.*, n. 265713 – 01, per quanto riguarda la sospensione condizionale, e Cass., Sez. V, 14 settembre 2017, G.M., in *DeJure*, con riferimento alla non menzione della condanna.

¹¹² In questo senso ad es. V. PATANÈ, *Il diritto al silenzio dell'imputato*, Giappichelli, Torino, 2006, p. 214 ss.; G. STANZIONE, *Autoincriminazione e diritto al silenzio. Le esperienze italiana, francese e inglese*, Wolters Kluwer-Cedam, Assago (MI), 2017, p. 114; M. NOBILI, *Il principio del libero convincimento del giudice*, Giuffrè, Milano, 1974, p. 346, 352.

giudice si trova ad escludere ipotesi alternative, attività necessaria per rispettare lo *standard* dell’“oltre ogni ragionevole dubbio”¹¹³, ovvero distinguendo tale ipotesi dalla valutazione positiva della condotta di collaborazione – la quale, si afferma, non entrerebbe in attrito con il *nemo tenetur*¹¹⁴.

Non constano precedenti specifici in materia per quanto riguarda il sindacato sul diritto al silenzio “digitale” ai fini della decisione di merito: non può tuttavia escludersi che simili ragionamenti possano venir riproposti, *mutatis mutandis*, anche in tale nuovo ambito applicativo¹¹⁵.

L’idea di valorizzare negativamente la mancata rivelazione della *password*, o il suo mancato inserimento, non sarebbe tuttavia appropriata, in quanto finirebbe per degradare la situazione giuridica soggettiva in parola da diritto ad onere.

Si potrebbe forse essere più “laici” per quanto riguarda la introduzione di un’ipotesi premiale. Questa potrebbe assumere la forma di una mitigazione della pena, da riconoscere nelle vesti di un’attenuante in caso di condanna dell’imputato che abbia effettivamente favorito l’accertamento del reato mediante lo sblocco del dispositivo sotto il suo controllo – sulla scorta di quanto già avviene in relazione ad altre fattispecie delinquenziali (es. 323-*bis* comma 2 c.p.)¹¹⁶; oppure in via interpretativa, facendo rientrare un simile comportamento nell’ambito delle c.d. attenuanti generiche (art. 62-*bis* c.p.). Tale ipotesi si porrebbe peraltro in linea con quanto previsto dalla Direttiva 343/2016/UE, secondo cui, sebbene «l’esercizio da

¹¹³ L. CARBONI, *La valutazione probatoria del silenzio: critiche e prospettive*, in *Proc. pen. giust.*, 2018, n. 5, p. 922 ss.; S. SOTTANI, voce *Silenzio (diritto al)*, in *Dig. disc. pen.*, VII aggiornamento, Utet, Torino, 2013, p. 558-559.

¹¹⁴ C. BONZANO, *L’interrogatorio investigativo*, Cedam, Padova, 2012, p. 31.

¹¹⁵ In Cass., Sez. I, 2 novembre 2023, Ni.Gi., in *DeJure*, il ricorrente ha avuto modo di lamentare, *inter alia*, la violazione di legge e il vizio di motivazione in ordine al trattamento sanzionatorio ricevuto, dal momento che i giudici d’appello avrebbero negato l’applicabilità delle circostanze attenuanti generiche in base al rifiuto di rivelare la *password* del proprio *smartphone* sottoposto a sequestro, valorizzandolo quale comportamento reticente. La Corte di legittimità non ha affrontato direttamente la questione, ritenendo piuttosto che la sentenza impugnata avesse argomentato la mancata concessione delle attenuanti ex art. 62-*bis* c.p. considerando sia la gravità delle condotte che l’intensità del dolo, essendo pacifico l’orientamento secondo cui, al fine di ritenere o escludere tali circostanze, il giudice potrebbe limitarsi a prendere in esame, tra gli elementi desumibili dall’art. 133 c. p., solo «quello che ritiene prevalente ed atto a determinare o meno il riconoscimento del beneficio, sicché anche un solo elemento attinente alla personalità del colpevole o all’entità del reato ed alle modalità di esecuzione di esso può risultare a tal fine sufficiente».

¹¹⁶ Art. 323-*bis* comma 2 c.p.: «[p]er i delitti previsti dagli articoli 318, 319, 319 ter, 319 quater, 320, 321, 322, 322 bis e 346 bis, per chi si sia efficacemente adoperato per evitare che l’attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l’individuazione degli altri responsabili ovvero per il sequestro delle somme o altre utilità trasferite, la pena è diminuita da un terzo a due terzi».

parte degli indagati e imputati del diritto al silenzio o del diritto di non autoincriminarsi non [possa] essere utilizzato contro di loro» (art. 7 comma 5), sarebbe comunque consentito tenere conto, in sentenza, del loro comportamento collaborativo (art. 7 comma 4).

In realtà, anche questa soluzione, per quanto non incostituzionale e non anti-comunitaria, non va esente da critiche, poiché finisce per dare luogo ad un'ulteriore ipotesi di quella «“soave inquisizione”»¹¹⁷, da tempo lamentata dalla dottrina penalistica, in cui la collaborazione processuale del prevenuto «risult[a] condizionata, in positivo, dalle blandizie del trattamento di favore, e, in negativo, dall'idea che il silenzio possa venire sanzionato da un'eventuale condanna senza “sconti”»¹¹⁸.

Insomma, quando si tratta di diritti fondamentali, quale è il *nemo tenetur*, negare un premio assomiglia molto a prospettare una sanzione¹¹⁹.

8. Cooperazione “fittizia” e attacchi a “forza bruta”

Una lettura lineare del *nemo tenetur* dovrebbe quindi orientare la prassi delle indagini verso altre vie, che non implicino la cooperazione diretta o indiretta dell'accusato¹²⁰. Minori perplessità desta in effetti, per ciò che concerne lo *ius tacendi*, un attacco condotto a forza bruta (*brute force*) nei confronti dell'apparecchio elettronico o realizzato inoculando captatori informatici (in funzione di *keylogger* o per la perquisizione del dispositivo bersaglio). Queste tecniche possono infatti venir eseguite d'autorità, senza coinvolgere l'individuo soggetto ad indagine penale.

Per vero, qualche dubbio potrebbe sorgere pure in questi frangenti. Si pensi alla “auto-installazione” del captatore informatico, ossia al *download* del *malware* inconsapevolmente ma proattivamente effettuato dall'in-

¹¹⁷ T. PADOVANI, *La soave inquisizione. Osservazioni e rilievi a proposito delle nuove ipotesi di “ravvedimento”*, in *Riv. it. dir. proc. pen.*, 1981, n. 2, p. 541.

¹¹⁸ *Ibidem*.

¹¹⁹ Non a caso, tale obiezione è stata sollevata anche in riferimento alla menzionata disciplina euro-unitaria (art. 7 comma 4 Direttiva 343/2016/UE), sottolineando come nel lungo termine una costante valutazione favorevole della rinuncia al silenzio possa finire per rappresentare una sanzione indirettamente rivolta a coloro che invece se ne avvalgono. Così M. CAIANIELLO, *Right To Remain Silent and Not to Incriminate Oneself in the European Union System*, (December 5, 2020), p. 15 del dattiloscritto, ssrn.com/abstract=3743329 o dx.doi.org/10.2139/ssrn.3743329; D. NEGRI, *Diritto al silenzio e verità estorte. Regressioni della storia, reticenze dell'Europa, ipocrisie domestiche*, in L. STORTONI-D. CASTRONUOVO (a cura di), *Nulla è cambiato? Riflessioni sulla tortura*, Bononia University Press, Bologna, 2019, p. 165.

¹²⁰ A. ZAMPINI, intervento alla conferenza *Dimensione giudiziaria e dimensione mediatica della presunzione d'innocenza*, cit.

dagato sul proprio dispositivo elettronico. La questione è stata in effetti posta proprio con riguardo alle captazioni ambientali eseguite tramite un “*trojan horse*”: parte della dottrina ha avuto modo di osservare come la cooperazione artificiosa richiesta al destinatario dell’intercettazione, necessaria per permettere al captatore informatico di “infettare” il dispositivo bersaglio e di controllarne il funzionamento (ad esempio, attivando il microfono), paia confliggere con l’art. 188 c.p.p., il quale vieta, anche con il consenso dell’interessato, l’impiego di metodi o tecniche idonei ad influire sulla sua libertà di autodeterminazione – in ciò distinguendosi dalle intercettazioni ordinarie, in cui sono gli inquirenti a dover piazzare materialmente la “cimice”¹²¹. Per questa via, vi è quindi chi ha affermato che sollecitare in maniera occulta una cooperazione «potenzialmente *contra se*» condurrebbe ad una violazione del *nemo tenetur*, «da intendersi in senso ampio, non solo come diritto a non rendere dichiarazioni autoincriminanti, ma anche come diritto a non compiere azioni» di tal fatta¹²².

Tale approccio va però incontro all’obiezione, difficilmente superabile, secondo cui la captazione così realizzata non implicherebbe alcuna «pressione sulla libertà fisica e morale della persona», non mirando il mezzo d’indagine «a manipolare o forzare un apporto dichiarativo» quanto piuttosto, «nei rigorosi limiti in cui sono consentite le intercettazioni», a captare «le comunicazioni tra terze persone, nella loro genuinità e spontaneità»¹²³. Pur essendo un atto *contra se*, quindi, la mancanza di un contatto diretto con l’autorità procedente pone il *download* del *virus* al di fuori dello spettro applicativo del *nemo tenetur*, rendendo la collaborazione di certo inconsapevole, ma non coartata¹²⁴.

In ciò sta tutta la differenza rispetto alla richiesta della *password*, della

¹²¹ A. CHELO, *Tutela della libertà morale e captatore informatico: è davvero tutto concesso a soddisfazione delle esigenze investigative?*, in *Dir. pen. proc.*, 2022, n. 7, p. 954 ss.; L. FILIPPI, *Il cavallo di troia e l’ispe-perqui-intercettazione*, in *Penale. Diritto e procedura*, 2022, n. 1, p. 69.

¹²² S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 238.

¹²³ Cass., Sez. V, 30 settembre 2020, P.G., con nota di R. APRATI, *Il trojan horse auto-installato non rientra tra i metodi che ledono la libertà morale dell’indagato*, in *Foro it.*, 6 gennaio 2021.

¹²⁴ Si veda ad esempio la posizione scettica di M. MIRAGLIA, *Il “Trojan (non) di Stato”: una disciplina da completare*, in *Proc. pen. giust.*, 2023, n. 5, p. 1232, la quale si domanda se la corrispondente attività svolta nel mondo fisico (nell’esempio «l’apertura della porta di casa ad un falso tecnico del gas che installi cimici tradizionali per eseguire intercettazioni») potrebbe mai andare incontro ad una simile qualificazione. Opinione analoga è espressa da A. CAMON, *Processo e libertà morale: tendenze recenti della giurisprudenza, della dottrina, della legislazione*, in *Proc. pen. giust.*, 2024, n. 4, p. 1029, secondo cui neanche chi assume la veste di indagato o di imputato potrebbe andare esente da incursioni nella propria sfera di autodeterminazione, non dovendo necessariamente «essere gradevoli e genuini» gli stimoli ri-

produzione o della decrittazione, ove la domanda degli inquirenti attiva quel rapporto di immediatezza idoneo ad ingenerare una soggezione psicologica non compatibile con la libertà che deve essere invece lasciata alle scelte auto-difensive.

Ad ogni modo, anche se appare corretto superare i dubbi circa il rispetto del diritto al silenzio, l'accesso *bruteforce* presenta comunque alcune ineliminabili criticità: innanzi tutto il costo delle tecniche di *hacking* impiegate, non trascurabile ove occorra fare ricorso a competenze o sistemi che non siano nella immediata disponibilità dell'autorità giudiziaria¹²⁵; la possibile dilatazione dei tempi investigativi richiesti al fine di bypassare le chiavi di accesso¹²⁶; nonché, come detto, il rischio di compromissione dell'integrità dei dati conservati nel dispositivo¹²⁷.

9. Obbligo di rivelazione della password e privilegio contro l'autoincriminação

Naturalmente, come osservato in dottrina, «il diritto a non collaborare spetta non solo alla persona indagata, ma anche a chi rischia, con il disvelare codici di accesso, di far emergere una sua responsabilità penale (art. 198, comma 2, c.p.p.)»¹²⁸.

Questa disciplina, in apparenza chiara, è però imperfetta, dal momento che il potenziale testimone, non attinto da sospetti di un reato pregresso, pare comunque tenuto a giustificare l'opposizione del privilegio: pertanto, egli non può limitarsi a tacere, ma deve indicare, sia pure in maniera sommaria, le ragioni che permettono di ritenere ragionevole la sua scelta – insomma, come notato da attenta dottrina, al fine di invocare il *privilege against self-incrimination* il teste pare «costretto a... “incriminarsi un poco”»¹²⁹.

Tuttavia, il vero *punctum dolens* che qui interessa è un altro, ossia la natura essenzialmente “comunicativa” della garanzia, che inerisce a una

cevuti nel corso del procedimento; a ragionar diversamente, infatti «nessuno potrebbe dirsi titolare d'una libertà morale piena».

La inoperatività del diritto al silenzio al di fuori di una sollecitazione da parte dell'autorità che procede viene peraltro affermata sin dalla storica Corte cost., 6 aprile 1973, n. 34, punto 3 del *Considerato in diritto*, con nota di V. GREVI, *Insegnamenti, moniti e silenzi della Corte Costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.*, 1973, n. 2, p. 317 ss.

¹²⁵ A. ZAMPINI, intervento alla conferenza *Dimensione giudiziaria e dimensione mediatica della presunzione d'innocenza*, cit.

¹²⁶ *Ibidem*.

¹²⁷ P. TONINI, *L'evoluzione delle categorie tradizionali: il documento informatico*, in A. CADOPPI - S. CANESTRARI - A. MANNA - M. PAPA (diretto da), *Cybercrime*, 2^a ed., cit., p. 1516.

¹²⁸ L. LUPÀRIA, *Computer crimes e procedimento penale*, cit., p. 388.

¹²⁹ A. CAMON, *Le prove*, in AA.VV. *Fondamenti di Procedura penale*, cit., p. 362.

deposizione e non già a una condotta. Tale stato di cose si riverbera sulla inutilizzabilità (relativa) che consegue al rilascio di affermazioni autoindizianti (art. 63 comma 1 c.p.p.), la quale difficilmente, visto il chiaro tenore letterale, potrebbe estendersi agli atti compiuti in seguito all'accesso al dispositivo, ancorché dotati di piena portata incriminante¹³⁰. Inoltre, bisogna considerare che, nella maggior parte dei casi, sarà solo dopo aver esaminato quanto rinvenuto nell'apparecchio che potrà emergere una vera e propria *notitia criminis*, venendo quindi meno quella contestualità tra dichiarazioni e autoincriminazione richiesta dalla norma¹³¹.

Riportando queste considerazioni al caso dei dispositivi elettronici, dunque, la tutela del terzo parrebbe invero piuttosto contenuta: egli potrebbe, invocando il privilegio, rifiutarsi di rivelare la chiave d'accesso; ma il divieto d'impiego processuale potrebbe al limite riguardare la dichiarazione forzosamente rilasciata (ossia il codice), non già gli elementi rinvenuti a seguito della successiva perquisizione del *device*.

Se la tutela dichiarativa pare limitata, ancora più compressa è l'autodifesa del terzo a cui venga imposta una cooperazione di carattere "materiale". Nonostante infatti tra le "persone idonee" (art. 348 comma 4 c.p.p.) e tra i "consulenti" (art. 359 comma 1 c.p.p.) tenuti a prestare la propria opera nel corso di indagini richiedenti specifiche competenze tecniche non possa certo ritenersi incluso il prevenuto¹³², lo stesso non può dirsi per colui che non è interessato dal procedimento. La legge processuale non mostra preclusioni: nel caso degli ausiliari di p.g. è la specifica necessità di volta in volta rilevata il parametro che permette di selezionare il soggetto a cui attribuire la servitù di giustizia¹³³, il quale ben potrà essere così individuato nell'utente del dispositivo; lo stesso dicasi per i consulenti del pubblico ministero, che solo «di regola» dovranno essere iscritti agli albi peritali, mancando qualsivoglia sanzione in caso di scelta difforme (art. 73 disp. att. c.p.p.)¹³⁴. Questi elementi lasciano intendere come una collaborazione non dichiarativa possa potenzialmente venir imposta al soggetto non indagato che utilizzi un dispositivo elettronico, o alla parte terza che abbia comunque conoscenza della modalità di accesso ai dati

¹³⁰ F.N. RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'autoincriminazione*, cit., p. 891.

¹³¹ A. MALACARNE, *Social network e giustizia penale. Nuovi scenari investigativi e probatori*, cit., p. 238.

¹³² M. TORRE, *Sull'obbligo per il privato di collaborare ad attività di digital forensics: il caso "Apple - F.B.I."*, in A. CADOPPI - S. CANESTRARI - A. MANNA - M. PAPA (diretto da), *Cybercrime*, 1^a ed., Utet Giuridica, Milano, 2019, p. 1684.

¹³³ *Ivi*, p. 1683.

¹³⁴ *Ivi*, p. 1684.

ricercati – cooperazione non rifiutabile¹³⁵, pena l'integrazione delle fattispecie di omissione di atti d'ufficio (art. 328 c.p.) o di rifiuto di uffici legalmente dovuti (art. 366 c.p.p.)¹³⁶.

In sostanza, la tutela del privilegio contro l'autoincriminazione sembra, *de iure condito*, piuttosto limitata¹³⁷. Talune garanzie potrebbero però venir delineate in un'ottica *de iure condendo*.

Innanzitutto, per evitare che l'accesso al *device* nasconda un intento meramente esplorativo, ed al fine di contenere il pregiudizio per la riservatezza del terzo, si potrebbe riconoscere espressamente l'inutilizzabilità delle prove estranee al procedimento in cui l'accesso sia stato disposto¹³⁸. Inoltre, l'obbligo collaborativo dovrebbe essere non solo legislativamente previsto, ma anche basarsi su un provvedimento motivato dell'autorità giudiziaria e risultare comunque rispettoso del principio di proporzionalità¹³⁹.

Se ci si limitasse a questo, però, nel caso della condotta collaborativa puramente materiale – rispetto alla quale, come si è detto, non sembra operare alcuna forma di legittima astensione – si rischierebbe comunque di lasciar scoperto il nucleo centrale del *privilege against self-incrimination*, vale a dire il rischio di far emergere una notizia di reato a proprio carico ottemperando all'ordine ricevuto. Perciò, sempre in una prospettiva *de iure condendo*, non sarebbe irragionevole aggiungere un'eccezione a quest'obbl-

¹³⁵ *Ivi*, p. 1685.

¹³⁶ *Ivi*, p. 1683-1684.

¹³⁷ Tale conclusione pare confermata in via implicita dal potere dell'autorità giudiziaria di ordinare l'esibizione di atti, documenti, dati, informazioni e programmi informatici, anche tramite copia su supporto idoneo (art. 256 c.p.p.): il soggetto destinatario è infatti qui obbligato a consegnare immediatamente quanto richiesto, salvo non dichiarare per iscritto che la *res* cercata è coperta dal segreto professionale. Cfr. es. Cass., Sez. II, 18 ottobre 2017, P.B., in *DeJure*.

¹³⁸ F.N. RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'autoincriminazione*, cit., p. 893 ss.

¹³⁹ Quest'ultimo, in particolare, impone che il protocollo di ricerca venga formulato in modo chiaro e che l'accesso sia limitato a dati adeguatamente identificati dall'autorità richiedente e pertinenti ai fatti oggetto dell'indagine, in ossequio ai canoni di idoneità, adeguatezza e proporzione in senso stretto. Cfr. R. ORLANDI, *Postulati del processo penale contemporaneo tra principi "naturali" e concezioni normative*, in *Riv. it. dir. proc. pen.*, 2024, n. 2, p. 482 ss.

Si può discutere in ordine ai parametri su cui basare questo giudizio di proporzionalità. Secondo F.N. RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'autoincriminazione*, cit., p. 894, quanto più specifico sarà l'oggetto dell'investigazione, tanto più intenso dovrà essere il dovere cooperativo. Al contrario, per A. MALACARNE, *Social network e giustizia penale. Nuovi scenari investigativi e probatori*, cit., p. 237-238, l'intensità del dovere di collaborazione dovrebbe dipendere dalla gravità dei reati oggetto d'indagine e dal tipo di dati richiesti, dimodoché l'obbligo di *disclosure* potrebbe tradursi alternativamente nella rivelazione della *password* o di altre chiavi di sicurezza, oppure, ove ciò risultasse sproporzionato, nella ostensione delle prove reali domandate dagli inquirenti.

go, analoga a quella già prevista sul piano dichiarativo: ossia la facoltà di opporre un rifiuto motivato ove le informazioni richieste possano far emergere una responsabilità di tipo penale.

10. Conclusioni

Il rapporto tra dispositivi elettronici e diritto al silenzio può a buon titolo dirsi controverso. La stretta integrazione che l'apparecchio stabilisce fra individuo e sua dimensione virtuale – icasticamente rappresentata dal sempre più frequente impiego del corpo stesso (dati biometrici) in funzione di *password* – attiva un'aspettativa di difesa e di riservatezza che, in assenza di una disciplina apposita, non può che venir soddisfatta ricorrendo ai principi generali.

La distinzione tra condotta attiva e passiva quale chiave di lettura del *nemo tenetur*, la impossibilità di punire il contegno non collaborativo del prevenuto e gli obblighi di cooperazione imponibili a testimoni e terze parti rappresentano le linee guida che ci si sente di avanzare.

D'altronde, non molto dissimili paiono le soluzioni a tal fine escogitate da altri ordinamenti. Piuttosto pacifica e trasversale sembra essere la distinzione tra tipologie di chiavi di sicurezza, con il codice alfanumerico posto al centro del nucleo dichiarativo del diritto al silenzio e la matrice biometrica invece potenzialmente esposta a coercizione, in quanto indipendente dalla volontà dell'utilizzatore. Tuttavia non mancano spinte e contropunte, volte da un lato a escludere dalla protezione anche le *passwords* tradizionali (es. Belgio, Francia), dall'altro a recuperare qualche margine di tutela al dato biometrico, mediante la valorizzazione della natura "comunicativa" dell'atto di sblocco (es. USA).

Se i ragionamenti fin qui illustrati sono corretti, l'ordinamento italiano pare inserirsi nel novero dei sistemi più garantisti, grazie alla natura non strettamente dichiarativa del principio *nemo tenetur se detegere*. Certo, tutte le conclusioni rassegnate vanno comunque prese con beneficio d'inventario, nella consapevolezza che, di pari passo con gli apparecchi in parola, l'evoluzione tecnologica e la sua crescente capacità di perscrutare l'individuo rischiano di porre anche le cautele processuali, pensate per il "mondo fisico", a rischio di obsolescenza¹⁴⁰.

¹⁴⁰ Si veda ad esempio, a favore del riconoscimento di un'ampia e inedita "libertà di pensiero" in grado di includere anche la facoltà di non autoincriminarsi, N.A. FARAHANY, *Difendere il nostro cervello: la libertà di pensiero nell'era delle neurotecnologie* (2023), trad. it. Francesca Pè, Bollati Boringhieri, Torino, 2024, specie p. 90.

I SISTEMI DI RICONOSCIMENTO FACCIALE IN FASE DI INDAGINE: UNA BREVE ANALISI

STEFANO BILLI

SOMMARIO: 1. Una breve ricognizione sui sistemi di riconoscimento facciale. – 2. Le criticità dei sistemi di riconoscimento facciale con riguardo al processo penale; problemi di una disciplina “incompiuta”. – 3. Segue. Il “pendio scivoloso” degli appigli preesistenti nella fase delle indagini preliminari. – 4. Segue. La disciplina del c.d. “decreto capienze”. – 5. “*Artificial Intelligence Act*” e riconoscimento facciale. – 6. Conclusioni.

1. Una breve ricognizione sui sistemi di riconoscimento facciale

Quando ci si riferisce ai sistemi di riconoscimento facciale, ci si muove nel campo di quella tecnologia dell’identificazione biometrica concernente la possibilità di avvalersi di dispositivi *hardware*¹ e componenti *software*² allo scopo di verificare l’identità di una persona mediante l’individuazione di un suo particolare connotato fisico: il volto³.

Sgomberando il campo da ogni possibile equivoco, è d’uopo precisare che l’attività di riconoscimento di un volto, da parte delle forze di polizia, si

¹ Come evidenziato in G. FELLUGA, *I computer crimes definizioni ed elementi principali*, in *Tigor; Rivista di scienze della comunicazione e di argomentazione giuridica*, 2012, f. 1, p. 33, «per hardware si intende l’unità centrale, le memorie e le periferiche; ovvero tutte le parti fisiche di un personal computer (magnetiche, ottiche, meccaniche ed elettroniche) che ne consentono il funzionamento».

² Senza volerci qui addentrare nel complesso gorgo nozionistico sedimentatosi sull’argomento, è possibile, tuttavia, precisare come «per *software* si intende l’insieme dei programmi di elaborazione che permettono a un computer di operare» (G. FELLUGA, *I computer crimes*, cit., p. 33).

³ Sul punto, taluni usano l’acronimo “TRF” per denominare le tecnologie di riconoscimento facciale (anche note come *face detection systems*), ossia «i sistemi in grado di identificare o autenticare una persona a partire dalle caratteristiche del volto» (vedasi, *ex multis*, M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sist. pen.*, 12 Settembre 2022, p. 2).

riferisce ad un procedimento investigativo che – già in passato – veniva utilizzato al fine di appurare l'identità di un soggetto sconosciuto. Oggigiorno, tuttavia, questa nuova modalità di “trattamento” dell'immagine facciale, rappresenta un'innovazione che, se da un lato entusiasma per la sua dirompente efficienza e potenzialità d'uso, dall'altro lato spaventa per i numerosi interrogativi che solleva tra gli studiosi interessati alla materia.

Occorre, altresì, precisare come tale attività di riconoscimento operata da una “macchina” (ossia, da quell'infrastruttura *hardware* e *software* che governa il compimento di questa “ricognizione”) non può essere *tout court* assimilata alla capacità intellettuale umana di identificare una persona, in ragione del fatto che «i meccanismi mnestici ed euristici, affinati attraverso il lungo processo evolutivo della specie umana, dipendono infatti da processi biologici e neurologici non riproducibili dalle macchine, i cui progettisti e programmatori possono – al più – imitare ma in alcun modo replicare»⁴.

I sistemi di riconoscimento facciale si basano, nello specifico, su metodi (automatici o semi-automatici) «che registrano e paragonano le differenze della struttura geometrica del viso, tra cui la forma e la posizione dei suoi attributi – gli occhi, le labbra, il mento – e le loro relazioni spaziali»⁵. La peculiarità di questi metodi di riconoscimento facciale sta dunque nel fatto che essi sono “artificiali”, nel senso che l'operazione di identificazione e/o individuazione del viso avviene – interamente o parzialmente – per il tramite di “macchine”, oltrepassando quindi la tradizionale attività di “accertamento” compiuta dagli esseri umani (i quali, solitamente, si riconoscono tra loro mediante una ricognizione *de visu*).

Ergo, tale operazione di riconoscimento muove, in primo luogo, dall'acquisizione – da parte di uno o più dispositivi *hardware* – di un dato biometrico «rappresentato dall'immagine di un volto umano»⁶, che avviene tramite sensori deputati alla registrazione di un'immagine (oppure di una serie di immagini) del viso di un certo soggetto e delle sue caratteristiche più rilevanti⁷ (si pensi, ad esempio, alla forma della faccia, alla di-

⁴ Vedasi, in argomento, G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*, in *Cass. pen.*, 2025, p. 645.

⁵ Si rimanda, sul punto, all'accuratissimo contributo in materia redatto da E. SACCHETTO, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Dir. pen. cont.*, 2019, f. 2, p. 470.

⁶ Vedasi, sul punto, J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, in I. MICHELI (a cura di), *Ragioni Comuni 2019 – 2020. Risultati delle attività progettuali realizzate tramite assegni di ricerca finanziati dalla Regione Friuli Venezia Giulia ai sensi della L.R. 34/2015, art. 5, c. 29-33*, Trieste, 2023, p. 169.

⁷ Anche in questo caso risulta preziosissimo il contributo di E. SACCHETTO, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, cit., p. 470.

stanza tra gli occhi, alla conformazione del naso, all'ampiezza della fronte, ecc.)⁸. Compiuta l'estrazione del dato biometrico, le immagini così "prelevate" vengono "elaborate" da un algoritmo deputato a riscontrare, al loro interno, le principali caratteristiche facciali (c.d. *features*) dell'effigie analizzata, onde poi convertirle – in una «rappresentazione numerica che distingue univocamente una persona»⁹ – in formato digitale e realizzare, dunque, un *template*, ossia un modello la cui funzione è quella di essere utilizzato per riscontrare una sua eventuale corrispondenza con altre immagini contenute in banche dati precedentemente allestite¹⁰. All'esito di questa procedura di comparazione, qualora emerga un'effettiva congruenza tra i predetti termini di paragone (il *template* artificialmente modellato del viso di una persona ed un'immagine già archiviata), l'operazione di riconoscimento darà un esito positivo, fornendo l'identificazione dell'individuo di cui si voleva appurare (e/o confermare) l'identità. Occorre, comunque, precisare come l'anzidetta corrispondenza tra persone già "schedate" e il volto della cui identità ci si interroga riguarda un processo probabilistico in cui il *software* di riconoscimento facciale esprime la somiglianza delle immagini comparate «tramite un valore percentuale chiamato "*similarity score*": più alto è questo punteggio, più alta sarà la probabilità che l'immagine campione raccolta corrisponda a quella nella galleria» o banca dati¹¹. A seguito di tale operazione di "raffronto", spetterà poi all'operatore umano confermare o disattendere il risultato fornito – in termini probabilistici – dalla "macchina".

Tali strumenti – le cui potenzialità sono già intrinsecamente sorprendenti¹² – divengono ancor più efficaci, ed esponenzialmente "potenti",

⁸ Vale la pena sottolineare come l'acquisizione – da parte di uno o più dispositivi *hardware* – della figura di un volto umano può avvenire, oltre che mediante l'utilizzo di sensori deputati alla registrazione di un'immagine (oppure di una serie di immagini) del viso di un certo soggetto, anche attraverso l'estrazione del dato biometrico di una faccia ritratta in una fotografia (cfr. M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali*, cit., p. 2).

⁹ G. MOBILIO, *L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?*, in E. DI CARPEGNA BRIVIO-A. SANCINO (a cura di), *La democrazia della società digitale: tensioni e opportunità*, Torino, 2023, p. 4.

¹⁰ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale: rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021, p. 11.

¹¹ G. MOBILIO, *L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?*, cit., p. 4-5.

¹² Con riferimento al grande potenziale degli strumenti di riconoscimento facciale è utile tenere in considerazione anche A. PIN, *Non esiste la "pallottola d'argento": l'Artificial Face Recognition al vaglio giudiziario per la prima volta*, in *Dir. pubblico comparato ed europeo (DPCE) online*, 2019, f. 4, p. 3076, il quale propone un'attenta disamina della sentenza "R (Bridges) v. The Chief Constable of South Wales Police et al." emessa dalla High Court of Justice

quando sono affiancati all'intelligenza artificiale, ossia quando i *face detection systems* sono designati per funzionare attraverso algoritmi¹³ in grado non soltanto di apprendere autonomamente tutte le informazioni necessarie all'identificazione di una persona, ma anche di svolgere – senza l'intervento di alcun apporto umano (o riducendo quest'ultimo ad un contributo “marginale”) – le operazioni di riconoscimento. In tal caso, è dunque possibile riferirsi al concetto di *automated facial recognition systems* (cosiddetti “AFRS”), ossia strumenti di riconoscimento facciale che consentono «di analizzare in diretta i flussi video *live* provenienti dalle telecamere presenti in una zona; di selezionare dai *frame* delle immagini le impronte facciali delle persone riprese e di cercare, infine, un *match* tra quest'ultime e i volti contenuti in un archivio di partenza»¹⁴. Questa modalità operativa viene sovente definita *real-time*, cioè “in tempo reale”, onde richiamare l'attenzione sull'aspetto più caratteristico della procedura di riconoscimento facciale, ossia la capacità «non solo di identificare in modo più rapido perso-

dell'Inghilterra e Galles, che merita di essere approfondita poiché rappresenta uno dei primissimi approdi giurisprudenziali – se non addirittura il primo – in materia di «utilizzo dell'Artificial Face Recognition (AFR) nella previsione e nella individuazione dei reati». All'interno di questa sentenza si ammette come il riconoscimento facciale si manifesti innegabilmente quale «tecnologia dal grande potenziale per “la prevenzione e l'individuazione del crimine, la cattura dei sospetti o dei colpevoli e la protezione del pubblico”, di gran lunga superiore alle tecniche che semplicemente riprendono i passanti». Come evidenziato dall'Autore, tuttavia nel medesimo provvedimento giudiziale la Corte *de qua* rileva come il ricorso a tali strumenti faccia emergere anche «aspetti inquietanti», posto che i *tools* di riconoscimento facciale possono autonomamente elaborare «i dati biometrici della popolazione su larga scala e senza il coinvolgimento di quest'ultima». In merito a questa pronuncia della High Court of Justice dell'Inghilterra e Galles ha scritto anche J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Dir. pen. cont.*, 2020, f. 1, p. 234, il quale evidenzia l'importanza di tale sentenza poiché, seppur giunta a conclusioni interpretative non pienamente condivisibili, si manifesta tuttavia come «il primo arresto a livello mondiale ad aver affrontato in modo analitico la questione della compatibilità dell'utilizzo da parte della polizia di mezzi di riconoscimento facciale con i diritti fondamentali alla riservatezza e alla tutela dei dati personali» (*ivi*, p. 239).

¹³ Un'interessante “prospettiva storica” di algoritmo la si può rinvenire nella sentenza n. 7003 pronunciata – il 14 novembre 2022 – dalla terza sezione del T.A.R. Campania e oggetto della nota di E. FALLETTI, *Mai accettare caramelle né atti amministrativi da sconosciuti, ancorché algoritmi*, in *Il diritto dell'informazione e dell'informatica*, 2023, f. 1, p. 93-94: «l'algoritmo, sin dalla nozione desunta dai papiri di Ahmes del XVII secolo a.c., consiste in una sequenza finita e ordinata di operazioni elementari e chiare di calcolo che permettono di risolvere, in maniera determinata, un problema. Si tratta di una procedura di calcolo ben definita che consente, attraverso un insieme di operazioni effettuate in un determinato ordine, partendo da un insieme di dati (input), di ottenere un risultato atteso (output)». L'Autrice, in nota, richiama altresì A. M. TURING, *Computer machinery and intelligence*, in *Mind*, New Series, 1950, vol. 59, f. 236, p. 433-460.

¹⁴ J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, cit., p. 233.

ne di cui non si conosca l'identità, ma anche di conoscere in tempo reale se un certo individuo, sospettato di aver compiuto (o di poter commettere) un reato, possa trovarsi in un determinato luogo, sottoposto a osservazione»¹⁵.

Oltre alla funzione di riconoscimento facciale, tali sistemi – sfruttando le potenzialità offerte dall'intelligenza artificiale – sono quindi in grado di accertare comportamenti potenzialmente sospetti – come accade, ad esempio, nei casi di vagabondaggio (cosiddetta funzione di *loitering detection*) – di individuare assembramenti pericolosi o, ancora, di rilevare movimenti “insoliti” delle masse e, finanche, riconoscere lo stato emotivo dei soggetti “monitorati”¹⁶. Tale funzione di sorveglianza da parte delle autorità di polizia potrebbe non limitarsi all'individuazione di un soggetto, ma anche tipizzare una certa persona in determinate categorie, mediante l'estrazione di «alcune caratteristiche dall'immagine facciale, come l'età, le origini etniche, il genere, lo stato di salute»¹⁷.

Questa modalità di riconoscimento “in tempo reale” è una concreta ed attuale possibilità tecnologica di cui molti soggetti giuridici – privati ed istituzionali – possono oggi avvalersi. In Italia, ad esempio, l'azienda leccese “Parsec 3.26” ha elaborato un *software* denominato “SARI” (ossia, “sistema automatico di riconoscimento immagini”) che può funzionare anche in modalità *real time*. Più specificamente, questa società – su incarico del ministero dell'interno¹⁸ – ha elaborato un *software*, in grado di analizzare immagini e video, che permette il riconoscimento automatico dei volti in due scenari operativi, definiti *enterprise* e *real-time*. Tale *software* è stato sviluppato a seguito della richiesta del dicastero di affiancare un nuovo strumento al «sistema AFIS-SSA, per fornire all'operatore un efficiente supporto informatico che ne agevoli l'attività di indagine»¹⁹.

¹⁵ J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, cit., p. 232.

¹⁶ Cfr. W. NOCERINO, *Sulle modalità di acquisizione delle immagini provenienti dalle telecamere di videosorveglianza*, in *Cass. pen.*, 2024, p. 2423, la quale evidenzia come – a seguito dei sorprendenti sviluppi dell'intelligenza artificiale e dell'esponentiale miglioramento dei *software* dedicati – il fenomeno del monitoraggio degli individui e del controllo capillare continuativo remoto dei consociati che abitano le moderne “*smart city*” abbia disvelato scenari (anche di natura giuridica) inimmaginabili persino nel più recente passato.

¹⁷ G. MOBILIO, *L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?*, cit., p. 5.

¹⁸ Vedasi approfonditamente, su questo punto, MINISTERO DELL'INTERNO (DIPARTIMENTO DELLA PUBBLICA SICUREZZA), *Capitolato tecnico: procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini S.A.R.I. (Lotto N° 1)*, p. 6.

¹⁹ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell'identità di un volto*, provvedimento n. 440 del 26 luglio 2018, doc. web n. 9040256. Come

La modalità definita *enterprise* del suddetto *software* è stata ideata per rispondere all'esigenza di acclarare l'identità di un volto presente in un'immagine mediante una ricerca²⁰ – compiuta in automatico, per mezzo di uno o più algoritmi di riconoscimento facciale – all'interno di una banca dati di grandi dimensioni (dell'ordine di milioni di immagini) contenente le generalità e le caratteristiche (anche biometriche) di persone già foto-segnalate o schedate. Conclusa l'attività automatica di elaborazione dati, il *software* offre all'operatore una lista di volti simili a quello ricercato ordinata in base ad un "punteggio" che ne indica il grado di similarità. A questo punto, l'operatore "umano" ha il compito di «confermare o meno il risultato del *tool*, applicando le procedure di comparazione fisionomica, rispetto alle quali le forze di polizia scientifica ricevono una specifica formazione»²¹. Appare sin da subito evidente come l'intervento dell'operatore umano sia fondamentale, giacché il suo imprescindibile ruolo consiste nel valutare e convalidare i risultati offerti dal *software enterprise*²².

La modalità *real-time* di questo *software* compie, invece, il riconoscimento automatico dei volti «in un'area geografica (...) ben delineata» analizzando «in tempo reale i volti dei soggetti ripresi dalle telecamere ivi installate confrontandoli con una banca dati ristretta e predefinita (denominata "watch-list") la cui grandezza è dell'ordine delle centinaia di migliaia di soggetti»²³. La peculiarità di questo «scenario *real-time*» concerne quindi la possibilità di analizzare «in tempo reale più volti presenti contemporaneamente nei fotogrammi dei video in ingresso», «ottenuti dalle telecamere installate in molteplici punti di osservazione a supporto di operazioni

esplicito in R. BIONDO, *La banca dati nazionale dna italiana*, in *Riv. it. med. leg.*, 2016, f. 1, p. 216, l'acronimo "AFIS" sta ad indicare l'espressione inglese *automated fingerprint identification system* e si riferisce al sistema che acquisisce e gestisce le impronte digitali in uso al «Casellario centrale d'identità del Ministero dell'interno, Dipartimento della pubblica sicurezza collocato presso la Direzione centrale anticrimine della Polizia di Stato, Servizio polizia scientifica».

²⁰ In base a quanto stabilito nel predetto capitolato tecnico ministeriale, l'operatore può limitare la ricerca dell'identità di un volto ad una singola banca dati o ad una porzione di essa, filtrandola sulla base di informazioni anagrafiche o descrittive (sesso, altezza, ecc.) associate alle immagini; peraltro, nel caso in cui all'interno dell'immagine da analizzare siano presenti più volti, il *software* consente all'operatore anche la possibilità di selezionare il (singolo) viso da ricercare (*ivi*, p. 6).

²¹ J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, cit., p. 171.

²² Cfr. L. CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, in *Riv. it. dir. proc. pen.*, 2024, p. 247. Come evidenziato dall'Autore, con riferimento alla modalità *enterprise* del SARI «ci sono tre tipi di ricerca disponibili: la prima è basata sull'immagine facciale (modalità di ricerca del volto); la seconda si fonda su informazioni anagrafiche o descrittive collegate alle immagini presenti nell'archivio fotografico (modalità di ricerca anagrafica/descrittiva); la terza combina le due precedenti modalità».

²³ MINISTERO DELL'INTERNO (DIPARTIMENTO DELLA PUBBLICA SICUREZZA), cit., p. 6.

di controllo del territorio in occasione di eventi e/o manifestazioni»: riscontrata un'eventuale corrispondenza tra il fotogramma del video ed un volto presente nella "watch-list", il *software* genererà «un *alert* in grado di richiamare l'attenzione degli operatori»²⁴.

Tra le due modalità operative sussiste dunque una differenza non trascurabile. Nel sistema SARI *enterprise* la funzione è quella di cercare l'identità di un volto a partire da immagini statiche contenute su banche dati di enormi dimensioni («dell'ordine di 10 milioni di immagini»), allo scopo di addivenire ad una lista di risultati «simili» a quello ricercato da sottoporre poi all'attenzione di un operatore (il quale dovrà, materialmente, provvedere all'identificazione). Nel sistema SARI *real-time*, invece, si procede con un riconoscimento in tempo reale di volti presenti in flussi video provenienti da telecamere, mediante un algoritmo che – in maniera completamente autonoma – confronterà i volti presenti nei filmati con quelli di una *watch-list* (avente una dimensione dell'ordine di 100.000 identità predeterminate), onde fornire un *alert* all'operatore in caso di positiva corrispondenza tra il fotogramma acquisito ed il volto ricercato, senza necessità di alcun intervento umano²⁵. Qualora si dovesse verificare una corrispondenza positiva (c.d. *match*), a seguito dell'anzidetto avviso (*alert*) generato dall'algoritmo di riconoscimento, spetta comunque ad un operatore umano «il compito finale di confermare il riconoscimento e provvedere agli interventi necessari»²⁶.

In buona sostanza, la differenza tra questi due sistemi risiede dunque nella "tempestività" della ricognizione operata. Il SARI – nella declinazione *enterprise* – svolge un'attività che potrebbe essere definita di identificazione *ex post*, in ragione di un riconoscimento che non avviene in tempo reale rispetto alla "cattura" del volto, bensì in un momento successivo all'originaria acquisizione del dato biometrico. Il SARI, in modalità *real-time*, invece, è in grado di individuare istantaneamente un soggetto la cui immagine è stata acquisita da un AFRS: questa versione del *software* funge anche da strumento di sorveglianza generalizzata di chiunque venga ripreso da telecamere o, più in generale, da qualsiasi *hardware* deputato a tale scopo²⁷.

Punto in comune, per converso, dei due scenari operativi è la intrinseca necessità che, al termine delle operazioni analitico-computazionali

²⁴ MINISTERO DELL'INTERNO (DIPARTIMENTO DELLA PUBBLICA SICUREZZA), cit., p. 6.

²⁵ MINISTERO DELL'INTERNO (DIPARTIMENTO DELLA PUBBLICA SICUREZZA), cit., p. 6.

²⁶ Cfr. L. CAMALDO, *Intelligenza artificiale e investigazione penale*, cit., p. 247.

²⁷ A. FONSI, *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in *Penale - Diritto e procedura*, 14 maggio 2021.

eseguite dal *software*, vi sia sempre un intervento umano “finale” cui spetta il compito di confermare o meno il riconoscimento ipotizzato dall’algoritmo «e di prendere i provvedimenti conseguenti»²⁸.

Ebbene, questa differenza tra le due modalità di funzionamento del sistema SARI si riflette non soltanto nel concreto impiego del *software* da parte delle autorità istituzionali, ma anche sui profili di legittimità ed ammissibilità di questo strumento.

2. *Le criticità dei sistemi di riconoscimento facciale con riguardo al processo penale; problemi di una disciplina “incompiuta”*

Ancorché foriero di innegabili vantaggi, l'utilizzo dei sistemi di riconoscimento facciale pone numerosi interrogativi circa la sua compatibilità con le garanzie costituzionali e con i principi del giusto processo. Tali strumenti, infatti, comportano necessariamente una captazione di un dato biometrico, incidendo sulle libertà fondamentali e sul trattamento dei dati personali²⁹. Basti considerare come i *tools* di cui si sta trattando siano più invasivi «di altre tecnologie biometriche: rispetto alle impronte digitali o ai campioni di DNA, infatti, è molto più facile catturare l'immagine di un volto, dal momento che ciò può avvenire a distanza, con persone in movimento, senza alcun contatto fisico e senza che vi sia alcuna consapevolezza o consenso»³⁰.

Dunque, il punto di partenza nell'affrontare il dibattito emergente riguardo l'impiego dei sistemi di riconoscimento non può non scaturire dalla presa di coscienza per cui l'accesso ad immagini facciali (o, più in generale, a qualunque dato biometrico) deve essere considerato come un'ingerenza nella vita delle persone e può trovare giustificazione soltanto quando esso trovi fondamento in una specifica base normativa³¹. Tuttavia, il punto chiave della questione sta proprio nel fatto che, ad oggi, non esiste alcuna specifica disposizione all'interno dell'ordinamento italiano

²⁸ J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, cit., p. 171.

²⁹ Più in generale (come rilevato da G. MOBILIO, *L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?*, cit., p. 2-3), l'interrogativo scaturente dall'utilizzo delle tecnologie di riconoscimento facciale concerne la compatibilità delle medesime non solo con la disciplina sulla protezione dei dati personali, ma anche – e soprattutto – coi diritti fondamentali tutelati dagli ordinamenti democratici.

³⁰ G. MOBILIO, *L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?*, cit., p. 2.

³¹ Cfr. S. EL SABI, *La violazione della privacy in caso di raccolta “sistematica” dei dati biometrici e genetici: lesi i diritti e le libertà della persona interessata?*, in *Giustizia civile.com*, 2023, f. 5, p. 9-10.

che legittimi espressamente l'impiego dei sistemi di riconoscimento facciale. In ragione di tale lacuna legislativa, si è cercato di validare l'impiego di tali nuove tecnologie mediante il richiamo a disposizioni già esistenti, muovendo però dalla consapevolezza che, *ab origine*, il riconoscimento facciale si configura come una modalità di trattamento di dati biometrici ed afferisce, anzitutto, alla materia della tutela e della protezione dei dati personali, entrambe tutelate dall'art. 8 Carta dir. fond. UE³².

Poiché, ai sensi di tale articolo³³, il rispetto delle regole sulla protezione dei dati di carattere personale deve essere soggetto al controllo di un'autorità indipendente, diviene dunque fondamentale considerare, in primo luogo, la posizione assunta dal Garante per la protezione dei dati personali.

Da questo punto di vista, il Garante si è espresso circa le eventuali criticità insorgenti dall'utilizzo «di un sistema automatico di ricerca dell'identità di un volto presente in un'immagine facciale all'interno di una banca dati, denominato "SARI Enterprise"»³⁴. Secondo tale autorità, «il trattamento dei dati biometrici ricavabili anche dall'immagine facciale, effettuato dalle forze di polizia a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, è previsto e disciplinato da una pluralità di fonti normative»³⁵. Il garante, inoltre, richiama anche le fonti di diritto europeo e si sofferma, in particolare, sul regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (ossia, sul regolamento generale sulla protezione dei dati, c.d. "GDPR"), per quanto concerne il trattamento dei dati biometrici (ivi compresi quelli ricavabili dall'immagine facciale)³⁶.

In particolare, il Garante – dovendosi esprimere sulla modalità ope-

³² Infatti, l'art. 8 Carta dir. fond. UE (rubricato «protezione dei dati di carattere personale») stabilisce, al suo primo comma, che «ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano».

³³ Vedasi il comma 3 dell'art. 8 Carta dir. fond. UE.

³⁴ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell'identità di un volto*, cit.

³⁵ In particolare, si citano: l'art. 4 del T.U.L.P.S., approvato con regio decreto 18 giugno 1931, n. 773 e art. 7 del relativo regolamento di esecuzione, approvato con regio decreto 6 maggio 1940, n. 635; l'art. 349 del codice di procedura penale; l'art. 11 del decreto legge 21 marzo 1978, n. 59, convertito in legge 18 maggio 1978, n. 191; l'art. 5 del decreto legislativo 25 luglio 1998, n. 286.

³⁶ Questa sede non consente di approfondire, per esigenze di sinteticità, l'interessante iter giuridico intrapreso dal GARANTE PER LA PROTEZIONE DEI DATI PERSONALI all'interno del provvedimento n. 440 del 26 luglio 2018, che merita attenzione poiché non soltanto ripercorre analiticamente le normative europee di riferimento, ma anche perché riassume – in maniera esauriente – i tratti salienti del funzionamento del sistema SARI e dei suoi scenari operativi *enterprise* e *real-time*.

rativa del SARI *enterprise* – ha ritenuto che criticità di tale sistema non sono riscontrabili in tale “scenario”, posto che quest’ultima declinazione del *software* compie un trattamento dei dati personali consistente in 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»³⁷. Infatti, seguendo le argomentazioni del garante, il SARI *enterprise* si configurerebbe come un *upgrade* dell’AFIS: quest’ultimo già «consente di effettuare ricerche nell’archivio dei soggetti fotosegnalati (...) tramite l’opera manuale di un operatore, che deve inserire nei campi presenti nella maschera di interrogazione informazioni anagrafiche, connotati e contrassegni (ad esempio, colore dei capelli, degli occhi, di tatuaggi), al fine di individuare la presenza nell’archivio AFIS del soggetto ricercato». Il SARI *enterprise*, d’altro canto, non produce risultati aggiuntivi rispetto al sistema AFIS, ma automatizza, invece, «alcune operazioni che prima richiedevano l’inserimento manuale di connotati identificativi, consentendo le operazioni di ricerca nel data base dei soggetti fotosegnalati attraverso l’inserimento di una immagine fotografica, che sarà elaborata automaticamente al fine di fornire l’elenco di foto segnaletiche somiglianti, ottenute attraverso un algoritmo decisionale che ne specifica la priorità»³⁸.

Il garante si è espresso, in seguito, anche in tema di SARI *real-time*, evidenziando come questa modalità di riconoscimento (orientata «all’effettuazione di un trattamento di dati personali per finalità di prevenzione di reati e minacce alla sicurezza pubblica e, anche su delega dell’Autorità Giudiziaria, di indagine, accertamento e perseguimento di reati») – poiché determina «una forte interferenza con la vita privata delle persone interessate» – deve trovare giustificazione in una adeguata base normativa che, attualmente, non è tuttavia rinvenibile all’interno di alcuna specifica disposizione di legge che consenta tale tipo di trattamento³⁹. Peraltro, il ga-

³⁷ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell’identità di un volto*, cit.

³⁸ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell’identità di un volto*, cit.

³⁹ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema SARI Real Time - 25 marzo 2021*, provvedimento n°127 del 25 marzo 2021, doc. web n°9575877. Interessante è il percorso motivazionale affrontato dal Garante, secondo cui il SARI *real-time* realizza un trattamento di dati biometrici «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; ancorché la valutazione di impatto indica che i dati di questi ultimi sarebbero immediatamente cancellati, nondimeno, l’identificazione di una persona in un luogo pubblico comporta il trattamento biometrico di tut-

rante non ha ritenuto applicabili quelle fonti normative che il ministero dell'interno aveva invece considerato conferenti al fine dell'inquadramento giuridico dell'utilizzo del SARI *real-time*. Nello specifico, l'autorità garante non ha ritenuto che gli «articoli del codice di procedura penale (agli artt. 134 c. 4, 234, 266, 431 c.1 lett. b, oltre gli artt. 55, 348, 354 e 370 sull'attività di polizia giudiziaria)» richiamati dal ministero potessero legittimare l'impiego del sistema SARI *real-time*, giacché «non costituiscono base giuridica idonea per trattamenti di dati biometrici diretti all'identificazione personale», in quanto non assurgono a «quella fonte normativa specifica richiesta dall'art. 7»⁴⁰ del d.lgs. 18 maggio 2018, n. 51.

In sintesi, la raccolta di dati biometrici (tra cui anche quelli concernenti le immagini facciali), seppur finalizzata e/o funzionale all'identificazione di determinati soggetti, può essere effettuata «solo in presenza di un'idonea previsione normativa ai sensi dell'art. 7 d.lgs. n. 51/2018, che al momento non pare rinvenibile»⁴¹.

3. Segue. Il “pendio scivoloso” degli appigli preesistenti nella fase delle indagini preliminari

Nel tentativo di legittimare l'utilizzo – in seno alla fase delle indagini preliminari – dei sistemi di riconoscimento facciale, ogni intenzione di ravvisare, all'interno del codice di procedura penale, un sostrato efficace a consentire l'impiego di tali strumenti si scontra, inevitabilmente, con l'evidenza che nessuna specifica disposizione legislativa dell'ordinamento interno (eccezion fatta per le precisazioni di seguito indicate) può avallare, *sic et simpliciter*, il ricorso a tali mezzi di trattamento del dato biometrico facciale.

Senza addentrarsi in un'esegesi specifica di ciascuna singola fonte od

te le persone che circolano nello spazio pubblico monitorato, al fine di generare i modelli di tutti per confrontarli con quelli delle persone incluse nella “watch-list”. Pertanto, si determina una evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui.

⁴⁰ Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time - 25 marzo 2021*, cit., in cui si richiama il ruolo pivotale dell'art. 7 d. lgs. 18 maggio 2018, n. 51, che così dispone: «il trattamento di dati di cui all'articolo 9 del regolamento UE è autorizzato solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento, ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato».

⁴¹ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento n. 54 del 26 febbraio 2020*, doc. web n. 9309458.

articolo di legge astrattamente accostabile al tema dei sistemi di riconoscimento facciale, è d'uopo evidenziare come in questo contesto sia cruciale distinguere preliminarmente a quale particolare tipo di AFRS ci si riferisca. Se nel caso di un riconoscimento facciale compiuto in modalità *enterprise* è comprensibile richiamare certi istituti giuridici propri del processo penale, viceversa, nei sistemi di riconoscimento funzionanti in maniera *real time*, non è possibile riscontrare alcuna disposizione codicistica utile per inquadrarne l'utilizzo.

Ciò premesso, un impiego dei sistemi di riconoscimento facciale nella fase delle indagini preliminari potrebbe trovare un proprio fondamento teorico nella disciplina di cui all'art. 349 c.p.p., dedicata, per l'appunto, all'identificazione della persona sottoposta alle indagini⁴². Sebbene l'art. 349 c.p.p. sia stato originariamente concepito per operazioni "tradizionali" di identificazione della persona, nulla osta – in linea teorica – a che sia possibile per le forze di polizia e per l'autorità giudiziaria continuare ad impiegare il SARI quale ausilio al compimento di tali fini⁴³. Difatti, un uso degli AFRS (in modalità avulse da automatismi in tempo reale, come accade, per esempio, per il SARI *enterprise*) in sede di indagini preliminari rappresenterebbe, in ultima analisi, un mero potenziamento degli strumenti oggi in uso al fine di identificare un individuo. Tale approdo argomentativo scaturisce dalla constatazione che la captazione (ed il conseguente trattamento) del dato biometrico derivante dall'uso dei sistemi di riconoscimento facciale altro non è che una delle varie modalità attraverso cui «la polizia giudiziaria procede alla identificazione della persona nei cui confronti vengono svolte le indagini»: l'automazione – richiedente sempre un intervento di un operatore umano – insita nel meccanismo di funzionamento dell'AFRS (*rectius*, del SARI *enterprise*) sarebbe, quindi, ascrivibile alla locuzione «altri accertamenti» di cui al comma 2 del medesimo art. 349 c.p.p.⁴⁴.

Sempre in ambito di indagini preliminari, diversamente la disciplina delle intercettazioni di cui all'art. 266 c.p.p. non può rappresentare una

⁴² Stabilisce l'art. 349 comma 1 c.p.p., che «la polizia giudiziaria procede alla identificazione della persona nei cui confronti vengono svolte le indagini e delle persone in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti»; il medesimo articolato specifica poi che «alla identificazione della persona nei cui confronti vengono svolte le indagini può procedersi anche eseguendo, ove occorra, rilievi dattiloscopici, fotografici e antropometrici nonché altri accertamenti».

⁴³ Cfr. J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, cit., p. 178.

⁴⁴ E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna*, Torino, 2025, p. 224.

«base giuridica idonea per trattamenti di dati biometrici diretti all'identificazione personale»⁴⁵.

Oltre all'ovvia considerazione per cui né l'art. 266 c.p.p., né l'art. 266-bis c.p.p., contengono elementi testuali che legittimino un'interpretazione estensiva verso gli AFRS, occorre altresì evidenziare come sussistano differenze ontologicamente inconciliabili tra la captazione di comunicazioni e le immagini che impediscono tale accostamento ermeneutico. Mentre un'intercettazione serve a carpire il contenuto di una comunicazione riservata tra due o più persone, il riconoscimento facciale, invece, consiste in un'analisi di dati biometrici, tratti da immagini o video, allo scopo di confrontarli poi con analoghi elementi presenti in un *database*. Allo stesso modo, neppure l'acquisizione in tempo reale di un flusso comunicativo può fungere da punto in comune con l'estrapolazione di figure di volti derivanti da un utilizzo di AFRS funzionanti in modalità *real time*: captare il contenuto di una comunicazione è attività intrinsecamente diversa (e oggettivamente non assimilabile), ancorché ciò avvenga in tempo reale, dal raffronto di volti ai fini di una loro identificazione. In sintesi è fondamentale precisare come sia errato interpretare la disciplina delle intercettazioni al fine di “modellarla” a sostegno dell'impiego degli AFRS giacché il riconoscimento facciale non è una forma di captazione di conversazioni né ad essa può essere in alcun modo assimilata⁴⁶.

4. Segue. *La disciplina del c.d. “decreto capienze”*

La volontà di una parte della pubblica amministrazione (e finanche della politica)⁴⁷ di far entrare in funzione quanto prima, all'interno dell'ordinamento italiano, i sistemi di riconoscimento facciale – onde perseguire gli scopi di investigazione, vigilanza e, più in generale, di contrasto al crimine – spinge i sostenitori di tali tecnologie a richiamare l'attenzione su certe disposizioni di matrice processual-penalistica, ancorché non specificamente dedicate all'enucleazione di regole in tema di trattamento del dato biometrico facciale, pur di individuarne un fondamento giuridico che ne legittimi l'impiego.

Tuttavia, questa prassi contrasta con quanto stabilito espressamente

⁴⁵ Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time* - 25 marzo 2021, cit.

⁴⁶ V. *amplius* V. BOSCO, *Il riconoscimento facciale all'interno del processo, tra contorsioni del sistema e ricadute mancate*, § 1.

⁴⁷ Cfr. J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, cit., p. 176.

dalle fonti di diritto europeo, a norma delle quali l'utilizzo di tecnologie di riconoscimento facciale per finalità di prevenzione e repressione di reati deve trovare necessariamente giustificazione in una adeguata base normativa, pena la sua inammissibilità⁴⁸.

Per tale ragione, in epoca recente il legislatore italiano è intervenuto con un primo embrione di intervento regolativo circa l'utilizzo dei sistemi di riconoscimento facciale, con lo scopo di consentire l'impiego del SARI e, al contempo, di assicurare il pieno rispetto dei diritti fondamentali sanciti dalle fonti normative europee⁴⁹.

Nello specifico, il d.l. 8 ottobre 2021, n. 139 (poi convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205) all'interno del suo art. 9 comma 9 stabilisce che 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, sono sospese fino all'entrata in vigore di una disciplina legislativa della materia⁵⁰ e comunque non oltre il 31 dicembre 2025⁵¹.

⁴⁸ Vale la pena richiamare il dettato dell'art. 9 (rubricato «trattamento di categorie particolari di dati personali») del citato regolamento (UE) 2016/679, all'interno del quale è enucleato il divieto di trattare «dati biometrici intesi a identificare in modo univoco una persona fisica», salvo i casi particolari enunciati dalla medesima disposizione. In merito al «trattamento di categorie particolari di dati personali» testé accennato interviene anche l'art. 7 d. lgs. n. 51 del 2018 che, in attuazione del predetto art. 9 del regolamento (UE) 2016/679, stabilisce come esso può essere «autorizzato solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento, ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato».

⁴⁹ Il richiamo alle fonti europee viene esplicitato dal medesimo Legislatore, il quale – all'*incipit* del predetto art. 9 – chiarisce che, nell'impiego di sistemi di riconoscimento facciale, occorre considerare sia «quanto disposto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016», sia «la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016» (cioè, la Direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, c.d. «LED»), nonché il «principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea» allorquando occorre disciplinare l'ammissibilità, le condizioni e le garanzie relativi all'impiego di sistemi di riconoscimento facciale.

⁵⁰ Cfr. art. 9 comma 9 d.l. 8 ottobre 2021, n. 139.

⁵¹ Non è da sottovalutare come tale scadenza – fissata dal Legislatore al giorno 31 dicembre 2025 – sia l'effetto di una «proroga», giacché *ab origine* la citata sospensione dell'installazione e dell'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) rimaneva subordinata non soltanto sino all'entrata in vigore di una disciplina legislativa della materia, ma soprattutto

Al contempo, però, il comma 12 del medesimo art. 9 mitiga la sospensione anzidetta prevedendo che essa non si applica «ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali»⁵², allorquando avvengano in presenza di un parere favorevole del garante per la protezione dei dati personali, «salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero»⁵³.

Da un'iniziale disamina di questa disposizione sembrerebbe come tale dettato normativo enuclei la possibilità – in taluni specifici casi – di adoperare sistemi di riconoscimento facciale, così escludendo l'operatività dei precedenti commi 9, 10 e 11 d.l. n. 139 del 2021 (per come poi convertito): infatti, lo stesso comma 12 ammette che l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale – operanti attraverso l'uso dei dati biometrici ed allestiti in luoghi pubblici o aperti al pubblico – possa essere consentita, purché essa sia riconducibile a «trattamenti»⁵⁴ effettuati da soggetti all'uopo autorizzati ed espres-

al termine del 31 dicembre 2023. Un siffatto differimento temporale di due anni (quale data di scadenza della sospensione *de qua*) sottolinea, in maniera evidente, come il Legislatore non abbia ancora deciso di regolamentare puntualmente la materia, lasciando dunque che, nell'ordinamento italiano, restino *de facto* inoperanti i sistemi di riconoscimento facciale (specialmente nella loro declinazione “*real-time*”).

⁵² Il richiamo al d. lgs. n. 51 del 2018 (rubricato «attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio»), si riferisce all'attuazione della già citata direttiva (UE) 2016/680, ossia la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (c.d. “LED”), la quale garantisce la protezione dei dati personali delle persone coinvolte in procedimenti penali, che siano testimoni, vittime o iniziati.

⁵³ L'art. 9 comma 12 d.l. n. 139 del 2021 stabilisce, più specificamente, che «i commi 9, 10 e 11 non si applicano ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali di cui al decreto legislativo 18 maggio 2018, n. 51, in presenza, salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero, di parere favorevole del Garante reso ai sensi dell'articolo 24, comma 1, lettera b), del medesimo decreto legislativo n. 51 del 2018».

⁵⁴ L'espressione «trattamenti» adoperata dal Legislatore italiano evoca quanto disposto dall'art. 4 comma 1 punto 2, del citato regolamento generale sulla protezione dei dati, secondo cui – con il termine “trattamento” – ci si riferisce a «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma

samente individuati nelle c.d. «autorità competenti»⁵⁵ e nella «autorità giudiziaria». È importante sottolineare, tuttavia, come l'autorizzazione all'impiego dei *facial recognition systems* diverga – ai sensi del comma 12 dell'art. 9 – a seconda che la fruizione di tali apparati sia compiuta, da un lato, dalle autorità di pubblica sicurezza o forze di polizia e, dall'altro, dall'autorità giudiziaria. Nella prima ipotesi si prevede espressamente la necessità di un previo «parere favorevole del garante reso ai sensi dell'articolo 24, comma 1, lettera b), del medesimo decreto legislativo n. 51 del 2018». Al contrario, se l'impiego dei *facial recognition systems* viene disposto dalla magistratura (ossia, quando ci si riferisce a «trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero»⁵⁶), l'autorizzazione amministrativa del garante per la protezione dei dati personali non è in alcun modo richiesta⁵⁷.

Sul punto, occorre però considerare come «l'effettiva portata da attribuire al comma 12 dell'art. 9» non debba essere confusa con un'indiscriminata possibilità – «per determinate istituzioni deputate al contrasto delle attività illecite» – di «utilizzare siffatti strumenti per scopi di prevenzione e di repressione della criminalità in luoghi pubblici e aperti al pubblico», bensì quale regola volta a ribadire che, anche al netto della moratoria generale, le autorità di *law enforcement* possano continuare ad avvalersene, «nei soli casi e con i limiti stabiliti dalle fonti sovraordinate e dal codice di rito»⁵⁸.

di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

⁵⁵ Il concetto di «autorità competenti», menzionato all'art. 12 d.l. n. 139 del 2021, deve essere inteso alla stregua della definizione stabilita all'art. 2 comma 1 lett. g, d. lgs. n. 51 del 2018 (ossia «qualsiasi autorità pubblica dello Stato, di uno Stato membro dell'Unione europea o di uno Stato terzo competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica»). Conseguentemente, in guisa dell'art. 47, comma 1, del d. lgs. n. 51 del 2018, per «autorità competenti» si fa riferimento alle autorità di pubblica sicurezza o forze di polizia.

⁵⁶ Cfr. art. 9 comma 12 d.l. n. 139 del 2021.

⁵⁷ Cfr. J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, cit., p. 177.

⁵⁸ J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, cit., p. 177-178. Come osservato da J. DELLA TORRE, una differente esegesi del comma 12 dell'art. 9 *de quo* «finirebbe per esporci a inevitabili profili di illegittimità costituzionale», dato che tale disposizione non soltanto «non rispetterebbe il rigido vaglio di proporzionalità (in astratto e in concreto), imposto dagli artt. 7, 8 e 52 della Carta di Nizza, nonché dall'art. 10 della direttiva 2016/680/UE, quale presupposto essenziale per il legittimo trattamento di dati biometrici, idonei a identificare in modo univoco una persona fisica», ma «non sarebbe neppure idonea a rispettare le condizioni stringenti a cui l'art. 13 Cost. subordina la possibilità di restringere la libertà dell'individuo; difatti, l'art. 9, comma 12, d.l. 139/2021 nulla

Avendo riguardo al sistema SARI *enterprise*, il comma 12 dell'art. 9 d.l. n. 139 del 2021 non ha dunque introdotto su questo argomento alcuna riforma palpabile, giacché anche prima era opinione diffusa ritenere che il sistema SARI *enterprise* potesse essere oggetto di legittimazione in guisa del dettato dell'art. 349 c.p.p.

Inversamente, non sono rinvenibili “appigli” processual-penalistici adeguati onde legittimare un'esegesi dell'art. 9 comma 12 d.l. n. 139 del 2021, finalizzata all'impiego del sistema SARI *real-time*, sia perché – come precisato dal garante per la protezione dei dati personali⁵⁹ – non si riscontrano, allo stato attuale, disposizioni codicistiche che soddisfino i requisiti imposti dall'art. 7 d.l. n. 51 del 2018, sia per il fatto che codesta peculiare declinazione del *software* non potrebbe nemmeno assurgere ad una forma (seppur atipica) di individuazione o, eventualmente, di ricognizione, pena l'indebita lesione di quelle “guarentigie” che il rito penale pone «a protezione della libertà morale della persona»⁶⁰. Pertanto, anche in quest'ultimo caso tale comma si palesa come fonte normativa del tutto inadeguata ai fini di una compiuta regolamentazione della materia dei sistemi di riconoscimento facciale di tipo *real-time*, posto che la sua entrata in vigore non è stata accompagnata da alcuna specifica disciplina in grado di legittimare questa peculiare (e particolarmente invasiva) specie di trattamento dei dati personali.

5. “Artificial Intelligence Act” e riconoscimento facciale

A rendere ancor più complessa la tematica della cornice giuridica entro la quale poter inquadrare il riconoscimento facciale si registra, inoltre, l'avvento del recentissimo “*Artificial Intelligence Act*” (il c.d. “regolamento sull'intelligenza artificiale”)⁶¹. In estrema sintesi, l'*AI Act* – che rappresenta il primo quadro giuridico globale sull'intelligenza artificiale a livello mondiale – stabilisce, «regole armonizzate sull'intelligenza artificiale» con lo scopo di promuovere, in tutta Europa, un utilizzo affidabile di tale stru-

dice circa i casi e i modi in cui le forze di polizia o la magistratura possono avvalersi dei sistemi di riconoscimento facciale automatico; né specifica alcuna garanzia a salvaguardia dei diritti e le libertà della persona».

⁵⁹ Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time - 25 marzo 2021*, cit.

⁶⁰ J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, cit., p. 178, l'Autore richiama l'art. 189 c.p.p. quale “barriera” di protezione verso un impiego «insidioso» degli AFRS, i cui “puntelli” possono essere ravvisati pure nel dettato degli artt. 64 comma 2, 188 e 220 comma 2 c.p.p.

⁶¹ Ci si riferisce, qui, al regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024.

mento⁶² da parte di soggetti pubblici e privati, attraverso un modello di governance armonizzato basato sulla classificazione dei rischi di questi sistemi»⁶³. Ebbene, in quest'ottica l'*AI Act* assume un'importanza notevolissima, giacché la disciplina in esso contenuta diviene fonte di regolamentazione anche in tema di riconoscimento facciale.

In particolare, merita profonda attenzione il dettato dell'art. 5 di tale regolamento, all'interno del quale sono elencate una serie di pratiche di intelligenza artificiale (tra cui quelle legate all'utilizzo di sistemi di riconoscimento facciale) vietate ovvero consentite al ricorrere di un complesso stringente di requisiti. Più specificamente, ai sensi dell'art. 5 dell'*AI Act* (che proibisce l'uso di sistemi di identificazione biometrica remota "in tempo reale"⁶⁴) va ritenuto inammissibile⁶⁵ ogni utilizzo degli AFRS in modalità *real-time*, giacché tale modalità del *software* corrisponde ad una pratica di intelligenza artificiale espressamente vietata. Un simile divieto origina dal fatto che, nel predisporre una classificazione delle soglie di rischio⁶⁶, il regolamento (UE) 2024/1689 qualifica come "inaccettabile" l'uso di sistemi di riconoscimento facciale aventi declinazione "in tempo reale" e altre tecniche di sorveglianza di massa⁶⁷. Il rischio derivante dall'impiego di tali strumenti viene infatti giudicato inaccettabile poiché essi risultano «capaci di impattare così severamente sui diritti individuali» che necessitano di essere *tout-court* proibiti⁶⁸.

Disciplina differente, invece, è stabilita da questa fonte normativa per

⁶² Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024.

⁶³ SERVIZIO STUDI DEL SENATO DELLA REPUBBLICA, *Dossier n. 289; Disposizioni e deleghe al Governo in materia di intelligenza artificiale - A.S. n. 1146*, 11 giugno 2024, p. 4.

⁶⁴ Cfr. art. 5, § 1, lett. b, regolamento (UE) 2024/1689.

⁶⁵ Fatte salve le eccezioni comunque previste dal regolamento. In tema v. *amplius* C. CESARI, *Il riconoscimento facciale dall'AI Act all'ordinamento italiano: le direttrici di un'evoluzione necessaria*, § 2.

⁶⁶ Lungi dal poter affrontare compiutamente un approfondimento dell'*AI Act*, si vuole in questa sede richiamare velocemente come tale regolamento europeo abbia creato un modello di *governance* che si basa sulla classificazione di rischi derivanti dall'impiego dell'intelligenza artificiale.

⁶⁷ Sul punto, è qui utile precisare come l'*AI Act* abbia delineato una classificazione del rischio derivante dall'utilizzo dell'intelligenza artificiale che si suddivide «in tre categorie principali (reclusus, tre più una), a seconda del livello di rischio che ciascuna presenta: 1) rischio inaccettabile; 2) alto rischio e 3) rischio limitato. A tali tre categorie se n'è aggiunta (...) una quarta relativa ai sistemi di GenAI (ossia ai sistemi di intelligenza artificiale a uso generale) che presentino un rischio sistemico per l'Unione Europea» (O. POLLICINO, *Costituzionalismo digitale, intelligenza artificiale e regolazione. alla ricerca dell'equilibrio sostenibile tra innovazione e tutela dei diritti fondamentali*, in *Riv. dott. comm.*, 2025, f. 3, p. 440).

⁶⁸ O. POLLICINO, *Costituzionalismo digitale, intelligenza artificiale e regolazione*, cit., p. 440.

tutti quei sistemi di identificazione biometrica c.d. “a posteriori”: per tali tipologie di AFRS, (di cui un esempio è il sistema SARI *enterprise*) il regolamento *de quo* non prevede specificamente un divieto di accesso al mercato, implementazione ed utilizzo, ma ne consente, invece, una fruizione a condizione «che siano rispettati diversi requisiti, come, ad esempio, la predisposizione di un sistema di gestione dei rischi, una serie di obblighi informativi per gli utenti e, soprattutto, la previsione della sorveglianza umana»⁶⁹.

La diversa classificazione del rischio sottesa all’impiego di tali sistemi (*real time* da un lato, *ex post* dall’altro) scaturisce, dunque, dalla consapevolezza circa la minore incidenza – sugli equilibri costituzionali e sui diritti fondamentali della persona – delle identificazioni biometriche che operano avvalendosi di meccanismi di intelligenza artificiale che non richiedono un riconoscimento in tempo reale.

A fronte dell’apposizione di tali divieti e/o limitazioni stringenti al loro utilizzo, l’atteggiamento del Parlamento europeo manifesta dunque una comprensibile diffidenza circa l’impiego di sistemi di riconoscimento facciale percepiti come meccanismi eccessivamente invasivi della sfera dei diritti e delle libertà delle persone coinvolte⁷⁰.

Tale diffidenza è peraltro presente anche all’interno della legge 23 settembre 2025, n. 132⁷¹, adottata – a seguito dell’entrata in vigore del regolamento (UE) 2024/1689 – con lo scopo di sostenere e promuovere lo sviluppo di sistemi di intelligenza artificiale che «siano basati su una visione antropocentrica, nonché su principi di trasparenza, responsabilità, equità e rispetto per i diritti fondamentali, che garantiscono un equilibrio tra le opportunità che offrono le nuove tecnologie e i rischi legati al loro uso improprio, al loro impiego dannoso e anche al loro sottoutilizzo»⁷².

Tale novella legislativa, che si pone come prima fonte nazionale vigente in tema di regolamentazione dell’intelligenza artificiale⁷³, merita in-

⁶⁹ L. CAMALDO, *Intelligenza artificiale e investigazione penale*, cit., p. 246.

⁷⁰ L. CAMALDO, *Intelligenza artificiale e investigazione penale*, cit., p. 246.

⁷¹ Ci si riferisce al provvedimento legislativo, rubricato «disposizioni e deleghe al Governo in materia di intelligenza artificiale», entrato in vigore lo scorso 10 ottobre 2025 e concernente – come indicato dal SERVIZIO STUDI DEL SENATO DELLA REPUBBLICA, cit., p. 4 – l’introduzione di una normativa nazionale volta a predisporre «un sistema di principi di *governance* e misure specifiche adatte al contesto italiano per mitigare i rischi e cogliere le opportunità dell’intelligenza artificiale».

⁷² SERVIZIO STUDI DEL SENATO DELLA REPUBBLICA, cit., p. 5.

⁷³ La legge n. 132 del 2025 si compone di 28 articoli, racchiusi all’interno di cinque capi, di cui il più rilevante – a sommosso avviso dello scrivente – è il primo, ossia quello concernente i principi da seguire per l’uso dell’intelligenza artificiale, attraverso un approccio trasparente e rispettoso dei diritti fondamentali. Uno specifico capo è dedicato alle c.d.

dubbiamente apprezzamento per aver dato un primissimo contributo ai problemi scaturenti dall'uso dell'intelligenza artificiale⁷⁴. In particolare, la legge n. 132 del 2025 propone alcuni principi⁷⁵ che, ispirati dall'intervento del legislatore europeo, costituiscono una iniziale risposta normativa rispetto agli interrogativi che emergono rispetto all'utilizzo dell'intelligenza artificiale.

Tuttavia, quanto al tema del riconoscimento facciale, la legge n. 132 del 2025 pare ancora lontanissima dal fornire un'adeguata base normativa all'impiego degli AFRS alla luce non solo delle fonti sovranazionali, ma anche dei principi costituzionali e, più in generale, dell'intero ordinamento giuridico italiano. In particolare, non è possibile rinvenire, all'interno della legge n. 132 del 2025, alcuna specifica disposizione relativa alle svariate tecniche di identificazione biometrica e ad una loro precipua inammissibilità. Difatti, in nessuno dei cinque capi della novella sono inseriti espliciti riferimenti alla tematica del riconoscimento facciale che, pertanto, continua ad essere unicamente disciplinata dalla sovraordinata fonte europea.

Per tali ragioni sarà necessario che il legislatore, per ottemperare a quei vincoli discendenti dalla normativa europea – dato che il regolamento (UE) 2024/1689 ha preminenza sulla legge italiana – intervenga anche nell'armonizzare l'ordinamento interno rispetto alla tematica del riconoscimento facciale, non solo al fine di cristallizzare il divieto di impiego di strumenti di riconoscimento facciale di tipo *real time*, ma anche – e so-

“disposizioni penali”, ossia a quegli interventi riformatori che prevedono l'entrata in vigore di nuove “aggravanti” (vedasi, ad esempio, la circostanza aggravante comune sancita all'art. 61 comma 1 11-*undecies*, qualora il reato sia commesso mediante sistemi di intelligenza artificiale) ovvero di nuove fattispecie incriminatrici (ci si riferisce al delitto di «illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale» previsto e punito all'art. 612-*quater* c.p.).

⁷⁴ Come rilevato dal SERVIZIO STUDI DEL SENATO DELLA REPUBBLICA (*ivi*, p. 9) la legge n. 132 del 2025 muove «dalla consapevolezza della rivoluzione informatica che, dal secondo Novecento, ha assunto una incidenza sulla vita individuale e collettiva tale da configurare una ‘società digitale’, in cui la diffusione del personal computer, l'avvento di internet e degli smartphone, hanno dilatato l'impiego di strumenti digitali nella quotidianità. In questo contesto, l'evoluzione tecnologica fa sì che le ‘macchine’ dispongano ormai di margini di auto-apprendimento, auto-organizzazione, auto-decisione. Ne segue che si pone all'etica, al diritto, al dibattito pubblico il tema della ‘intelligenza artificiale’ e di una sua regolazione».

⁷⁵ Tra queste prescrizioni è doveroso richiamare il dettato dell'art. 3 comma 1 che stabilisce come «la ricerca, la sperimentazione, lo sviluppo, l'adozione, l'applicazione e l'utilizzo di sistemi e di modelli di intelligenza artificiale per finalità generali avvengono nel rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione, del diritto dell'Unione europea e dei principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità».

prattutto – allo scopo di approntare una disciplina specifica per i sistemi di intelligenza artificiale classificati “ad alto rischio”, come quelli di identificazione biometrica di tipo *ex post*.

6. Conclusioni

Viene da chiedersi se l’apporto tecnologico offerto dai *tools* giustifichi – in ultima analisi – un sacrificio (più o meno invasivo) delle libertà individuali e, quindi, una loro utilizzazione basata *sic et simpliciter* sulle norme codicistiche vigenti, ovvero se l’introduzione di tali applicativi risulti ancora prematura (e, pertanto, differibile) rispetto ad un archetipo di procedimento penale che, nei suoi necessari schematismi, abbisogna di interventi legislativi ponderati e mirati ai fini di una sua rimodulazione finalizzata sia ad accogliere tutte le potenziali novità che sembrerebbero offrire gli AFRS, sia a fronteggiarne le criticità.

Nel tentativo di rispondere a tale interrogativo, occorre preliminarmente constatare come ad oggi, sembrerebbe mancare una seria e concreta volontà di regolamentare in modo esaustivo l’impiego dei *devices* di riconoscimento facciale, al di là dell’insoddisfacente testo normativo cristallizzatosi nell’art. 9 d.l. n. 139 del 2021, oppure dell’embrionale dettato di cui alla legge n. 132 del 2025. Ciò appare desumibile, ad esempio, proprio considerando come la sospensione di cui all’art. 9 comma 9 del citato d.l. (originariamente fissata al 31 dicembre 2023), anziché essere sostituita da «una disciplina legislativa della materia», sia stata invece prorogata al 31 dicembre 2025 ⁷⁶.

In secondo luogo, nonostante le “spinte” europee ad enucleare una disciplina *ad hoc* sul tema dei sistemi di riconoscimento facciale, il legislatore è rimasto ancora pressoché in uno stato di inerzia, demandando *de facto* alle autorità amministrative l’arduo compito di scandagliare – all’interno dell’ordinamento italiano – un sostrato normativo estendibile anche all’ambito degli AFRS. Tale atteggiamento appare non solo poco rispettoso degli obblighi sovranazionali incombenti nei confronti dello Stato italiano, ma confligge altresì con i principi (anche costituzionali) in virtù dei quali non è consentito comprimere le libertà personali senza una precisa base giuridica.

Tra le ragioni di tale inerzia non si può sottacere come la tematica in esame, in guisa della sua spiccata complessità tecnica (derivante dalla compenetrazione di concetti scientifici e giuridici) ingeneri nei confronti

⁷⁶ Cfr. art. 9 comma 9 d.l. n. 139 del 2021.

dell'interprete non poche difficoltà ricognitive, che sovente si traducono in una scarsa comprensione del modo in cui il "mezzo informatico" operi e incida nelle dinamiche processuali. Questa scarsa comprensione potrebbe riverberarsi, conseguentemente, non soltanto in sede di dibattito legislativo, ma anche in seno all'opinione pubblica, così complicando la formazione di una "coscienza" – comune e condivisa – circa i benefici, le implicazioni e gli svantaggi scaturenti dall'applicazione degli AFRS.

Non è nemmeno da sottovalutare, inoltre, come questa inattività del legislatore potrebbe eventualmente discendere da una volontà (più o meno implicita) di aprire indiscriminatamente «al riconoscimento facciale di massa», sfruttando un'interpretazione particolarmente estensiva delle norme processual-penalistiche, giustificata da intento di prevenzione e di repressione della criminalità in luoghi pubblici e aperti al pubblico⁷⁷.

Ebbene, quali che siano, in concreto, le motivazioni, si auspica, dunque, che il legislatore prenda coscienza dell'impellente necessità di dotare l'ordinamento italiano di una disciplina che regoli, in sede procedimentale, l'utilizzo dei sistemi di riconoscimento facciale, affinché il processo non resti una monade, aliena dalla realtà tecnologica che la circonda, bensì possa beneficiare – attraverso un bilanciamento «dei rischi connessi all'uso dei dispositivi *de quibus* rispetto alla congrua tutela delle prerogative individuali» – delle straordinarie potenzialità che, per certo, il progresso scientifico-informatico saprà offrire al rito penale⁷⁸. D'altronde, «il progresso non può essere fermato, ma deve essere governato nel suo sviluppo; a tal fine è perciò, necessario realizzare un modello di processo penale tecnologicamente avanzato che tuteli le garanzie delle parti anche quando le stesse vengono declinate nei moderni territori digitali: questo deve essere il terreno di confronto, questo deve essere lo spirito profondo della *digital transformation* giudiziaria il cui futuro è solo nelle nostre mani, oggi più che mai»⁷⁹.

⁷⁷ J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, cit., p. 178.

⁷⁸ D. POLIDORO, *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale*, in *Arch. pen. (web)*, 2020, f. 3, p. 38.

⁷⁹ V. BOVE, R. PATSCOT, *Processo penale telematico: dalla fase emergenziale alla digital transformation della giustizia penale*, in *Ius*, 6 aprile 2021, p. 20.

IL RICONOSCIMENTO FACCIALE ALL'INTERNO DEL PROCESSO, TRA CONTORSIONI DEL SISTEMA E RICADUTE MANCATE

VALERIA BOSCO

SOMMARIO: 1. Il difficile inquadramento all'interno del sistema probatorio. – 2. Le analogie e le differenze con l'istituto della ricognizione *ex* art. 213 c.p.p. – 3. L'utilizzo dei risultati del riconoscimento tramite la perizia e la consulenza tecnica. – 4. Il vaglio preliminare ai fini del soddisfacimento dei criteri della prova scientifica. – 5. L'ammissibilità come prova atipica. – 6. Conclusioni.

1. *Il difficile inquadramento all'interno del sistema probatorio*

Considerate le molteplici potenzialità offerte dai sistemi di riconoscimento facciale, la questione che inevitabilmente si pone riguarda la possibilità di introdurre i dati da essi generati nel processo, verificando la praticabilità di incasellare gli strumenti di identificazione automatizzata all'interno del quadro normativo del sistema probatorio.

Innanzitutto - in ragione della complessità del tema - partendo da un'analisi "in negativo" e procedendo per esclusione, la circostanza che alla videoripresa manchi il presupposto rappresentato dal contenuto comunicativo rende non accessibile la strada dell'utilizzo, sia pure per analogia, della disciplina relativa alle intercettazioni¹.

¹ Cass., Sez. Un., 28 marzo 2006, Prisco, in *Riv. it. dir. e proc. pen.*, 2006, p. 1537; sul punto v. L. CAMALDO, *L.A. e investigazione penale predittiva*, in *Riv. it. dir. proc. pen.*, 2024, p. 249; J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.*, 2022, f. 3, p. 1081; M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in *Giurisprudenza penale, intelligenza artificiale e d etica del giudizio*, Giuffrè, Milano, 2021, p. 63 s.; ID., *Prove fondate sull'intelligenza artificiale e diritti fondamentali*, in *Dir. difesa*, 15 gennaio 2025; E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna*, Giappichelli, Torino, 2025, p. 240 s.; L. SAPONARO, *Le nuove frontiere tecnologiche dell'individuazione personale*, in *Arch. pen. (web)*, 2022, f. 1, p. 16.

Il riconoscimento facciale si configura infatti come un processo di raccolta, analisi e trattamento di dati biometrici, effettuato tramite sistemi di elaborazione automatica, che prescinde dall'attività comunicativa. Una metodologia che «si differenzia ontologicamente dalle intercettazioni, in quanto non implica l'invasione di uno spazio comunicativo privato, né presuppone l'acquisizione di informazioni attinenti alla sfera dialogica e relazionale dell'individuo»².

Analogamente, appare problematico anche il collocamento dei *facial recognition systems* all'interno della struttura della prova documentale.

Ad un primo esame, le videoriprese sembrerebbero poter essere ricondotte nell'ambito dello schema di cui all'art. 234 c.p.p., essendo consentita l'acquisizione di documenti, formati al di fuori del procedimento penale, «mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo». Un parametro dunque in grado di ricomprendere altresì il fotogramma di videoregistrazioni³, ossia l'immagine estratta dalla ripresa audiovisiva, quale rappresentazione di un contenuto conoscitivo incorporato su supporto digitale⁴.

Tuttavia, si tratterebbe di una ricostruzione che, oltre a costituire una forzatura del dato normativo⁵, non pare poter essere ulteriormente estesa «ad altre fattispecie ancora più invasive della “semplice” videoripresa»⁶. Il documento «in senso processuale viene generalmente inteso come un supporto materiale o digitale che riproduce un'informazione statica»⁷; diversamente, gli strumenti del riconoscimento facciale non si limitano a catturare e a registrare passivamente le immagini dei volti, ma operano at-

² E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 241.

³ Cass., Sez. Un., 28 marzo 2006, Prisco, cit.

⁴ W. NOCERINO, *Sulle modalità di acquisizione delle immagini provenienti dalle telecamere di videosorveglianza*, in *Cass. pen.*, 2024, p. 2422.

⁵ L. SAPONARO, *Le nuove frontiere tecnologica dell'individuazione personale*, cit., p. 15, rileva infatti come il nostro codice di rito non preveda «alcuna disciplina circa l'utilizzo delle immagini all'interno del procedimento penale, così il *modus* di ingresso e di valutazione delle stesse nella dinamica processuale è stato costruito nel tempo attraverso concordi pronunce giurisprudenziali che, utilizzando norme codicistiche affini, hanno legittimato l'uso dello strumento investigativo attribuendogli, in alcuni casi, anche valore probatorio». V., al riguardo, la sentenza *Prisco* (Cass., Sez. Un., 28 marzo 2006, Prisco, cit.), in base alla quale «le videoregistrazioni effettuate fuori dal procedimento possono essere introdotte nel processo come documenti e diventare quindi una prova documentale».

⁶ L. SAPONARO, *Le nuove frontiere tecnologica dell'individuazione personale*, cit., p. 16 s., ritiene che le immagini contenenti dati biometrici, in quanto idonee a identificare in maniera certa un individuo, meritino una disciplina *ad hoc* e non l'applicazione estensiva di un'interpretazione giurisprudenziale per legittimarne l'uso.

⁷ F. ZACCHE', *La prova documentale*, Giuffrè, Milano, 2012, p. 7 ss.; v. anche E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 241 s.

traverso procedure di trattamento ed analisi dei dati, capaci di produrre risultati autonomi, che «implicano un'elaborazione finalizzata a generare un esito identificativo immediato»⁸. Una differenza strutturale, un cambiamento ontologico, che li renderebbe più correttamente qualificabili come meccanismi di elaborazione dei dati; i loro prodotti non andrebbero pertanto intesi come semplici documenti in senso tradizionale, ossia quali mere rappresentazioni passive di fatti o informazioni⁹, essendo invece frutto di un' "estrazione" automatizzata.

Dalla logica propria della prova documentale emerge inoltre un ulteriore profilo di criticità legato all'individuazione della sede in cui viene determinato l'*output*, risultando difficile assicurare che la procedura del sistema di *facial recognition* venga interamente sviluppata fuori dal procedimento penale. Se è vero, infatti, che «le immagini poste a base del riconoscimento possono provenire da un contesto extra procedimentale, l'utilizzo dei sistemi – e il conseguente *match* di corrispondenza – avviene comunque, di regola, in uno scenario "pre-investigativo" o di indagine oppure di accertamento della responsabilità penale»¹⁰.

Pur alla luce delle limitazioni di cui sopra, va comunque valutata l'ammissibilità di altre forme di inquadramento, legate alle differenti forme di impiego, che, in ambito processuale, potrebbero essere perseguite attraverso detti sistemi.

In effetti, ci si confronta con meccanismi capaci di svolgere, oltre a un'attività di identificazione e riconoscimento delle persone, per determinare l'identità di un individuo «ossia rispettivamente stabilire chi sia il soggetto oppure se il soggetto sia esattamente chi dichiara di essere»¹¹, anche una funzione di categorizzazione, usata per dedurre dalle immagini del volto gli elementi distintivi dell'individuo, come il sesso, l'età o l'etnia¹², nonché di individuazione di possibili testimoni, persone offese ovvero indiziati.

⁸ E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 241.

⁹ E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 241.

¹⁰ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, Wolter Kluwer Cedam, Milano, 2025, p. 281.

¹¹ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 15.

¹² Cfr. A. MANGIARACINA, *Il riconoscimento facciale: nuove sfide nel processo penale*, in P. DI SIMONE-A. MANGIARACINA-L. PARLATO (a cura di), *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, 2023, Palermo University press, Palermo, p. 80

2. *Le analogie e le differenze con l'istituto della ricognizione ex art. 213 c.p.p.*

L'elaborazione algoritmica è difatti in grado - attraverso l'associazione di foto o video del volto di uno sconosciuto con un'immagine, contenuta in un *database*, di un soggetto le cui generalità sono già note - non solo di procedere ad una identificazione in modo rapido ed automatizzato, ma anche di conoscere in tempo reale se un certo individuo, «sospettato di aver compiuto (o di poter commettere) un reato, possa trovarsi in un determinato luogo, sottoposto a osservazione»¹³. Un risultato che sembrerebbe analogo a quello raggiunto, nel corso del dibattimento, dalla ricognizione *ex artt. 213 e seguenti c.p.p.*, vale a dire quel mezzo di prova «mediante il quale, a una persona che abbia percepito con i propri sensi un essere umano, si chiede di riconoscerlo individuandolo tra altri simili», che può essere disposto anche «quando occorre procedere al riconoscimento di cose (art. 215), voci, suoni o quanto altro può essere oggetto di percezione sensoriale (art. 216)»¹⁴.

La ricognizione, così come suggerisce l'etimologia del termine, è legata all'atto di identificare qualcosa o qualcuno già noto. L'essenza sta dunque nello stabilire un legame tra ciò che si presenta ad un individuo in un determinato momento e quanto già rientra nella sua sfera di conoscenza: «un paragone tra una percezione attuale e il ricordo d'una passata: chi la esegue è chiamato a dire se coincidano o differiscano»¹⁵. La struttura di tale prova è, infatti, costruita intorno a questi due passaggi ineludibili: la percezione, prima, e il riconoscimento, poi. Un mezzo che, proprio perché basato su un vissuto, un'esperienza personale impressa nella memoria, il cui ricordo può essere modificato o attenuato dal tempo, richiede una serie di garanzie¹⁶.

È pertanto necessaria una procedura articolata, volta ad assicurare un elevato livello di affidabilità e attendibilità a quanto emerge dalla ricognizione.

Alla luce di tale disciplina, va dunque verificato se l'individuazione ottenuta mediante il riconoscimento facciale automatico possa essere equiparata, a fini giuridici e probatori, a una forma di ricognizione.

¹³ J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Dir. pen. cont.*, 2020, f. 1, p. 232 s.

¹⁴ P. TONINI-C. CONTI, *Il diritto delle prove penali nel sistema accusatorio contemporaneo*, Giuffrè, Milano, 2025, p. 373. V. anche F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 217.

¹⁵ A. CAMON, *Le prove*, in A. CAMON-M. DANIELE-D. NEGRI-C. CESARI-M.L. BITONTO-P.P. PAULESU, *Fondamenti di procedura penale*, Wolters Kluwer Cedam, Milano 2025, p. 385.

¹⁶ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 135.

Data la fallibilità della memoria umana e la possibile distorsione del ricordo, si potrebbe ritenere il riconoscimento facciale una sorta di versione più evoluta e formalizzata, affidata non alla mente, ma al calcolo, non alla percezione sensoriale ma alla computazione¹⁷, ravvisando una certa similitudine tra le operazioni eseguite dalla macchina e i processi neurologici ed euristici propri dell'uomo.

In questo caso, gli strumenti di intelligenza artificiale, sottoposti a continue evoluzioni, grazie agli allenamenti e affinamenti progressivi dei sistemi informatici, certamente sopperiscono all'imperfezione della memoria umana, essendo il "ricordo" digitale non degradabile. Gli algoritmi passano in rassegna le immagini contenute nei *database* confrontandole e sovrapponendole con quella della persona da identificare, verificano la possibilità di determinare eventuali somiglianze, giungendo al risultato di *matching* in pochissimi secondi e in modo oggettivo, ancorché legato a un indice di probabilità di corrispondenza.

Eppure, da ciò che a prima vista potrebbe apparire come un punto di forza, scaturiscono effetti che mettono in rilievo profili di marcata debolezza. I meccanismi digitali di intelligenza artificiale non "ricordano" l'immagine come l'uomo. Mente e macchina non possono essere assimilati: l'essere umano interpreta, valuta e riconosce attraverso processi qualitativi, esperienziali e contestuali; la macchina elabora dati secondo regole predeterminate e criteri quantitativi matematici, geometrici e fisici. In ciò risiede la differenza sostanziale tra cognizione umana e computazione automatica. «Per risalire al dato ignoto (la corrispondenza o meno del volto) a partire da un dato noto (due o più immagini poste in comparazione) il cervello umano ricorre a meccanismi molto complessi e, in molti casi, ancora sconosciuti ma, indubbiamente, eterogenei rispetto a quelli della macchina»¹⁸. I *software* operano sulla base di modelli algebrici-matematici, che trasformano la immagini acquisite in informazioni digitali, sviluppate all'interno di modelli informatici secondo logiche computazionali¹⁹, prive di percezione e interpretazione diretta. Tali meccanismi non "colgono" la realtà, ma la traducono in dati numerici che vengono poi elaborati secondo algoritmi e schemi matematici. Nel riconoscimento delle immagini, il processo di analisi e classificazione automatica non si fonda su una per-

¹⁷ G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego come finalità investigative e probatorie*, in *Cass. pen.*, 2025, p. 645.

¹⁸ G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 647; nello stesso senso F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 222.

¹⁹ V. G. UBERTIS, *Processo penale telematico, intelligenza artificiale e costituzione*, in *Cass. pen.*, 2024, p. 439 ss.

cezione visiva in senso umano, ma sull'elaborazione di relazioni statistiche tra valori numerici associati a *pixel*²⁰.

Da un lato, nella ricognizione “tradizionale”, ci si basa sulla rilevazione sensoriale e sulla multidimensionalità della memoria umana (elementi del processo cognitivo della persona che possono comunque influenzarne l'esito); dall'altro, nei sistemi di riconoscimento facciale, fondati su algoritmi di intelligenza artificiale, l'operazione avviene tramite l'analisi automatica di dati generalmente bidimensionali siano essi riprese video o immagini statiche. I due sistemi non sembrano dunque assimilabili²¹. Nel *software* di identificazione, difatti, non trovano spazio il rigoroso protocollo formale e procedurale, le garanzie, il contraddittorio e la supervisione del giudice, che caratterizzano, invece, la ricognizione²².

Da tali differenze discendono, analogamente, anche errori di natura diversa. Quelli dell'uomo sono di origine psicologica, cognitiva ed emotiva e producono errori di percezione, di memoria, di interpretazione dovuti anche a fattori di stress²³. Nella macchina, per contro, dall'origine tecnica e statistica scaturiscono distorsioni derivanti dalla qualità dei dati (*garbage in, garbage out*)²⁴, *bias* algoritmici²⁵, errori di classificazione²⁶.

L'art. 213 c.p.p., come già evidenziato, è implicitamente modellato su

²⁰ Tali sistemi vengono progettati e addestrati attraverso l'utilizzo di enormi quantitativi di dati, immagini estratte da *database* di notevoli dimensioni, che consentono al modello di apprendere schemi (*pattern*) ricorrenti e di formulare probabili corrispondenze.

²¹ G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 647; v. anche F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 219.

²² Allo stesso modo e per le medesime ragioni, non è neppure possibile qualificare questa modalità come ricognizione atipica, a causa della mancanza delle coordinate fondamentali, costituite dalla percezione diretta e dal conseguente richiamo mnemonico, nonché della possibilità di calare il riconoscimento automatico all'interno dell'assetto di garanzie previsto dall'art. 213 c.p.p. Al riguardo v. F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 222 s., sottolinea che «non sono ammesse forme di forzatura delle disposizioni tali da poter inquadrare il riconoscimento in esame nella pur discussa categoria delle c.d. ricognizioni atipiche o informali»; così anche L. CAMALDO, *I.A. e investigazione penale predittiva*, cit., p. 249.

²³ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 135; su questo tema v. G. CECANESE, *Aspetti problematici e snodi interpretativi dell'individuazione di persone e di cose*, in *Arch. pen. (web)*, 2018, f. 1, p. 20.

²⁴ La qualità dell'*output* è direttamente dipendente dalla qualità dell'*input*, pertanto dati in entrata erronei, incompleti, inaccurati o non rappresentativi producono risultati errati.

²⁵ Sul punto v. M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale (web)*, 12 settembre 2022, p. 9; J. DELLA TORRE, *Novità dal Regno Unito*, cit., p. 233.

²⁶ Il modello in questo caso sbaglia a identificare a causa di limiti statistici o parametri inadeguati.

un meccanismo proprio dell'essere umano, ed è dunque teso a scongiurare unicamente gli errori ad esso imputabili.

D'altronde, in questa direzione, anche la sede in cui tale attività viene svolta è al riguardo indicativa: la ricognizione si colloca in dibattimento o nell'incidente probatorio, dinanzi al giudice, nel contraddittorio delle parti; mentre, il sistema automatico agisce fuori dal contesto processuale, essendo progettato per operare in spazi pubblici, consentendo il riconoscimento sia in tempo reale, mediante l'elaborazione immediata delle immagini, o *ex post*, tramite il confronto con le banche dati dei volti archiviati²⁷.

È, quindi, evidente che il riconoscimento digitale costituisca "altro", che necessita di un'apposita disciplina e, pertanto, di sistemi di validazione dell'algoritmo, controllo e verifica del risultato e di una gestione dell'errore dedicati²⁸.

3. *L'utilizzo dei risultati del riconoscimento tramite la perizia e la consulenza tecnica*

Il risultato che scaturisce dall'algoritmo non può essere traghettato nel processo neanche attraverso l'istituto della perizia o della consulenza tecnica. L'attività che conduce all'elaborazione delle immagini e alla formulazione della conclusione è svolta integralmente dalla macchina²⁹, nel senso che il sistema non si limita a fornire un supporto tecnico,

²⁷ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 222 s.

²⁸ In questa direzione v. J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 1093; W. NOCERINO, *Sulle modalità di acquisizione delle immagini*, cit., 2425; C. PALLANTE, *L'IA nel procedimento penale: tra riconoscimento facciale e finalità investigative*, in *Riv. dir. media*, 2025, f. 1, p. 89; L. SAPONARO, *Le nuove frontiere tecnologiche dell'individuazione personale*, cit., p. 17; A. SCALEATI, *IA e processo penale: prospettive d'impiego e livelli di rischio*, in *Proc. pen. giust.*, 2024, p. 1408 s.; M. TORRE, *Il Regolamento europeo sull'intelligenza artificiale: i profili processuali*, in *Proc. pen. giust.*, 2024, f. 6, p. 1544. Diversamente, F. DI MATTEO, *La riservatezza dei dati biometrici nello Spazio europeo dei diritti fondamentali: sui limiti all'utilizzo delle tecnologie di riconoscimento facciale*, in *Freedom, Security & Justice: European Legal Studies*, 2023, f. 1, p. 110, reputa che «una normativa specificamente dedicata alle tecnologie di riconoscimento facciale, tanto reclamata dagli attivisti dei diritti umani nella speranza di vederne affermato il divieto di utilizzo, non solo non sia necessaria, ma al contrario potrebbe risultare funzionale proprio a chi si prefigge l'obiettivo di sfruttare economicamente i benefici che tale tecnologia, rientrando nella famiglia dell'artificial intelligence, può comportare. Non vi è dubbio, pertanto, che *iure condito* le *facial recognition technologies* trovino già una precisa, e stringente, regolamentazione; e che, a ben vedere, ogni ulteriore disciplina di cui si auspica l'adozione correrebbe il rischio di creare un diritto particolare per tali tecniche rispetto ad altre tecnologie già sperimentate, parimenti idonee a ledere la vita privata dei consociati».

²⁹ G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 649.

ma realizza autonomamente l'intero percorso che a partire dalle immagini disponibili conduce alla determinazione del *matching* più attendibile.

Indubbiamente, l'analisi degli esiti prodotti dalla macchina può essere oggetto di valutazione, ma si tratta di qualcosa di diverso, che rientra in una sorta di verifica degli *output* scaturiti dai sistemi automatici di riconoscimento: un «ausilio alla comprensione e alla “lettura” del risultato offerto dal *software*»³⁰.

Un'attività svolta da soggetti che operano in qualità di periti o consulenti tecnici: professionisti dotati di competenze specialistiche, incaricati di analizzare e interpretare gli esiti dell'elaborazione algoritmica secondo protocolli metodologici verificabili. Un'azione, dunque, distinta dal riconoscimento automatico, ma ad esso collegata al fine di offrire supporto alla validazione dell'*output* fornito dalla macchina.

Il contributo dell'operatore “umano” è peraltro, già presente all'interno di tale procedura. Elemento imprescindibile, indispensabile allo scopo di sottoporre immediatamente a controllo il risultato prodotto dal sistema, potendolo approvare e ratificare ovvero renderlo nullo, dimostrandone l'erroneità³¹.

Si tratta, tuttavia, di un apporto necessario, ma non del tutto risolutivo, in quanto non in grado di coprire compiutamente le “falle” della macchina, dal momento che non consente di intervenire sugli esiti di esclusione e di eliminare il rischio del “falso negativo”³². Tutto ciò che viene scartato dall'algoritmo risulta infatti definitivamente perduto. Ne consegue che il controllo umano può solo intervenire ed operare all'interno delle corrispondenze positive.

4. *Il vaglio preliminare ai fini del soddisfacimento dei criteri della prova scientifica*

Il sistema del riconoscimento facciale, il cui funzionamento è governato da algoritmi di intelligenza artificiale fondati su meccanismi di *machine learning*, e non tradizionalmente procedurali (in base alla sequenza dell'*if-then-else*), richiede che tali tecnologie siano sottoposte al controllo relativo alla validità scientifica, rendendosi necessario accertare se l'identificazione compiuta dai meccanismi automatici soddisfi i requisiti della prova

³⁰ G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 649.

³¹ Nel SARI *Enterprise* infatti è l'operatore umano che ha il compito di controllare l'output del *software* che restituisce una serie di possibili accoppiamenti (*matching*) tra l'immagine in verifica e quelle già presenti in banca dati, unitamente a una percentuale di corrispondenza.

³² G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 649 s.

scientifica³³. Ciò che si ricerca infatti è un esame rigoroso della loro attendibilità, ripetibilità, affidabilità e verificabilità secondo criteri scientificamente accreditati.

Un passaggio, questo, che si intreccia con quello della dimostrazione dell'idoneità di simili sistemi all'accertamento del fatto di cui all'art. 189 c.p.p.³⁴.

È evidente che il mero impiego delle tecnologie moderne non è sinonimo di garanzia di scientificità della prova. L'uso di strumenti avanzati non implica automaticamente che il metodo adottato soddisfi i requisiti di rigore richiesti affinché un risultato possa dirsi scientificamente fondato. L'esigenza è infatti quella di preservare il processo dalla c.d. "scienza spazzatura" (*junk science*)³⁵.

Il giudice deve pertanto intervenire al fine di accertare la credibilità in senso ampio delle nuove tecnologie, dovendo darne riscontro, non in sede di valutazione, al termine del giudizio, bensì in fase di ammissione delle prove.

A questo scopo, i principali criteri operativi e interpretativi cui fa riferimento la giurisprudenza internazionale, inclusa quella italiana³⁶, trovano fondamento nella giurisprudenza statunitense, che ha dapprima tracciato l'orientamento con la sentenza *Frye* e lo ha poi affinato e consolidato con la sentenza *Daubert*³⁷.

³³ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 243; sul punto v. E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 228 s.

³⁴ G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 650; O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, 2005, p. 102 e p. 207; per G. UBERTIS, *La prova scientifica e la nottola di Minerva*, in L. DE CATALDO NEUBURGER (a cura di), *La prova scientifica nel processo penale*, Cedam, Milano, 2017, p. 83 s., l'art. 189 c.p.p. si potrebbe applicare solo per le prove che non possono essere ricomprese nella perizia o nell'esperimento giudiziale o in un'altra prova tipica; sul punto v. A. CAMON, *Le prove*, cit., p. 336 s.

³⁵ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 245; G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 650. V., sul tema, C. CONTI, *Scienza controversa e processo penale: la Cassazione e il "discorso sul metodo"*, in *Dir. proc. pen.*, 2019, p. 848 ss.

³⁶ Criteri che sono stati recepiti dalla giurisprudenza italiana da Cass., Sez. IV, 17 settembre 2010, n. 43786, Cozzini, in *C.e.d.*, n. 248943; fra le molte pronunce successive v. Cass., Sez. IV, 16 novembre 2018, De Santis, in *C.e.d.*, n. 274831; Cass., Sez. IV, 15 maggio 2018, Beduschi, in *C.e.d.*, n. 274272; Cass., Sez. IV, 3 novembre 2016, Bordogna, in *C.e.d.*, n. 270385;

Cass., Sez. IV, 29 gennaio 2013, Cantore, in *Giust. pen.*, 2013, p. 695. In dottrina v. P. TONINI, *La Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza*, in *Dir. pen. proc.*, 2011, p. 1341.

³⁷ Court of Appeals of District of Columbia, 3 dicembre 1923, n. 293, *Frye v. United States* e Supreme Court of the United States, 28 giugno 1993, *Daubert e a. v. Merrel Dow Pharmaceuticals*. Sul punto v. L. ALGERI, *La prova neuroscientifica nel processo penale*, Cedam,

L'organo giudicante, non potendo chiaramente assumere il ruolo dello scienziato, non è in grado di decretare ciò che può rientrare nel dominio riconosciuto della scienza, trattandosi di un giudizio che appartiene esclusivamente alla comunità scientifica. Il suo compito è, però, quello di saper valutare se lo strumento utilizzato sia qualificabile come scientificamente valido³⁸. Di conseguenza, non può limitarsi ad essere un mero destinatario passivo del sapere scientifico³⁹, ma ha l'onere di vagliare l'affidabilità del risultato delle nuove tecnologie nel contesto probatorio, affinché tale prodotto possa legittimamente concorrere alla formazione del convincimento giudiziale.

Il giudice diviene così «il guardiano (gatekeeper) del metodo»: colui «che previene l'introduzione nel processo della cosiddetta scienza spazzatura»⁴⁰.

Il pericolo principale che si deve scongiurare è infatti quello di conferire al risultato algoritmico un valore determinante, riconoscendo all'esito fornito dal sistema automatico «un'implicita affidabilità», non perché effettivamente verificata, ma in ragione di una sorta di «autorità tecnica» tacitamente delegata allo strumento tecnologico. I dati elaborati digitalmente rischiano così di «vedersi attribuita una patente di intrinseca attendibilità probatoria, semplicemente perché la verifica dell'iter che li ha generati è troppo complessa o sfugge, almeno in parte, ad un controllo *ex post*»⁴¹. In modo inconscio e irrazionale, la tentazione è dunque quella di

Milano, 2020, p. 16 ss.; M. CECCHI, *Il giudice dinanzi alla prova scientifica*, in *Arch. pen. (web)*, 2022, f. 1, p. 9; C. CONTI, *Scienza controversa e processo penale*, cit., p. 848 ss.; G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 652; M. MOTISI, *Luci ed ombre della prova scientifica nel processo penale*, in P. DI SIMONE-A. MANGIARACINA-L. PARLATO (a cura di), *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, cit., p. 136 s.; G. GENNARI, *I criteri di ammissione della prova scientifica nel contesto internazionale*, in di G. CANZIO-L. LUPARIA DONATI (a cura di), *Prova scientifica e processo penale*, Cedam, Milano, 2022, p. 157 ss.

³⁸ G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 652; v. anche M. BARGIS, *Note in tema di prova scientifica nel processo penale*, in *Riv. dir. proc.*, 2011, p. 51.

³⁹ L. ALGERI, *La prova neuroscientifica nel processo penale*, cit., p. 20; E. DE PAOLIS, *Prova scientifica e scorciatoie cognitive*, in *Arch. pen. (web)*, 2025, f. 1, p. 10; O. DOMINIONI, *L'esperienza italiana di impiego della prova scientifica nel processo penale*, in *Dir. pen. proc.*, 2015, p. 601 ss.; G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 651; L. LUPARIA DONATI, *La promessa della giustizia tecnologica*, in *Sistema penale (web)*, 1° agosto 2024, p. 7; M. MOTISI, *Luci ed ombre della prova scientifica nel processo penale*, cit., p. 136 s.

⁴⁰ G. UBERTI, *Prova scientifica e processo penale*, in *Riv. it. dir. proc. pen.*, 2016, p. 1202; v. anche G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 651.

⁴¹ S. QUATTROCOLO, *Prova e intelligenza artificiale*, in C. CONTI-A. MARANDOLA (a cura di), *La prova scientifica*, Giuffrè, Milano, 2023, p. 484; per F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 266, occorre «rifuggire da ogni forma di “deresponsabilizzazione” del giudice penale, il quale deve necessariamente mantenere capacità critica e autonomo razionamento che gli consenta di dissentire rispetto al parere espresso dalla macchina e non appiattirsi sul verdetto emesso dalla stessa». Sul tema v. anche L. LUPARIA DONATI,

affidarsi ciecamente alle nuove tecnologie, «ritenute oggettive e meritevoli di fiducia per il solo fatto di ... essere tecnologie»⁴².

Allo stato, però, l'unico dato oggettivo risiede nell' "assoluta incertezza" che regna sui sistemi di riconoscimento automatico. Le procedure sono infatti avvolte da un'opacità generalizzata⁴³ che non permette a tali metodi di essere equiparati ad una prova scientifica.

Pur essendo oramai trascorsi diversi anni dall'introduzione dei software di *facial recognition*, questi risultano ancora privi delle informazioni essenziali per comprendere il loro funzionamento e, dunque, valutarne la concreta attendibilità⁴⁴.

Assodato il loro incardinamento all'interno dei processi di apprendimento automatico propri degli applicativi di intelligenza artificiale, permanente, infatti, il limite rappresentato dall'impossibilità di conoscere e verificare la struttura operativa. I meccanismi algoritmici utilizzati non sono pienamente accessibili, essendo coperti dal segreto industriale⁴⁵, né risultano disponibili le specifiche progettuali riguardanti gli elementi costitutivi, la grandezza dei *dataset*, la qualità delle immagini impiegate e gli esiti

Intelligenza artificiale e libero convincimento del giudice, in G. CANZIO-L. LUPARIA DONATI (a cura di), *Prova scientifica e processo penale*, Cedam, Milano, 2022, p. 944.

⁴² P. COMOGGIO, *Prefazione*, in J. NIEVA-FENOLL, *Intelligenza artificiale e processo*, Giappichelli, Torino, 2019, p. X-XI; v. anche C. CESARI, *Editoriale: l'impatto delle nuove tecnologie sulla giustizia penale - un orizzonte denso di incognite* in *Rev. brasileira de direito processual penal*, 2019, p. 1167; G. RICCIO, *Ragionando su intelligenza artificiale e processo penale*, in *Arch. pen. (web)*, 2019, f. 3, p. 8; F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 139; L. LUPARIA DONATI, *La promessa della giustizia tecnologica*, cit., p. 2.

⁴³ Sul c.d. fenomeno dell' "opacità algoritmica" v. L. ALGERI-M. TORRE, *Aspetti definitori e delimitazione della materia*, in G. BACCARI- P. FELICIONI (a cura di), *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, Giuffrè, Milano, 2023, p. 104 ; J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 1082 ss.; G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 652 s.; L. LUPARIA DONATI, *Intelligenza artificiale e libero convincimento del giudice*, cit., p. 944; A. MARANDOLA, *Il riconoscimento facciale*, in C. CONTI-A. MARANDOLA (a cura di), *La prova scientifica*, cit., p. 511 ss.; C. PALLANTE, *L'LA nel procedimento penale*, cit., p. 77; M. TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. proc.*, 2021, f. 8, p. 1053 ss.

⁴⁴ Così J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, in G. DI PAOLO-L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Editoriale scientifica, Trento, 2022, p. 38; E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 231, evidenzia che, nonostante il SARI sia operativo in Italia da circa sette anni, solo di recente e in seguito ad alcune sollecitazioni, sono state rese pubbliche informazioni ufficiali in merito all'incidenza percentuale delle comparazioni effettuate con successo mediante tale tecnologia.

⁴⁵ A. BALSAMO, *L'impatto dell'intelligenza artificiale nel settore della giustizia*, in *Sistema penale (web)*, 22 maggio 2024, p. 13, afferma che, quando un siffatto strumento sia impiegato da autorità giudiziarie in un processo penale, non dovrebbe essere mai consentito opporre il segreto industriale sui dati, che integrano il c.d. codice sorgente.

della validazione dell'algoritmo, quali, in particolare, il tasso di errore relativo ai falsi positivi e negativi⁴⁶.

A fronte di un nucleo essenziale avvolto nell'incertezza, è invece nota, pur se non in maniera pienamente dettagliata, la significativa fallibilità dell'algoritmo, capace anche di gravi rischi discriminatori⁴⁷, che nella maggior parte dei casi vanno a scapito delle minoranze etniche⁴⁸. Errori che spesso scaturiscono dall'inadeguatezza dei dati immessi in fase di istruzione del sistema e dai pregiudizi che l'uomo, anche inavvertitamente, può introdurre nel processo di programmazione, che possono appunto determinare varie forme di *bias*⁴⁹.

Al riguardo, appare pertanto fondamentale che i risultati, gli *output* del *software*, vengano dimostrati attraverso un processo di *reverse engineering* o, comunque, spiegati nella loro correlazione con gli *input*. Un'operazione logica e razionale di ricostruzione puntuale del percorso seguito dal sistema, che tuttavia, paradossalmente anche gli stessi sviluppatori potrebbero non essere in grado di svolgere. Nei processi algoritmici fondati sull'ap-

⁴⁶ Su questi aspetti, v. L. CAMALDO, *L.A. e investigazione penale predittiva*, cit., p. 249; M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali*, cit., p. 9; J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, cit., 38 s.; G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 653; M. GIALUZ, *Prove fondate sull'intelligenza artificiale e diritti fondamentali*, cit.; Id., *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., p. 64 s.; R. LOPEZ, *La rappresentazione facciale tramite software*, in A. SCALFATI (a cura di), *Le indagini atipiche*, 2^a ed., Giappichelli, Torino, 2019, p. 244; C. PALLANTE, *L'LA nel procedimento penale*, cit., p. 67.

⁴⁷ E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Dir. pen. uomo*, 2021, p. 15 s.; J. DELLA TORRE, *Novità dal Regno Unito*, cit., p. 233; E. SACCHETTO, *Spunti per una riflessione sul rapporto tra biometria e processo penale*, in *Dir. pen. cont.*, 2019, f. 2, p. 471. Per un approfondimento v. A. MANGIARACINA, *Il riconoscimento facciale*, cit., p. 78 s.

⁴⁸ Studi del Massachusetts Institute of Technology (v. J. BUOLAMWINI, *Gender Shades study*, in *MIT Technology Review*, 2018) hanno dimostrato che le donne afroamericane hanno tassi di errore fino al 34,7%, contro lo 0,8% degli uomini bianchi. Questo significa che per ogni tre donne nere analizzate, una viene identificata erroneamente. In particolare, in relazione alla vicenda relativa all'impiego dell'applicativo COMPAS (*Correctional offender management profiling for alternative sanctions*), si è accertato che gli imputati neri avevano molte più probabilità degli imputati bianchi di essere erroneamente giudicati a più alto rischio di recidiva. V anche G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 653; S. DEL GATTO, *La governance delle nuove tecnologie tra tentativi di regolazione e istanze di self regulation. Il caso del riconoscimento facciale*, in *Riv. it. dir. pubbl. comunit.*, 2023, p. 48; M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Dir. pen. cont.(web)*, 29 maggio 2019, p. 7 e ss.

⁴⁹ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 136-139; J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, cit., p. 7; Id., *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 1067; G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, Napoli, 2021, p. 219; M. TORRE, *Nuove tecnologie e trattamento dei dati personali*, cit., p. 1053 s.

prendimento automatico (*machine learning*), il modello evolve attraverso lo sviluppo di catene decisionali, che si modificano continuamente in base alle scelte precedenti. Diviene dunque estremamente arduo per i programmatori ricomporre la sequenza logica del “ragionamento”, che a partire dai dati di *input* conduce alla produzione del *match*, con inevitabili ricadute in termini di verificabilità e controllo. L'oscurità e la non percorribilità a ritroso del funzionamento di taluni meccanismi pregiudica irrimediabilmente il diritto alla tutela giurisdizionale, dato che «il soggetto non può contestare ciò che non conosce»⁵⁰.

Questa manifesta opacità strutturale riconduce il riconoscimento facciale nell'alveo delle c.d. “scatole nere”, quali meccanismi caratterizzati da una generale inaccessibilità⁵¹. Un aspetto che solleva non poche preoccupazioni riguardo alla trasparenza e alla giustificazione dei prodotti ottenuti⁵², impedendo qualsiasi forma di controllo sull'affidabilità del risultato con inevitabili ricadute sotto il profilo del diritto di difesa e del principio del contraddittorio⁵³.

⁵⁰ E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, cit., p. 13.

⁵¹ G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 668; nello stesso senso L. LUPARIA DONATI, *La promessa della giustizia tecnologica*, cit., p. 4; per R.E. KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale*, in *Cass. pen.*, 2024, p. 203, «sono sistemi ai quali bisogna accostarsi con una massiccia dose di fideismo, rilevando che funzionano, ma non è dato sapere come e perché, non essendo controllabile il percorso attraverso il quale hanno portato ad un certo risultato».

⁵² G. TESSITORE, *Riconoscimento automatico del volto e confronto in ambito forense*, in P. DI SIMONE-A. MANGIARACINA-L. PARLATO, *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, cit., p. 75; in senso analogo, J. DELLA TORRE, *Quale spazio per ridursi di riconoscimento facciale nella giustizia penale?*, cit., p. 41; al riguardo, F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 243, parla di «black box» inespugnabili che non permette di verificare la controllabilità e la falsificabilità della teoria seguita né di individuare con precisione il tasso di errore della stessa neppure sottoporla ad un controllo da parte della comunità scientifica di riferimento».

⁵³ A. BALSAMO, *L'impatto dell'intelligenza artificiale nel settore della giustizia*, in *Sistema penale (web)*, 22 maggio 2024, p. 13; F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 277; E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 229 s.; L. LUPARIA DONATI, *La promessa della giustizia tecnologica*, cit., p. 4, evidenzia che la tecnologia «rosicchia costantemente margini di difesa all'interno dell'agone processuale, erodendo i più classici *rights of defence*»; R. COLUCCINI - A. GIANNINI - L. SOTTILE, *Il Viminale ci tiene all'oscuro su come e quanto usa il sistema di riconoscimento facciale*, <https://irpimedia.irpi.eu/sorveglianza-viminale-riconoscimento-facciale-trasparenza>, 2024 rilevano che «senza una normativa *ad hoc* c'è il rischio che i risultati forniti da Sari finiscano per condizionare l'individuazione di un sospettato già nella primordiale fase di indagini, per poi successivamente ricevere la conferma in dibattimento senza che la difesa possa interloquire sul punto. Sono quindi necessarie tutele adeguate rispetto ai rischi collegati all'utilizzo di tali tecnologie e al trattamento dei dati biometrici. Ribattere a Sari è infatti impossibile, visto che non se conosce il funzionamento e il modo in cui identifica le somiglianze».

In sintesi, i sistemi di riconoscimento facciale attualmente esistenti sono nell'impossibilità di fornire le evidenze richieste dalla comunità scientifica di riferimento. Considerato infatti che non si conoscono ancora le reali modalità di funzionamento il vaglio di "scientificità" risulta, almeno per ora, insuperabile⁵⁴.

5. *L'ammissibilità come prova atipica*

A completamento dell'analisi in esame occorre verificare se il contributo conoscitivo derivante dall'individuazione effettuata mediante sistemi automatici possa comunque trovare ingresso nel processo attraverso il varco costituito dalla disciplina della prova atipica⁵⁵ ex art. 189 c.p.p.⁵⁶.

Com'è noto, il sistema probatorio previsto dal codice di procedura penale non configura un catalogo chiuso di mezzi di prova, rendendo così possibile un'apertura verso le nuove tecnologie. È pertanto necessario interrogarsi se, anche nel caso del *facial recognition*, possa essere utilizzata quella «porta spalancata sul futuro»⁵⁷, concepita proprio per accogliere le prove che derivano dagli sviluppi del progresso scientifico⁵⁸.

In questi casi, però, al giudice dibattimentale viene richiesta una valutazione preliminare di ammissibilità «necessariamente più ampia e del tutto originale rispetto a quella attivata dalla richiesta di assumere una

⁵⁴ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 247; così anche E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, cit., p. 21; G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 652; G. TESSITORE, *Riconoscimento automatico del volto e confronto in ambito forense*, cit., p. 70; R.V.O. VALLI, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, in *Il penalista*, 16 gennaio 2019.

⁵⁵ Sul concetto di prova atipica v. P. TONINI-C. CONTI, *Il diritto delle prove penali*, cit., p. 163.

⁵⁶ Sul tema v. G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *Leg. pen. (web)*, 11 dicembre 2021, p. 9 ss.; G. CANZIO, *AI act e processo penale: sfide e opportunità*, in *Sistema penale (web)*, 14 ottobre 2024, p. 10; S. DE FLAMMINEIS, *Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale*, in *Sistema penale (web)*, 8 marzo 2024, p. 21; J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 1082 ss.; M. TORRE, *Nuove tecnologie e trattamento dei dati personali*, cit., p. 1052; P. FERRUA, *Ammissibilità della prova e divieti probatori*, in *Rev. bras. de direito processual penal*, 2021, f. 1, p. 228; A. MARANDOLA, *Il riconoscimento facciale*, cit., p. 511 ss.; C. PALLANTE, *L'IA nel procedimento penale*, cit., p. 77; A. SCALFATI, *IA e processo penale: prospettive d'impiego e livelli di rischio*, cit., p. 1408.

⁵⁷ A. CAMON, *Le prove*, cit., p. 336.

⁵⁸ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 270, sottolinea come si tratti di «un canale "ad apertura controllata" che deve rispettare i requisiti di cui all'art. 189 c.p.p.».

prova prevista dalla legge processuale»⁵⁹. Al riguardo, infatti, i consueti presupposti costituiti dall'assenza di divieti (e dalla non manifesta superfluità e irrilevanza) vanno analizzati in maniera ancora più puntuale: la prova atipica non deve porsi «in contrasto né con le regole processuali né con il diritto sostanziale, sia esso di fonte primaria o addirittura costituzionale»⁶⁰, nel senso che, come sottolineato dalla giurisprudenza, «non può considerarsi “non disciplinata dalla legge” la prova basata su un'attività che la legge vieta»⁶¹. Il divieto legale in questo caso non va rinvenuto all'interno della disciplina del processo penale, ma va necessariamente coordinato con gli eventuali divieti stabiliti in altri settori dell'ordinamento⁶².

Oltre alle condizioni di cui sopra, l'art. 189 c.p.p. prevede tre ulteriori parametri strutturati secondo una progressione logica: la prova deve essere idonea all'accertamento del fatto; non deve pregiudicare la libertà morale della persona e deve essere garantita la necessità di sentire le parti in merito alle modalità di acquisizione.

Per quanto riguarda il primo criterio, i profili di opacità e fallibilità precedentemente evidenziati non possono non avere una ricaduta immediata sull'art. 189 c.p.p. Ai fini dell'accertamento del fatto si richiede che il mezzo di prova sia tecnicamente affidabile, controllabile e verificabile nelle sue procedure di funzionamento. Tuttavia, a causa dell'assenza di trasparenza e ripercorribilità i sistemi di riconoscimento facciale rischiano, almeno per ora, di non essere in grado di superare il vaglio di ammissibilità⁶³.

Chiaro, infatti, che si tratta di una valutazione riferita all'immediato

⁵⁹ G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 660.

⁶⁰ G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 660; v. anche F.R. DINACCI, *Sequestro di dispositivi informatici: in posizioni tecnologiche e scelte interpretative alla ricerca di un recupero della legalità probatoria*, in *Arch. pen. (web)*, 2025, f. 1, p. 13.

⁶¹ Cass., Sez. un., 28 marzo 2006, n. 26795, Prisco, cit.

⁶² M.L. DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni unite*, in *Cass. pen.*, 2006, p. 3960; v. anche G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 660.

⁶³ Una conclusione condivisa dalla dottrina, v. G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale*, cit., p. 10; L. CAMALDO, *I.A. e investigazione penale predittiva*, cit., p. 247; E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, cit., p. 21; F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 272; J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 1062; ID., *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, cit., p. 37 s.; G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 654; M. GIALUZ, *Prove fondate sull'intelligenza artificiale e diritti fondamentali*, cit.; ID., *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., p. 64; C. PALLANTE, *L'IA nel procedimento penale*, cit., p. 77 s.; E. SACCHETTO, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *Leg. pen. (web)*, 16 ottobre 2020, p. 10 ss.; M. TORRE, *Nuove tecnologie e trattamento dei dati personali*, cit., p. 1053.

presente, in quanto sicuramente in futuro l'evoluzione tecnologica e lo sviluppo dei modelli algoritmici porterà a un progressivo miglioramento in termini di efficacia dei sistemi di *facial recognition*, riducendo il margine di errore, collegato in particolare ai *bias* discriminatori originati dal metodo di progettazione, selezione dei dati e addestramento del sistema⁶⁴.

Quanto al rispetto della libertà morale, il prelievo dell'immagine potrebbe apparentemente presentarsi come un atto privo di intrusività, qualcosa di innocuo: avviene infatti in modo occulto, e, pur in presenza della consapevolezza di trovarsi in un'area videosorvegliata, non richiede nessuna modalità di collaborazione, né l'adozione di comportamenti attivi⁶⁵. A differenza di altri metodi di identificazione biometrica, quale per esempio quello basato sul DNA, il riconoscimento facciale ha il vantaggio di non essere invasivo, non determinando alcuna forma di coazione fisica diretta sulle persone⁶⁶. Peraltro, la ripresa facciale costituisce un'operazione agevolmente conseguibile: «il volto è facile da osservare e da 'acquisire' sia nello spazio fisico (ad esempio, mediante le videocamere di sorveglianza installate soprattutto negli spazi pubblici) sia in quello digitale (pensiamo alle immagini caricate sui diversi social network)»⁶⁷.

Eppure, proprio nel fatto di mostrarsi come “formalmente neutro” sul piano dell' “impatto” verso l'individuo va ravvisato il profilo di maggiore pericolosità. L'assenza di un'interazione diretta con il soggetto e di una percezione immediata dell'ingerenza rende tale strumento qualcosa da cui difficilmente ci si può difendere. Un mezzo silente, poco visibile, non controllabile, e di conseguenza maggiormente lesivo dei diritti fondamentali. «Senza richiedere il “consenso” del prevenuto, durante il processo penale l'autorità può essere in grado di “apprendere” dati (peraltro ca-

⁶⁴ Tuttavia, la presenza di altri fattori, quali l'angolazione di ripresa, il grado di inclinazione del volto, il livello di illuminazione, la risoluzione dell'immagine, come pure il “rumore” causato da ulteriori variabili, agenti nel contesto in cui viene compiuto il riconoscimento (come per esempio i cambiamenti nel look, l'uso del trucco e della barba, le caratteristiche dell'acconciatura, l'utilizzo di occhiali, mascherine o altri accessori) costituiscono criticità difficilmente eliminabili. Si ritiene, pertanto, che tali elementi, andranno comunque ad incidere in modo significativo sull'affidabilità del risultato, che avrà scarse probabilità di condurre alla identificazione univoca del soggetto.

⁶⁵ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 273 s.

⁶⁶ A. MANGIARACINA, *Il riconoscimento facciale*, cit., p. 78; E. SACCHETTO, *Face to face*, cit., p. 1 s.; v. anche G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale*, cit., p. 3.

⁶⁷ A. MANGIARACINA, *Il riconoscimento facciale*, cit., p. 78; d'altronde sottolinea E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 261, come al contempo, queste caratteristiche rappresentino «un importante vantaggio operativo per le autorità, poiché consente l'acquisizione dei dati senza la necessità di procedure complesse o di un'interazione diretta con gli individui monitorati, ottimizzando così l'efficienza delle fasi di raccolta e di analisi delle informazioni».

paci, in ipotesi, di valere quali ammissioni di responsabilità) che sono parte della sfera individuale del singolo e la cui acquisizione si potrebbe sostenere dover essere subordinata all'esercizio della libertà morale della persona»⁶⁸.

I diritti che rischiano di essere violati, o comunque limitati, dall'utilizzo delle tecnologie di riconoscimento facciale sono infatti plurimi coinvolgendo, oltre al diritto alla riservatezza, alla protezione dei dati personali, il diritto al rispetto della vita privata e familiare (la raccolta e l'analisi delle immagini incidono sulla sfera privata), il diritto alla dignità delle persona (l'uso non controllato e opaco di tecnologie di sorveglianza di massa può ridurre l'individuo a mero oggetto di analisi tecnica), il diritto a non subire discriminazioni, nonché il godimento delle altre libertà fondamentali riconosciute dalla Carta costituzionale e dalle Carte internazionali poste a protezione dei diritti individuali (artt. 2, 3, 13 e 117 Cost., art. 8 Conv. e.d.u., artt. 7 e 8 Carta dir. fond. UE)⁶⁹.

Ne consegue, che l'esito generato dai sistemi di *facial recognition* non può essere considerato alla stregua di un'attività probatoria atipica, non solo a causa dell' "inidoneità" dello strumento ad accertare i fatti⁷⁰, ma anche perché sussiste un ulteriore e invalicabile ostacolo costituito dalla lesività dei diritti fondamentali della persona⁷¹.

Basti pensare come dall'utilizzo del Sari *Real time* discenda il controllo di tutti gli individui presenti nel luogo di ricerca, portando alla degenerazione del controllo di massa⁷². Tale modalità è difatti in grado di imma-

⁶⁸ L. LUPARIA DONATI, *Privacy, diritti della persona e processo penale*, in *Riv. dir. proc.*, 2019, p. 1464.

⁶⁹ Su questo tema v., tra i molti, E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, cit., p. 10 ss.; L. LUPARIA DONATI, *Privacy, diritti della persona e processo penale*, cit., p. 1448 ss.; J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 1068 ss.; F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 277; F. DI MATTEO, *La riservatezza dei dati biometrici nello Spazio europeo dei diritti fondamentali*, cit., p. 80 ss.; GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 660; M. GIALUZ, *Prove fondate sull'intelligenza artificiale e diritti fondamentali*, cit.; ID., *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., p. 64; A. MARANDOLA, *Il riconoscimento facciale*, cit., p. 509 ss.; M. PISATI, *Indagini penali e intelligenza artificiale: efficienza e rischi per i diritti fondamentali*, in *Proc. pen. e just.*, 2020, p. 962 s.

⁷⁰ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 278.

⁷¹ E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, cit., p. 24, evidenzia come i rischi connessi all'uso di tali tecnologie rispetto ai diritti fondamentali siano stati avvertiti anche nel contesto del mercato, intimorendo alcuni colossi americani, come Amazon, IBM e Microsoft, che, dati gli errori e le problematiche relative al diritto alla *privacy*, al principio di non discriminazione e alla libertà di espressione, hanno deciso di sospendere la commercializzazione dei sistemi di FRT.

⁷² V. G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale*, cit., p. 4 s.; G.

gazzinare informazioni relative ad «un numero indeterminato di soggetti ... spesso estranei all'attività di indagine»⁷³. La preoccupazione di essere esposto al trattamento biometrico da parte dei *tools* di intelligenza artificiale e di essere costantemente monitorato e tracciato dalle autorità statali induce indubbiamente il soggetto a modificare le proprie abitudini, auto-limitandosi nell'esercizio dei diritti fondamentali, come ad esempio la libertà di circolazione, di riunione, di associazione, di sciopero ecc., realizzando così un marcato effetto *chilling*⁷⁴.

La salvaguardia della libertà morale non va infatti limitata al contesto

MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 240 ss.; M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali*, cit., p. 17; R. LOPEZ, *Videosorveglianza biometrica tramite riconoscimento facciale: parere negativo del Garante per la "privacy"*, in *Proc. pen. giust.*, 2022, p. 798 ss.; L. SAPONARO, *Le nuove frontiere tecnologica dell'individuazione personale*, cit., p. 17, rileva che «nella sorveglianza "di massa" l'obiettivo non è più controllare un luogo, ma controllare le persone presenti in quel luogo, con l'effetto che i dati dei soggetti presenti potranno essere analizzati e utilizzati per valutazioni diverse quali, ad esempio, la partecipazione ad un comizio politico, ad una cerimonia religiosa, o ad un incontro sessuale. con una palese, quanto inaccettabile, lesione dei diritti individuali di libertà»; per L. CAMALDO, *I.A. e investigazione penale predittiva*, cit., p. 246, allo stesso modo, anche i programmi di identificazione "a posteriori" rappresentano «una grave minaccia per la *privacy* e potrebbero facilmente trasformarsi in strumenti potenti per effettuare una sorveglianza di massa».

⁷³ A. MANGIARACINA, *Il riconoscimento facciale*, cit., p. 81. Come sottolineato dal Garante per la protezione dei dati personali, *Parere sul sistema SARI Real Time*, provv. n. 127 del 25 marzo 2021 «l'identificazione di una persona (...) comporta il trattamento biometrico di tutte le persone che circolano nello spazio pubblico monitorato (...) Pertanto, si determina una evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale».

⁷⁴ In tal senso, tra molti, L. CAMALDO, *I.A. e investigazione penale predittiva*, cit., p. 249; E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, cit., p. 1 ss.; S. DEL GATTO, *La governance delle nuove tecnologie*, cit., p. 47; J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, cit., p. 23 s.; F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 274 ss.; F. DE SIMONE, *Una nuova tipologia di misure di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale*, in *Arch. pen. (web)*, 2023, f. 2, p. 18 ss.; F. DI MATTEO, *La riservatezza dei dati biometrici nello Spazio europeo dei diritti fondamentali*, cit., p. 79; M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., p. 64; G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 57 ss.; F. PAOLUCCI, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *Riv. dir. media*, 2021, f. 1, p. 10; L. SAPONARO, *Le nuove frontiere tecnologica dell'individuazione personale*, cit., p. 17. Sul punto A. CAMON, *Processo e libertà morale: tendenze nelle recenti della giurisprudenza, della dottrina, della legislazione*, in *Proc. pen. giust.*, 2024, p. 1030, ritiene invece che vi sia una "iperestensione" del concetto di libertà morale, «che contrassegna anche la posizione di chi combatte gli strumenti automatici di riconoscimento facciale», nel senso che ci si può domandare se il chilling effect indotto dalle tecnologie della sorveglianza «vada davvero guardato attraverso le lenti dell'art. 188 o non piuttosto attraverso quelle della specifica libertà (di circolazione, di comunicazione, di manifestazione del pensiero, di riunione ...), che di volta in volta ne risulta "congelata"».

dell'assunzione della prova, riferendosi al più generale ambito dell'esercizio dei diritti inviolabili dell'uomo garantiti dall'art. 2 Cost.⁷⁵.

In particolare, per garantire una tutela effettiva dalle tecniche basate sul riconoscimento facciale, si è ipotizzata una possibile "copertura", facendo ricorso a un'interpretazione estensiva dell'art. 13 Cost., sviluppando ed ampliando il concetto della libertà personale, non più limitato alle sole intrusioni fisiche. In tale direzione, emergerebbe «una nuova concezione integrale della persona, alla cui proiezione nel mondo corrisponde il diritto al pieno rispetto di un corpo che ormai è, al tempo stesso, "fisico" ed "elettronico". In questo nuovo mondo la *data protection* adempie alla funzione di assicurare quell' "habeas data" che i tempi mutati esigono, diventando così, com'è avvenuto con l'*habeas corpus*, un elemento inscindibile dalla civiltà»⁷⁶.

Analizzando inoltre il versante della protezione dei dati di carattere personale, dalla Carta dei diritti fondamentali dell'Unione europea risulta come i singoli non siano più titolari soltanto della "classica" libertà negativa di non subire interferenze nella propria sfera personale (il nucleo fondante del diritto alla *privacy*, ossia il diritto ad essere lasciati soli, *right to be left alone*, che si ottiene proteggendo la propria sfera privata da intrusioni esterne), ma anche di una libertà positiva riguardante il diritto del singolo di poter sempre controllare i propri dati personali, ovvero tutte «quelle informazioni, che identificano o rendono identificabile, direttamente o in modo indiretto, una persona fisica e che possono fornire notizie sulle sue caratteristiche, abitudini, stile di vita, relazioni personali, stato di salute, situazione economica, etc.»⁷⁷.

⁷⁵ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 276; Corte cost. 19 giugno 1998, n. 229; secondo M. TORRE, *Nuove tecnologie e trattamento dei dati personali*, cit., p. 1054 «nessuno è in grado di sapere con esattezza se e quando la propria immagine (...) verrà captata dal sistema per essere confrontata con quella di soggetti ritenuti sospetti o pericolosi, ma il solo fatto di essere a conoscenza che esiste tale tecnologia e che il suo impiego non è soggetto ad alcuna previsione normativa che ne precisi casi e modi di impiego mette di fatto a rischio la stessa libertà morale della persona».

⁷⁶ Così S. RODOTÀ, *Privacy, libertà, dignità. Discorso conclusivo*, 26^a Conferenza Internazionale sulla *Privacy* e sulla Protezione dei Dati Personali, Poland, Wroclaw (PL), 14, 15, 16 settembre 2004, in <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293#:~:text=Senza%20una%20forte%20tutela%20del,la%20costruzione%20di%20una%20socie%C3%A0>; nello stesso senso ritengono che debba essere senz'altro valorizzata l'inviolabilità della libertà personale di cui all'art. 13 Cost., intesa come *habeas data*, J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 1068 ss.; M. GIALUZ, *Prove fondate sull'intelligenza artificiale e diritti fondamentali*, cit.; sul tema v. anche L. PARLATO, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in *Proc. pen. giust.*, 2020, p. 297 e ss.

⁷⁷ L. LUPARIA DONATI, *Privacy, diritti della persona e processo penale*, cit., p. 1454.

L'aspetto allarmante scaturisce dunque dal fatto che le nuove tecnologie dei sistemi di riconoscimento facciale non si "limitano" ad una sorveglianza massiva ed indiscriminata, ma sono in grado di "catturare" e di "impossessarsi" di ciò contraddistingue ogni essere umano: gli «aspetti unici ed insostituibili della persona»⁷⁸.

A ciò si aggiunge peraltro l'altissimo rischio di "*scope creep*" costituito dalla deviazione e dall' indebito ampliamento progressivo, rispetto all'ambito inizialmente dichiarato, della raccolta di dati personali, pertanto un sistema che ne preveda l'utilizzo deve includere salvaguardie atte a prevenire impieghi non autorizzati⁷⁹.

Quello che si presenta è dunque un quadro fortemente problematico in cui i rischi e le criticità sembrano superare i vantaggi in termini di benefici attesi⁸⁰.

6. Conclusioni

In conclusione, tornando al tema delle ricadute dei risultati del riconoscimento facciale nel processo penale, un'indagine condotta "in negativo" e "allo stato" potrebbe essere utile per prefigurare un percorso di analisi. Partire dalle considerazioni "preclusive" costituisce il primo passo per ragionare in termini di divieti ovvero di possibili legittimi utilizzi, necessariamente e rigidamente regolamentati, a seconda del metodo automatico di ricerca impiegato (ad esempio il Sari in modalità *Real Time* ovvero *ex post Enterprise*). Definito l'*an* e il *quomodo*, il sistema dovrà comunque adeguarsi e sapersi adattare al costante sviluppo tecnologico attraverso la costruzione di un'apposita e robusta disciplina *ad hoc*, tesa alla trasparenza del processo, all'affidabilità del risultato, all'eliminazione delle mag-

⁷⁸ F. PAOLUCCI, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, cit., p. 5.

⁷⁹ V. sul punto F. DI MATTEO, *La riservatezza dei dati biometrici nello Spazio europeo dei diritti fondamentali*, cit., p. 90 s.

⁸⁰ Così J. DELLA TORRE, *Novità dal Regno Unito*, cit., p. 233; M. FASAN, *Intelligenza artificiale, giustizia e sostenibilità costituzionale*, in G. DI PAOLO (a cura di), *Trasformazioni della giustizia. Norme, organizzazione, tecnologie*, Università di Trento, Editoriale scientifica, 2024, p. 116, evidenzia che nell'impossibilità «di negare sia la presenza di benefici che di rischi nell'applicazione dell'AI nel settore della giustizia, occorre capire quale sia la strada da intraprendere per garantire un uso di questa tecnologia concretamente ed effettivamente compatibile con le categorie e gli strumenti costituzionali che qui vengono in rilievo, al netto delle criticità evidenziate e confrontando la dimensione giuridica tradizionale con le novità di un modo nuovo non più arginabile nel suo impatto».

giori criticità evidenziate e in grado di garantire i diritti e le libertà fondamentali del singolo.

La continua e inarrestabile evoluzione dell'intelligenza artificiale e dell'elaborazione delle immagini nell'ambito del riconoscimento rende infatti ogni giorno più problematica tale regolamentazione. Le previsioni delineano uno scenario sempre più inquietante: il futuro prossimo corre nella direzione di un'ulteriore riduzione della *privacy* e di una ancora maggiore sorveglianza generalizzata. Si stima, infatti, che l'accuratezza del riconoscimento facciale raggiungerà in condizioni ottimali percentuali prossime all'unità, con algoritmi in grado di ridurre i *bias* al 98-99% su tutti i gruppi demografici. L'incremento della potenza di calcolo aumenterà la quantità di dati che potranno essere processati a parità di tempo consentendo analisi sempre più dettagliate. I sistemi ibridi (3D e termici) renderanno inutili sotterfugi basati su trucchi ottici. La tecnologia sarà in grado di superare potenzialmente ogni possibile forma di contromisura, permettendo l'identificazione del soggetto, anche in presenza di mascherine e occhiali da sole, ad esempio attraverso l'analisi della camminata, della forma delle orecchie e persino dei *pattern* delle vene delle mani⁸¹.

Un incremento delle prestazioni che, tuttavia, potrebbe non essere accompagnato dalla risoluzione delle criticità evidenziate (opacità del metodo "*black box*", videosorveglianza generalizzata) e paradossalmente, addirittura, amplificarle.

Al fine di prevenire possibili lesioni ai diritti fondamentali⁸², l'Europa, e l'Italia in particolare, diversamente da altri Paesi (Cina, Russia e Stati Uniti), hanno per ora mantenuto un approccio prudentiale e di particolare cautela basato sul principio della precauzione⁸³.

In questa situazione di limbo, nonostante le indicazioni del Garante e la posizione assunta dal legislatore, pur riconoscendo tutte le criticità del

⁸¹ Clearview ha infatti sviluppato strumenti di "*deblur*" per migliorare immagini sfocate e "*mask removal*" per rimuovere digitalmente le mascherine, v. *Clearview Ai e facial recognition: il tuo volto è in un database (e tu non lo sapevi)*, in *ICT Security Magazine*, 4 ottobre 2025.

⁸² Secondo *Clearview Ai e facial recognition*, cit., gli esperti avvertono che stiamo trasformando ogni spazio pubblico in una "prigione digitale". La *Electronic Frontier Foundation*, insieme a 180 esperti mondiali, ha chiesto lo stop immediato della sorveglianza con riconoscimento facciale, definendola "incompatibile con i diritti umani". *Privacy International* parla di "sorveglianza costante dei nostri corpi" che minaccia le vite *online* e *offline*.

⁸³ Il legislatore ha sospeso l'installazione e l'utilizzo di impianti di videosorveglianza muniti di sistemi di riconoscimento facciale in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, sino all'entrata in vigore di una disciplina legislativa *ad hoc* e, comunque, sino alla data del 31 dicembre 2023 (d.l. 8 ottobre 2021, n. 139, conv. con modif. dalla legge 3 dicembre 2021, n. 205), termine poi prorogato, al 31 dicembre 2025.

facial recognition, la giurisprudenza pare propendere comunque per il suo impiego. L'esito dell'algoritmo, non in grado di offrire certezze, ma solo risultati di compatibilità, viene tuttavia considerato come una sorta di tassello, un indizio, all'interno del contesto probatorio complessivo. Per il giudice, infatti, può assumere il valore di un indicatore di "apprezzabile somiglianza"⁸⁴, utilizzabile unitamente ad altri mezzi di prova (quali, ad esempio, il confronto antroposomatico, basato su parametri fisionomici individualizzanti dell'individuo, le dichiarazioni accusatorie di coimputati ecc.) e in presenza di una motivazione rafforzata sulla compatibilità e l'assenza di difformità significative⁸⁵.

A fronte di tale scenario, è dunque necessario che si intervenga al più presto - come d'altronde richiesto anche dal regolamento sull'intelligenza artificiale (UE) 2024/1689 di recente introduzione⁸⁶ - per regolamentare compiutamente l'impiego delle tecnologie basate sull'intelligenza artificiale e, in particolare, dei sistemi di riconoscimento facciale.

La vera sfida sarà dunque quella di concepire un inquadramento legislativo che stabilisca i limiti di utilizzo di tali meccanismi, sia in grado di garantire i diritti fondamentali dell'individuo e, soprattutto, sia sufficientemente flessibile per potersi adeguare alla loro rapidità di cambiamento.

⁸⁴ Corte App. Roma, 25 ottobre 2024, *inedita*.

⁸⁵ In questo senso, v. Cass. pen., Sez. II, 20 marzo 2025, n. 18099, *inedita*; Cass. pen., Sez. II, 13 luglio 2023, n. 39551, *inedita*; Cass. pen., Sez. I, 21 luglio 2020, n. 21823, *inedita*.

⁸⁶ Il reg. (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 sull'intelligenza artificiale ha istituito un quadro giuridico uniforme per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale demandando però ai legislatori dei singoli Stati Membri la necessaria introduzione di una disciplina dettagliata per l'uso di sistemi di riconoscimento biometrico, v. *amplius* C. CESARI, *Il riconoscimento facciale dall'AI Act all'ordinamento italiano: le direttrici di un'evoluzione necessaria*, § 3; S. QUATTROCOLO, *Intelligenza artificiale e processo penale: le novità dell'AI Act*, in *dirittodidifesa.eu*, 16 gennaio 2025; E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 203 ss. e 275; L. AGOSTINO-G. BORGIA, *La disciplina dei sistemi di IA ad alto rischio: biometria, attività di contrasto e amministrazione della giustizia*, in *Proc. pen. giust.*, 2024, p. 1061 ss.

IL RICONOSCIMENTO FACCIALE DALL'AI ACT ALL'ORDINAMENTO ITALIANO: LE DIRETTRICI DI UN'EVOLUZIONE NECESSARIA

CLAUDIA CESARI

SOMMARIO: 1. Lo stato dell'arte: tecnologie di riconoscimento e ricadute concettuali e sistematiche. – 2. L'AI Act: le indicazioni del *framework* europeo. – 3. L'impatto sul sistema interno, tra legislazione codicistica e novellazione.

1. *Lo stato dell'arte: tecnologie di riconoscimento e ricadute concettuali e sistematiche*

In nessun campo, come in quello delle tecnologie di riconoscimento facciale, si assiste oggi in maniera emblematica a uno sviluppo tecnologico massivo, a una diffusione applicativa incontrollabile, sia nel settore pubblico che in quello privato (e persino nella vita quotidiana dei singoli)¹, a un interesse dottrinale sempre più marcato², e tuttavia a una preoccupante (sia pur guardinga) inerzia legislativa. Le cosiddette FRT (*Facial Recognition Technologies*) sono ovunque e sempre di più, di conseguenza, sono oggetto di attenzione da parte di una ricerca giuridica consapevole dell'ineludibilità dei problemi che comportano, senza che dal legislatore giungano prese di posizione chiare, che appaiono non più rinviabili. Mentre le fonti europee si schierano almeno sui punti chiave della problematica,

¹ Per una panoramica in chiave critica, F. DI MATTEO, *La riservatezza dei dati biometrici nello spazio europeo dei diritti fondamentali: sui limiti all'utilizzo delle tecnologie di riconoscimento facciale*, in *Freedom, Security and Justice. European legal studies*, 2023, n. 1, p. 74 ss.; v. anche M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale*, 2022, n. 9.

² Per limitarci, in prima battuta, ai lavori monografici recenti, cui si rinvia per la bibliografia completa di riferimento, si vedano F. DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, Cedam, 2025; E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna*, Giappichelli, 2025; nonché, nella più ampia prospettiva della tutela dei diritti fondamentali, G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, Napoli, 2021.

benché in un quadro più ampio di gestione dei temi cruciali dell'intelligenza artificiale e delle sue applicazioni nella vita dei singoli e delle comunità, quelle nazionali esitano, riflettono, rinviando, adottano soluzioni generiche e nebbiose in un contesto in cui l'unica strategia di gestione sarebbe invece la chiarezza.

Il tema, infatti, è estremamente articolato, anche in ragione dell'intreccio con i profili tecnici dello strumentario di riferimento, che comportano distinzioni e definizioni tutt'altro che neutre dal punto di vista degli utilizzi che se ne possono fare e quindi dell'impatto sui diritti e, per quel che qui ci riguarda, sul sistema processuale e su regole e garanzie che è chiamato ad approntare.

Non è questo lo spazio adeguato a una disamina delle peculiarità tecniche dei *tools* preposti al riconoscimento facciale³, ma pur in questa sede ne vanno rammentate quelle caratteristiche che hanno riflessi immediati sulla relativa regolamentazione, perché implicano modalità diverse di operatività in concreto e quindi differenti modi e intensità di incidenza sui diritti coinvolti.

È il caso della distinzione – cruciale anche nelle fonti di riferimento – tra riconoscimento *in tempo reale* e riconoscimento *a posteriori*. Il riconoscimento in tempo reale (definito anche “contestuale”, “dal vivo”, “*live*”, “*in real time*”) è effettuato da un sistema che cattura le immagini analizzando flussi video ed effettua contestualmente una comparazione di questi con i contenuti di una banca dati predefinita, segnalando con un *alert* le eventuali corrispondenze (*matches*), quando superino una data soglia di compatibilità indicata in valori percentuali. In questo caso, il riconoscimento è effettuato dal sistema senza ritardi significativi, ossia in pratica immediatamente, da cui la definizione di riconoscimento “in tempo reale”. La versione “*a posteriori*”, invece (detta anche “statica” o “*post remote*”), effettua una comparazione tra l'immagine acquisita e quelle disponibili nella banca dati utilizzata, a una significativa distanza di tempo rispetto alla raccolta

³ Per tutti, cfr. S. Z. LI, A. K. JAIN, *Handbook of face recognition*, Springer, 2004; nonché la ricostruzione e i richiami in E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, Giappichelli, 2025, p. 46 ss. Consistente anche la documentazione a livello europeo: *inter alios*, v. Art. 29 *Data protection Working Party* (2012), *Opinion 02/2012 on facial recognition in online and mobile services*, 00727/12/EN, WP192, Brussels, 22 marzo 2012, p.2; S. AZRIA, F. WICKERT, *Facial recognition: current situation and challenges, Report for the Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data. Convention 108*, 13 novembre 2019, in <https://tm.coe.int>; *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, 12 maggio 2022, European Data Protection Board; T. MADIEGA, H. MILDEBRATH, *Regulating facial recognition in EU*, European Parliamentary Research Service, 2021.

del dato, sempre comparando l'immagine stessa con i profili disponibili nel data set archiviato, producendo risultati in termini di possibili corrispondenze⁴.

Le differenze strutturali tra le due metodologie e i relativi sistemi operativi sono decisive nel contesto normativo in cui vanno collocate, in considerazione dei differenti impieghi e dell'impatto sensibilmente diverso sui diritti fondamentali coinvolti. Gli strumenti che operano "in differita" sono infatti collegati in maniera più evidente alle pratiche quotidiane di riconoscimento a fini identificativi effettuate dalle forze di polizia in corso di indagine e hanno i caratteri delle operazioni più selettive e mirate, oltre che connotate da tempistiche più distese, controlli più accurati e minori margini di errore. Quelli che si applicano "in diretta" sono di uso meno frequente, ma correlati a scansioni più concitate e a forme di sorveglianza massificata, presentando quindi livelli di affidabilità più ridotti, a fronte di rischi elevati di coinvolgimento di terzi estranei all'accertamento penale o privi di precedenti di sorta e pericoli significativi di uso distorto a scopi di controllo dei cittadini.

Non a caso, nell'ordinamento nazionale, la vicenda che ha aperto in maniera più significativa il dibattito intorno alle tecnologie di riconoscimento facciale ruotava appunto intorno alla distinzione tra applicativi in diretta o in differita. Come è noto, la valutazione effettuata dal Garante della Privacy sulla legittimità degli applicativi di polizia noti come SARI (da tempo in uso in Italia) è stata positiva rispetto al SARI *Enterprise* (sistema di riconoscimento facciale *a posteriori*) e negativa rispetto alla funzionalità *Real Time* (sistema *live*), essendo soltanto il primo riconducibile al quadro normativo esistente, come modalità tecnologica di effettuare l'identificazione di un sospettato, e restando invece del tutto avulso dalla cornice legislativa il secondo⁵. Del resto, la classificazione è cruciale an-

⁴ Sulla distinzione e sulle sue caratteristiche tecniche, v. *amplius*, fra gli altri, E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto penale e uomo*, 19 maggio 2021, p. 5; J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.*, 2022, p. 1061; E. SACCHETTO, *Tecnologie di riconoscimento*, cit., p. 50 ss. Cfr. anche *Biometric and Behavioural Mass Surveillance in EU Member States, Report for the Greens/EFA in the European Parliament*, 2021, p. 27, per l'inserimento del distinguo in posizione chiave nell'assetto definitorio di base di questa tematica.

⁵ Sul SARI e sulle sue vicissitudini la dottrina si è ampiamente spesa e ad essa si fa rinvio per ricostruzione tecnica, approfondimenti e rilievi critici: v., in particolare, G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuri sviluppi normativi sul fronte eurounitario*, in *Leg. pen. (web)*, 11 dicembre 2021; M. COLACURCI, *Riconoscimento facciale*, cit., p. 37 ss.; J. DELLA TORRE, *Tecnologie di riconoscimento facciale*, cit., p. 1076 ss.; F. DEMARTIS, *I sistemi automatici*, cit., p. 106 ss.; G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*, in *Cass.*

che nell'*AI Act*, che – come si vedrà - irrigidisce la disciplina per i sistemi di riconoscimento in tempo reale, mentre ammette con adeguate cautele quelli *a posteriori*.

I sistemi di riconoscimento facciale, inoltre, fanno parte a pieno titolo dell'area delle prove digitali, condividendone tutte le criticità. Anche a voler tacere delle specifiche implicazioni e ricadute problematiche degli algoritmi di riconoscimento, comportano di per sé gli stessi profili dubbi correlati alle basi digitali della fonte di prova: l'opacità del codice sorgente, la scarsa trasparenza dei dati di riferimento e del training dell'algoritmo, i problemi correlati al tasso di errore, il *knowledge impairment*, e i riflessi di queste tematiche sui diritti fondamentali e sulla struttura processuale (diritto di difesa, parità delle armi, metodo dialettico, imparzialità del giudice, presunzione di innocenza)⁶.

Essendo basati sull'intelligenza artificiale, infine, sono fra i primi sistemi ad essere interessati dalla nuova regolamentazione europea dedicata al tema, dalla quale ricevono infatti una specifica e dettagliata disciplina, essendo fra le tecnologie *AI based* più diffusamente utilizzate e commercializzate e fra quelle con gli impatti lesivi di diritti fondamentali più ampi e potenzialmente gravi.

Sullo sfondo delle complesse problematiche che lo strumentario in esame comporta, va considerata del resto la potente versatilità funzionale che lo contraddistingue. I sistemi di riconoscimento facciale, infatti, hanno ricadute a molteplici livelli sul sistema della giustizia penale. Anche a voler mettere da parte i possibili usi in sede di prevenzione e strategie di sicurezza, e considerando solo gli impieghi collocabili entro lo stretto pe-

pen., 2025, p. 640 ss.; R. LOPEZ, *Videosorveglianza biometrica tramite riconoscimento facciale: parere negativo del Garante per la privacy*, in *Proc. pen. giust.*, 2022, p. 798 ss.; A. MARANDOLA, *Il riconoscimento facciale*, in C. CONTI - A. MARANDOLA (a cura di), *La prova scientifica*, Milano, 2023, p. 504 ss.; G. MOBILIO, *Tecnologie di riconoscimento*, cit., p. 240 ss.; E. SACCHETTO, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *Leg. pen. (web)*, 16 ottobre 2020; L. SAPONARO, *Le nuove frontiere tecnologiche dell'individuazione personale*, in *Arch. pen.*, 2022, n. 1, p. 1 ss.; R. V.O. VALLI, *Sull'utilizzabilità processuale del SARI: il confronto automatizzato dei volti rappresentati in immagini*, in *ius.giuffrè.it*, 16 gennaio 2019.

⁶ Le problematiche della prova digitale sono da tempo oggetto di riflessione dottrinale. Per una panoramica essenziale, anche con riferimento alle tematiche rammentate in testo, v., per tutti, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018; nonché S. QUATTROCOLO, *Qualcosa di meglio del diritto (e del processo) penale?*, in *Discrimen*, 26 giugno 2020; EAD., *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Leg. pen.*, 18 dicembre 2018; EAD., *Equità del processo penale e automated evidence alla luce della convenzione europea dei diritti dell'uomo*, in *Rev. it. esp. der. pen.*, 2019, p. 107 ss.; L. PRESSACCO, *Gli elementi di prova generati o raccolti tramite intelligenza artificiale*, in G. DI PAOLO - L. PRESSACCO (a cura di), *Indagini e prove nella società digitale*, Editoriale Scientifica, Napoli, 2025, p. 273 ss.

rimetro del rito penale, i modi in cui potenzialmente si possono utilizzare si collocano in più ambiti. Possono essere strumenti alternativi di identificazione, mirati solo a consentire l'aggancio (più rapido e affidabile di quelli tradizionali) tra una persona fisica e le sue generalità. Possono servire a rintracciare indagati o condannati in fuga. Possono valere a stabilire se, quando, dove una persona si trovava in passato, in circostanze a vario titolo utili alla ricostruzione del fatto criminoso e delle relative responsabilità, corrispondendo funzionalmente, a seconda della fase del procedimento, alle individuazioni o ricognizioni. Possono persino – in teoria – ricostruire le emozioni provate nel momento del fotogramma dalla persona rappresentata, permettendo le più svariate valutazioni aggiuntive, da ciò che provava l'indagato colto in un momento e luogo rilevanti nella vicenda criminosa a quello che prova un testimone mentre depone o una persona informata quando le si rivolgono le domande. Ognuno di questi impieghi conduce a livelli di criticità differenti, a diversi assetti di norme di riferimento, a differenti ricadute e limiti d'uso, a differenti impatti sulla struttura del procedimento e sulle regole che lo informano.

Quello che sembra certo, è che a questa sfida non ci si possa sottrarre. La massiccia presenza di questa tecnologia nella vita quotidiana, individuale e collettiva, il crearsi progressivo di archivi che effettuano lo stoccaggio sistematico delle informazioni raccolte, la conseguente disponibilità di informazioni preziose, economiche, disponibili e facilmente accessibili, non permettono di pensare ragionevolmente di potervi rinunciare. Quello che è indifferibile, è però una legislazione di riferimento che ne tracci le coordinate di impiego, i presupposti, i limiti d'uso e – in un quadro di regole chiare, entro il perimetro di un razionale bilanciamento degli interessi in gioco – anche i divieti.

2. *L'AI Act: le indicazioni del framework europeo*

Il tema del riconoscimento facciale è presente in maniera marcata nella trama normativa del regolamento europeo sull'intelligenza artificiale (reg. (UE) 2024/1689, da qui in avanti *AI Act*), dedicato alla costruzione di una normativa di base fondata sull'adeguato bilanciamento tra opportunità e criticità degli applicativi di intelligenza artificiale nel quadro dell'Unione. Se la chiave di volta della normativa è la costruzione di un'intelligenza artificiale al contempo etica, sicura, affidabile e antropocentrica, gli applicativi finalizzati all'analisi biometrica delle persone fisiche e il sottinsieme di questi legato ai tratti del volto, affiorano come una delle principali fonti di preoccupazione del legislatore. Almeno 25 dei 180 considerando del Regolamento sono espressamente dedicati ai sistemi di identifi-

cazione mediante dati biometrici e di riconoscimento delle emozioni, e ad essi vanno aggiunti nel contesto processualpenalistico i numerosi considerando che si riferiscono a rischi e cautele di impiego dei sistemi di intelligenza artificiale nell'ambito delle attività di contrasto, che si saldano ai primi nella costruzione di un sistema estremamente complesso e articolato.

A volerne disegnare la fisionomia, si deve partire dalle scelte di fondo, riferibili ad alcuni pericoli di maggiore peso avvertiti dal legislatore, cui vanno riferiti altrettanti chiari divieti, cui si aggiungono poi una serie di scelte autorizzative, legate alle esigenze pratiche delle attività di contrasto ed improntate però ad estrema cautela. In altri termini, è palese in questo ambito di operatività degli applicativi di intelligenza artificiale, come a livello europeo si sia consapevoli dell'impossibilità di prescindere dai vantaggi che offrono, come di recedere dalla diffusività che già nei fatti hanno conquistato, ma anche dell'esigenza di regolarne rigidamente gli impieghi, considerando gli altissimi rischi che presentano. Fra questi ultimi, spiccano, quanto ai sistemi di identificazione biometrica, la scarsa affidabilità, il rischio che per contro influenzino le decisioni in maniera troppo marcata, sottraendosi al controllo umano, e l'impatto forte sui diritti fondamentali, processuali e non, come il diritto di difesa, la presunzione di innocenza, la riservatezza, la libertà di riunione e associazione, il principio di eguaglianza.

Di qui, la struttura della regolamentazione che riguarda gli applicativi di riconoscimento facciale, basata sul *risk based approach*, che connota l'impianto regolamentare e si basa sulla nota tripartizione fra attività vietate, ad alto rischio e a basso rischio, adeguando i livelli di tutela e le salvaguardie in ragione dell'impatto potenziale degli applicativi di IA sui diritti fondamentali⁷. Ne consegue che, nel campo dell'identificazione biometrica mediante immagini facciali, alcune pratiche sono nettamente vietate, alcune vietate con eccezioni ammissibili, altre consentite con forti clausole di garanzia e limitazioni.

Nettissimo è il divieto di *scraping*, innanzitutto, ossia la raccolta non mirata di immagini facciali da internet o da filmati di telecamere a circuito chiuso (art. 5 § 1 lett. *e Ai Act*), legato all'impatto di simile forma di collazione "a strascico" delle immagini dei volti sul diritto alla privacy, ma

⁷ In termini generali, sulla struttura del Regolamento e in particolare sull'impatto sugli ambiti della giustizia penale, cfr. A. BALSAMO, *L'impatto dell'Intelligenza artificiale nel settore della giustizia*, in *Sistema penale (web)*, 22 maggio 2024; L. BELVINI, *Intelligenza artificiale e circuito investigativo*, Cacucci editore, Bari, 2025, p. 80 ss.; G. CANZIO, *AI Act e processo penale: sfide e opportunità*, in *Sistema penale (web)*, 14 ottobre 2024; S. QUATTROCOLO, *Intelligenza artificiale e processo: le novità dell'AI Act*, in *Dir. difesa (web)*, 16 gennaio 2025; M. TORRE, *Il Regolamento europeo sull'intelligenza artificiale*, in *Proc. pen. giust.*, 2024, p. 1534 s.

anche al rischio di sorveglianza di massa che esso comporta (consid. n. 43).

Risulta abbastanza nitida, senza però giungere al rifiuto, la preoccupazione relativa ai sistemi che dall'analisi biometrica dei tratti fisionomici identificano o inferiscono le emozioni o intenzioni delle persone fisiche (consid. n. 18), che sono collocati tra i sistemi ad alto rischio (All. III, n. 1 lett. *c* e art. 6 § 2 *AI Act*). Il regolamento solleva infatti dubbi seri sulla stessa base scientifica di tali strumenti, oltre a temere che possano condurre ad esiti discriminatori o lesivi di diritti e libertà fondamentali. Il divieto d'uso che li concerne, tuttavia, è circoscritto all'ambito dell'istruzione e del lavoro, mentre non sembra che vi sia una preclusione *ex se* all'impiego in altri ambiti, sia pure con le garanzie imposte dalla qualifica di applicativi ad alto rischio. Anzi, per il procedimento penale sono previste eccezioni alle clausole di garanzie specifiche: è il caso dell'informativa specifica prevista a vantaggio delle persone fisiche esposte ai sistemi di riconoscimento delle emozioni, che non è dovuta proprio per i sistemi «autorizzati dalla legge per accertare, prevenire o indagare reati», salve le tutele per i diritti dei terzi e in conformità al diritto dell'Unione (art. 50 § 3 *AI Act*).

Appare invece oggetto di considerazione approfondita, sin dal momento definitorio, la scansione tra identificazione biometrica remota in tempo reale e *a posteriori*, caratterizzata dalle vive preoccupazioni del legislatore europeo rispetto alla prima e dall'accettazione sostanziale dell'utilizzabilità della seconda.

In particolare, nei considerando si sottolinea come i sistemi di identificazione biometrica in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto risultino particolarmente invasivi della *privacy*, possano far sentire i cittadini sotto sorveglianza e quindi ledere diritti e libertà fondamentali come la libertà di riunione e rischino di avere esiti discriminatori legati alle inesattezze di carattere tecnico e al conseguente pericolo di impatto diversificato su differenti gruppi etnici, anagrafici o connotati da condizioni fisiche specifiche, come il sesso o le disabilità (consid. n. 32). Di qui la scelta, apparentemente radicale, di vietarne l'utilizzo, con la significativa eccezione, però, di situazioni specifiche e tassative nelle quali lo scopo perseguito è considerato di tale rilievo da bilanciare i rischi, e in cui comunque va seguito accuratamente uno specifico protocollo di garanzie procedurali, che il regolamento disegna in maniera piuttosto dettagliata. I casi eccettuati, in ogni caso, rientrano negli impieghi ad alto rischio e quindi condividono di questi anche l'assetto generale di tutele previsto dal regolamento.

Norma di riferimento a tale riguardo è l'art. 5 *AI Act*, che elenca le attività vietate, includendovi, al § 1 lett. *b*, l'uso di sistemi di identificazio-

ne biometrica remota in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto, fatta eccezione per tre casi. Si tratta delle ipotesi in cui tale uso risulti strettamente necessario per: 1) la ricerca di persone scomparse o vittime di sottrazione, tratta o sfruttamento sessuale di esseri umani; 2) la prevenzione di una minaccia specifica e imminente per la vita o l'incolumità fisica di persone fisiche o di una minaccia concreta (reale, nonché attuale o prevedibile) di attacco terroristico; 3) la localizzazione o l'identificazione di un sospetto a fini di svolgimento di un'indagine penale, dell'esercizio dell'azione penale, o dell'esecuzione di una sanzione penale. In teoria, tutte e tre le evenienze si potrebbero collocare in seno a un procedimento penale, essendo potenzialmente collegate direttamente o indirettamente all'accertamento di reati già commessi, ad evitare che se ne commettano di ulteriori o che si aggravino le conseguenze di quelli già commessi, alla salvaguardia e all'individuazione delle persone offese, ad accertare ulteriori reati, connessi o collegati a quelli per i quali l'indagine è già in corso, e così via. L'area delle eccezioni, insomma, così perimetrata, non risulta necessariamente ristretta.

Nell'ottica delle limitazioni all'uso, quindi, risultano cruciali le ulteriori precisazioni del regolamento, in parte funzionali a restringere l'ambito operativo delle eccezioni, in parte mirate a costruire un procedimento autorizzativo che assicuri il controllo e la "messa in sicurezza" degli usi consentiti.

Dal primo punto di vista, rileva la limitazione relativa al punto n. 3 delle eccezioni ammesse, che autorizza l'impiego di sistemi di identificazione biometrica live in sede di procedimento penale per localizzare o identificare l'indagato, imputato o condannato, solo quando si proceda per i reati di cui alla lista contenuta nell'Allegato II del regolamento che siano punibili con una pena o una misura di sicurezza privativa della libertà personale non inferiore nel massimo a quattro anni. Il limite, tracciato sul piano sia qualitativo che quantitativo, è abbastanza definito⁸ e – pur nella prevedibile varietà delle opzioni di cui alle legislazioni nazionali – offre una mappa nitida dei confini di ammissibilità dello strumen-

⁸ La lista dei reati rilevanti ai fini di cui in testo è contenuta nell'Allegato II all'*AI Act*, e comprende i reati di: terrorismo; tratta di esseri umani; sfruttamento sessuale dei minori e pornografia minorile; traffico illecito di armi, munizioni ed esplosivi; omicidio volontario e lesioni gravi; traffico illecito di organi e tessuti umani; traffico illecito di materie nucleari e radioattive; sequestro, detenzione illegale e presa di ostaggi; reati che rientrino nella competenza giurisdizionale della Corte penale internazionale; illecita cattura di aeromobile o nave; violenza sessuale; reato ambientale; rapina organizzata o a mano armata; sabotaggio; partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati sopra.

to, a questo punto sufficientemente circoscritti⁹. Inoltre, l'uso autorizzato dei risultati ottenuti dai sistemi di identificazione è solo quello di «confermare l'identità della persona specificamente interessata» (art. 5 § 2), sicché: *in primis*, gli esiti non potrebbero essere impiegati come prova o elemento di prova della responsabilità, risultando utilizzabili solo per l'accertamento dell'identità della vittima o dell'indagato/imputato; *in secundis*, anche a tale fine, non potrebbero valere come elementi esclusivi di prova, dovendo fungere solo da elementi di corroborazione di altre prove dell'identità dell'interessati, già presenti in atti e da confermare tramite il riconoscimento facciale automatizzato. E non solo: l'impiego autorizzato in simili evenienze deve fondarsi altresì su un giudizio di bilanciamento che sostanzia la valutazione preliminare di stretta necessità e proporzionalità ad esso sottesa e che impone di considerare, da un lato, la gravità, la probabilità e l'entità del danno che sarebbe causato dal mancato uso del sistema; dall'altro, le conseguenze dell'uso del sistema per le persone interessate, ossia gravità, probabilità ed entità delle conseguenze ad esse arrecate.

Dal secondo punto di vista, ossia in un'ottica squisitamente procedurale, l'art. 5 impone una serie di passaggi a garanzia del rispetto delle tutele sostanziali descritte, che devono essere oggetto di specifica ponderazione. Prescrive, innanzitutto, che sia lo stesso diritto nazionale che legittime l'impiego dei sistemi a prevedere limitazioni temporali, geografiche e personali all'uso autorizzato. L'uso, inoltre, è autorizzato solo quando l'autorità di contrasto ha completato una valutazione d'impatto del sistema sui diritti fondamentali *ex art. 27 AI Act* e ha registrato il sistema nella banca dati *ex art. 49 Ai Act*. Inoltre, ogni singolo utilizzo del sistema deve essere preventivamente autorizzato da un'autorità giudiziaria (si deve ritenere, nella genericità deliberata che connota le fonti europee, sia un magistrato d'accusa, che un giudice) o da un'autorità amministrativa indipendente. L'atto di impulso deve essere una richiesta motivata – che tenga conto dei presupposti sanciti dalla normativa nazionale. Da tali passaggi

⁹ F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 82, osserva che «l'elenco è abbastanza dettagliato e che non si limita a riportare formule amplissime, quali, ad esempio, “fatti di notevole gravità”, “pericoli per la sicurezza nazionale”, etc.», che in effetti sono note alle fonti sovranazionali proprio per lasciare agli Stati ampio argine di manovra. Compatibilmente con le differenze degli ordinamenti nazionali, in questo caso, l'elenco di cui alla nota precedente combinato con le soglie edittali sancite dalla normativa regolamentare, tracciano un binario abbastanza preciso, al netto delle peculiarità dei singoli sistemi. *Contra* E. SACCHETTO, *Tecnologie di riconoscimento facciale*, cit., p. 183, ad avviso della quale le tipologie coinvolte sarebbero invece troppo generiche e idonee a coinvolgere anche fatti di gravità troppo bassa per essere compatibili con il canone di proporzionalità.

si potrà prescindere solo in casi di urgenza, giustificati *ex post*, nei quali comunque dovrà essere richiesta una convalida all'autorità deputata all'autorizzazione, senza indebito ritardo e in ogni caso al massimo entro 24 ore. Il rigetto dell'autorizzazione (nonché, si deve ritenere, la mancata richiesta) comporta l'immediata interruzione delle attività di riconoscimento e la distruzione dei risultati (nonché, logicamente, la sopravvenuta inutilizzabilità di quelli nel frattempo acquisiti al procedimento ed eventualmente impiegati). Anche per il rilascio dell'autorizzazione sono sanciti parametri stringenti, giacché questa deve basarsi su prove oggettive "o indicazioni chiare" (verosimilmente equivalenti a elementi di prova comunque inequivoci) che sussistano le situazioni eccezionali previste dal regolamento per l'uso dei sistemi di identificazione remota in tempo reale, oltre alle relative condizioni di stretta necessità e proporzionalità e al rispetto dei limiti geografici, personali e temporali previsti dalla legge. Il regolamento prevede, infine, un chiaro limite all'uso probatorio degli elementi raccolti in questo modo: nessuna decisione, infatti, può essere adottata unicamente sulla base dell'output del sistema di identificazione biometrica in tempo reale (art. 5, § 3, ult. periodo *AI Act*), che dunque dovrà costituire elemento di corroborazione di altri elementi già in atti o essere da altri elementi comunque corroborato, ma soffre palesemente di un deficit di attendibilità che ne esclude l'impiego esclusivo a fini decisori.

A chiudere il sistema, sta il § 5 dell'art. 5, che impone agli Stati membri che vogliano ammettere – nei limiti consentiti dal Regolamento – l'uso dei sistemi di identificazione biometrica in tempo reale in spazi accessibili al pubblico e con finalità di contrasto, l'adozione «nel proprio diritto nazionale» delle «necessarie regole dettagliate» relative alle richieste, al rilascio delle autorizzazioni, agli obiettivi consentiti e al perimetro operativo dei medesimi. La clausola è decisiva, per disegnare il rapporto tra la cornice europea e il diritto interno, giacché l'*AI Act* esprime a chiare lettere l'idea di non essere – malgrado la forma regolamentare – *self executing* nel campo che qui interessa, presupponendo che le eccezioni contemplate trovino una traduzione normativa specifica a livello nazionale, senza la quale non sarebbero in condizioni di operare. In effetti, ciò comporta che senza questo tipo di impegno legislativo a livello interno, debbano ri-espandersi i divieti previsti dal regolamento, che invece non hanno bisogno – visto il contenuto esclusivamente negativo – di alcuna scelta interna. Nel caso di specie, insomma, si dovrebbe ritenere che i sistemi di riconoscimento facciale in tempo reale in spazi accessibili al pubblico e per attività di contrasto siano sempre vietati, a meno che e fino a quando l'ordinamento nazionale non legiferi specificamente sulle eccezioni ammissibili, stabilendone i presupposti, i limiti di operatività, le procedure di autorizzazione, le condizioni d'uso e le garanzie di contesto.

Diverso è il quadro, quanto ai sistemi di identificazione biometrica *a posteriori*, che sono visti con minore diffidenza, ma non considerati privi di criticità e quindi risultano utilizzabili, ma con una serie di dovute cautele (consid. n. 95). In particolare, il loro uso dovrebbe essere comunque «proporzionato, legittimo e strettamente necessario e quindi mirato», precisando le persone da identificare, il luogo e l'ambito temporale, e operando comunque in base a un set di dati chiuso e filmati acquisiti legalmente. Tali sistemi non dovrebbero mai essere impiegati per condurre forme di sorveglianza indiscriminata (neppure in sede di attività di contrasto) o come mezzi surrettizi per eludere le più rigide preclusioni relative alla sorveglianza in tempo reale. Ai sensi dell'Allegato III, n. 1 lett. *a* e dell'art. 26 § 10 ss. *AI Act*, in ogni caso, i sistemi di identificazione biometrica *a posteriori* per la ricerca di una persona sospettata o condannata per aver commesso un reato sono disciplinati come ad alto rischio e sono circondati di alcune garanzie specifiche. Innanzitutto, è necessaria un'autorizzazione preventiva oppure una convalida entro le successive 48 ore, rilasciate da un'autorità giudiziaria (magistrato d'accusa o giudice, quindi) ovvero amministrativa indipendente. Tale decisione deve comunque essere passibile di successivo controllo giurisdizionale. Si sottrae al meccanismo autorizzativo solo l'uso del sistema per l'identificazione iniziale di un sospetto, che però tale sia in base ad altri elementi, descritti come «fatti oggettivi e verificabili direttamente connessi al reato», quindi dotati di concretezza e consistenza, ben oltre la soglia dei meri sospetti o supposizioni. Anche in questa ipotesi, il rigetto della richiesta di autorizzazione (nonché, si direbbe, la mancata richiesta) comporta l'interruzione immediata dell'utilizzo e la distruzione dei dati personali nel frattempo raccolti.

Inoltre, ogni uso va limitato a quanto strettamente necessario per le indagini su uno specifico reato, apparentemente limitando la circolazione del dato, lo stoccaggio e, si direbbe, anche l'impiego probatorio e il ricorso a tale strumento oltre il limite della assoluta necessità, ossia quando l'identificazione del sospetto possa avvenire mediante strumenti o attività di indagine di diversa natura.

In ogni caso, è vietato l'uso non mirato di tali sistemi, dunque è precluso ogni impiego che non sia collegato alla commissione di un reato, alla ricerca di una persona scomparsa, a un procedimento penale o a una minaccia reale, attuale o prevedibile di un reato. Il regolamento, anzi, contempla una precisa regola di valutazione, prescrivendo che nessuna decisione che comporti effetti giuridici negativi su una persona possa essere adottata dalle autorità di contrasto «unicamente sulla base dell'output di tali sistemi di identificazione biometrica remota *a posteriori*»: la clausola esclude quindi l'adozione di provvedimenti penali *contra reum* che utilizzi-

no tali risultanze in maniera esclusiva, senza altri elementi nella base probatoria di riferimento.

Ulteriori garanzie di contesto consistono nell'obbligo di segnalare l'uso di tali strumenti identificativi nel fascicolo di polizia, che va messo a disposizione dell'autorità di vigilanza del mercato o dell'autorità garante per la protezione dei dati personali a livello nazionale. Una apposita relazione annuale sull'impiego di tali sistemi va presentata alle medesime autorità.

Va tenuto presente, infine, che ulteriori limiti legati all'impiego di *AI tools* da parte delle autorità di contrasto, discendono dal loro essere ad alto rischio in ogni caso, anche nelle ipotesi eccezionali ammesse rispetto ai divieti. Alcune di queste, innanzitutto, espulse dal novero delle pratiche vietate, vengono immesse nell'insieme contiguo a pericolosità immediatamente più bassa e quindi nell'area delle attività ad alto rischio. Inoltre, tali sono, per definizione e in ogni caso, tutti i sistemi di identificazione biometrica remota (sia *live*, che *a posteriori*), ai sensi dell'Allegato III n. 1, lett. *a*, pur nella misura in cui siano consentiti dal diritto dell'Unione o da quello nazionale.

Ciò implica che per questi vadano comunque rispettati gli standard di sicurezza elevati che sono richiesti per tutte le attività ad alto rischio, nell'ambito dei quali alcuni sono di particolare importanza nel procedimento penale e talora presentano richiami specifici e clausole di rafforzamento proprio con riferimento ai sistemi di identificazione remota. È il caso della previsione relativa alla sorveglianza umana, l'art. 14 *AI Act*, che al § 5 prescrive che i sistemi di identificazione biometrica descritti dall'Allegato III, punto 1, lett. *a* siano oggetto di particolare cautela nell'utilizzo: in particolare, è previsto che il *deployer*, ossia l'utilizzatore finale (incluso, per chi interessa, il magistrato o il giudice)¹⁰, non compia azioni o adotti decisioni sulla base dell'output identificativo, se questo non sia stato confermato separatamente da almeno due persone fisiche dotate della necessaria competenza, formazione e autorità. Unica eccezione a tale requisito è che il diritto nazionale lo reputi sproporzionato nell'ambito delle attività di contrasto.

Anche altri standard di garanzia richiesti per le attività ad alto rischio presentano vistosa rilevanza nell'ambito del rito penale, in genere, e in quello dei sistemi di riconoscimento facciale, in specie, benché non li ri-

¹⁰ Ai sensi dell'art. 3 n. 4 *AI Act*, il *deployer* è «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza una sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale».

chiamino espressamente. Si pensi all'esigenza che i set di dati di addestramento, convalida e prova siano conformi agli standard di qualità previsti dall'art. 10 §§ 2-5, che riveste particolare rilievo in un contesto nel quale l'affidabilità dell'*output* del sistema poggia proprio su come è stato effettuato il *training*, in modo da assicurare che sia credibile e non discriminatorio¹¹. Si pensi anche alla dimensione particolare che assumono in sede giudiziaria le garanzie legate alla trasparenza dei sistemi e alla sorveglianza umana, che impongono ad esempio che il giudice che si trovi ad utilizzare i risultati di un sistema di identificazione *AI based* sia non solo in condizione di comprenderne il funzionamento in base a un assetto di istruzioni chiaro e comprensibile, ma anche di essere reso edotto del rischio di farci eccessivo affidamento in sede di adozione delle proprie decisioni (art. 14 § 4 lett. b *AI Act*).

¹¹ Il tema dei margini di errore dei sistemi di riconoscimento facciale, dei *bias* e della qualità dei dati di riferimento, oltre che di quelli sui quali i modelli algoritmici dei sistemi sono progettati e allenati, è tra i più sondati nella letteratura di riferimento. È noto, infatti, che l'affidabilità dei FRS è più bassa e a maggiore rischio di distorsione rispetto ad altri sistemi identificativi, sia perché il volto umano ha un grado di riferimento individualizzante più basso rispetto ad altri dati biometrici, sia perché la categorizzazione dei dati di riferimento iniziali può essere in sé discriminatoria, sia perché le scelte sulle categorie di dati che l'algoritmo deve valutare in sede di allenamento possono non rispecchiare la varietà adeguata che consenta comparazioni più affidabili. A ciò peraltro vanno aggiunte la qualità e le caratteristiche delle immagini di riferimento, che possono influenzare negativamente l'attendibilità dei risultati in ragione di diverse variabili, come la risoluzione delle immagini, i riflessi della luce, il movimento, ma anche le caratteristiche fisionomiche della persona, quali età, colore della pelle, espressione facciale, e così via. In argomento, cfr., anche per ulteriori riferimenti, J. DALLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, cit., p. 20; F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 135 s.; G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 217 ss.; E. SACCHETTO, *Tecnologie di riconoscimento facciale*, cit., p. 74 ss.; nonché J. BUOLAMWINI, *When the robot doesn't see dark skin*, in *The New York Times*, 21 giugno 2018. Può essere interessante osservare che, con riferimento all'ampio spettro dei dati biometrici e al loro impiego in molti campi, già da tempo si è fatta strada il concetto di "disabilità biometrica", per segnalare i rischi di maggiore discriminazione ai danni di alcune fasce di utenti rispetto proprio alle caratteristiche e variazioni dei dati di riferimento e alla conseguente inattendibilità degli output (cfr. COMITATO NAZIONALE PER LA BIOETICA, Presidenza del Consiglio dei Ministri, *L'identificazione del corpo umano: profili bioetici della biometria*, 26 novembre 2010, p. 16). Va altresì rammentato come, per contro, valga per i sistemi di riconoscimento facciale il fenomeno di impropria influenza dei sistemi di intelligenza artificiale sul giudizio umano definito *automation bias*, e consistente nell'attitudine dell'intelligenza artificiale ad essere considerata più affidabile di quella umana – in forza delle sue basi scientifiche e tecnologiche – sicché questa tende a riporvi una fiducia "cieca" agli errori e alle opacità che invece connotano gli algoritmi: v. P. COMOGLIO, *Prefazione*, in J. NIEVA-FENNOLL (a cura di), *Intelligenza artificiale e processo*, Torino, 2019, p. X s.; G. UBERTIS, *Perizia, prova scientifica e intelligenza artificiale nel processo penale*, in *Sistema penale (web)*, 3 giugno 2024, p. 14; F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 137.

Infine, i requisiti richiesti per gli applicativi di questo tipo dal Regolamento europeo vanno verificati per gli strumenti già in uso e per quelli adottabili in futuro all'interno del sistema. Basti richiamare i connotati di «accuratezza, robustezza e cybersicurezza» o il novero degli obblighi dei fornitori dei sistemi, per comprendere come siano tutti da verificare i connotati dei *tools* oggi a disposizione del sistema nazionale o del mercato, per consentirne un impiego in ambiti delicatissimi come quello della giustizia penale.

3. *L'impatto sul sistema interno, tra legislazione codicistica e novellazione*

L'*Artificial Intelligence Act* ha dunque una trama fitta e complessa, con riferimento ai sistemi in esame, trama che può riverberarsi sul sistema interno in vario modo, ma che comporta *in primis* una presa di posizione da parte del legislatore nazionale, che invece pare più cercare di guadagnare tempo, che di affrontare la questione in modo sistematico. Vero è che la fonte di riferimento è regolamentare e che quindi dovrebbe in astratto essere suscettibile di applicazione diretta, vantando una certa autonomia rispetto alle probabili esitazioni degli Stati membri. Tuttavia, l'*AI Act* ha una struttura che non sempre si presta ad applicazioni in via immediata, esigendo piuttosto - talora esprimendosi esplicitamente in tal senso - un'articolata normativa nazionale che ne recepisca gli input e li adatti all'ordinamento interno¹². Quest'ultimo dovrà adeguarsi rapidamente, pena la paralisi, alla luce della fitta trama di divieti ed eccezioni circoscritte e subordinate a una serie di regole specifiche, sulle quali non può, alla lunga, esimersi dal pronunciarsi.

Quelli che sembrano infatti immediatamente applicabili sono di certo i divieti, che bloccano semplicemente l'impiego di strumenti *AI based* che non rispondano ai criteri minimali di salvaguardia che sono richiesti o che

¹² La scelta di adottare le norme in esame con lo strumento regolamentare invece che con una direttiva, in effetti, poteva anche suonare singolare: la direttiva avrebbe di certo espresso meglio quell'esigenza di flessibilità e adattamento a livello nazionale che molta parte del regolamento di fatto presuppone e prescrive addirittura; tuttavia, la fonte regolamentare offre maggiore chiarezza e consente di assicurare applicazioni minime più omogenee fra gli Stati membri. Così M. TORRE, *Il Regolamento europeo*, cit., p. 1534; nonché, adesivamente, F. DEMARTIS, *I sistemi automatici di riconoscimento facciale*, cit., p. 79; v. anche A. SIMONCINI, *La proposta di regolazione europea dell'intelligenza artificiale: prime riflessioni*, in A. ADINOLFI - A. SIMONCINI (a cura di) *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle conseguenze giuridiche*, Napoli, 2022, p. 10. Segnala le critiche al ricorso al regolamento, sottolineando tuttavia la difficoltà di individuare percorsi alternativi, S. QUATTROCOLO, *Intelligenza artificiale e processo penale*, cit., p. 2 s.

rientrano *tout court* in quegli ambiti di intollerabile pericolosità che ne precludono l'utilizzo in ogni caso. Lo *scraping*, per esempio, è in ogni caso vietato e ci si dovrà chiedere se reputare inutilizzabile radicalmente ogni forma di riconoscimento facciale che sia eventualmente basata su simile forma di raccolta indiscriminata e incontrollata di dati personali fisionomici.

La verifica coinvolge non solo i tipi di utilizzo, però, come avviene nella sede del procedimento penale, ma anche i sistemi in quanto tali, ove non rispondano ai criteri di garanzia minima richiesti dal regolamento: gli applicativi di polizia di uso comune, ad esempio, dovranno essere assoggettati a un vaglio critico accurato, per verificare se rispondano o meno agli standard di sicurezza e affidabilità che la disciplina europea richiede¹³.

Più complesso, invece, l'assetto del sistema rispetto agli ambiti per i quali la disciplina regolamentare chiede che il legislatore nazionale si pronunci. Il problema si pone, nell'ordinamento interno, su due piani e in modi diversi, tenendo conto dei diversi livelli di rischio e delle differenti declinazioni delle tutele riferibili alle due note forme di riconoscimento facciale, in tempo reale e *a posteriori*. Nel primo caso, infatti, ci troviamo dinanzi a un'attività vietata, salve le eccezioni ammesse dal regolamento, per le quali si esige però una normativa di dettaglio nazionale; nel secondo, si tratta invece di un'attività consentita, ma ad alto rischio, per la quale comunque si esige una disciplina di contesto che articoli adeguate garanzie nel singolo Stato membro.

Per entrambi, il sistema italiano è assai indietro ed ha perso nel 2025 un'occasione preziosa per prendere posizione.

Nella prima ipotesi, quella dei riconoscimenti in tempo reale, la normativa regolamentare è esplicita nel sancire un divieto, che è derogabile solo in una serie tassativa di ipotesi, non immediatamente applicabile a livello interno, in assenza di una normativa che si faccia carico di definirne i contorni. A tacer d'altro, si dovrebbero individuare i reati che costituiscono l'ambito operativo della terza eccezione, oltre alle caratteristiche del procedimento autorizzativo (requisiti, struttura dei provvedimenti, autorità competenti, tempistica, e così via). Del resto, è lo stesso Atto sull'IA a

¹³ Questo comporta che il destino del SARI in Italia sia quanto meno dubbio. Anche rispetto al modello *Enterprise*, infatti, la dottrina ha osservato come non siano mai state rese pubbliche informazioni sul suo funzionamento, risultando ignoti i dati di ricerca con cui opera il sistema, i test sull'idoneità di riconoscimento, nonché i dati sui falsi positivi e negativi o su come sia validato il sistema: cfr. G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale*, cit., p. 10; E. SACCHETTO, *Tecnologie di riconoscimento facciale*, cit., p. 231 s.; R.V. O. VALLI, *Sull'utilizzabilità processuale*, cit.

richiedere al legislatore nazionale la predisposizione di una disciplina legislativa di dettaglio. In assenza di questa, si dovrebbe ritenere che l'attività per la quale manca la base normativa che ammetta e definisca l'area delle eccezioni legittime, resti *tout court* vietata: plausibile, che la presenza del divieto espresso comporti, per quel che ci riguarda, che l'uso dei sistemi sia precluso e che i relativi risultati siano comunque inutilizzabili.

Meno nitido il contesto di riferimento per le attività che sono invece di per sé tollerate, benché considerate ad alto rischio. Per queste, infatti, non siamo di fronte a un divieto radicale, ma ad una serie di prescrizioni di dettaglio atte a garantirne un uso sicuro, affidabile e insuscettibile di avere riflessi negativi sui diritti fondamentali (inclusi quelli che si snodano nella trama del rito penale), che tuttavia comportano alcune preclusioni espresse. Queste ultime si direbbero immediatamente applicabili: ad esempio, l'uso non mirato, al di fuori di un procedimento penale, è vietato di per sé e la previsione pare immediatamente applicabile e non sembra necessitare di specificazioni. Di puntualizzazioni si potrebbe in teoria fare a meno anche per quanto riguarda la regola di valutazione, che impone di non adottare decisioni che possano avere effetti negativi su una persona "unicamente" sulla base dell'output di un sistema di identificazione biometrica *a posteriori*; la "traduzione" processualpenalistica della regola pare essere l'esigenza di non porre a base di un provvedimento *contra reum* (si direbbe, di qualunque natura, quindi anche cautelare) il risultato di un riconoscimento facciale *a posteriori*, quando non sia parte di un corredo di elementi conoscitivi di diversa natura, ossia non da solo. Sulla funzione e sul peso entro tale corredo probatorio il regolamento non si pronuncia, quindi la sola cosa certa è che l'output di sistema non possa sostenere la decisione come fattore esclusivo, ma debba essere componente di un paniere conoscitivo più articolato: nulla vieta però che in tale ambito possa di fatto risultare decisivo, a meno che non sia la normativa nazionale a precisare tale esigenza, strutturando meglio la regola di valutazione. Anche il punto che riguarda l'esigenza che l'identificazione risultante dal sistema non venga usata se non previa conferma separata di due persone fisiche adeguatamente competenti, formate e dotate della necessaria autorità, sembra apparentemente immediatamente applicabile, dovendosi andare a verificare se il sistema interno preveda già questo doppio filtro, di fatto; tuttavia, anche qui c'è spazio per il dettaglio normativo, se si pensa all'esigenza di standardizzare questo tipo di controllo, di fare in modo che operi in modo omogeneo coinvolgendo effettivamente soggetti preparati in una solida filiera, nonché al fatto che lo stesso regolamento consente nelle attività di contrasto di fare a meno di questa regola, se reputata sproporzionata (e quindi il legislatore potrebbe individuare casi eccezionali nei quali farne a meno per ragioni di efficienza).

Più ardua la questione dal punto di vista del procedimento autorizzativo, per il quale è necessaria una normativa interna, non foss'altro per sciogliere le questioni che il regolamento lascia parzialmente aperte, sui tempi (*ex ante* o entro 48 ore al massimo), sulle autorità competenti (giudiziaria o amministrativa) sui controlli (va strutturato un controllo giurisdizionale successivo obbligatorio, con un iter specifico, che il regolamento non struttura affatto). L'unico elemento che in questo quadro è chiaro, è che di tale assetto si può fare a meno per l'impiego del riconoscimento facciale per l'identificazione iniziale di un sospetto (che tale sia in base a fattori oggettivi differenti), sicché per un impiego limitato a questo, l'utilizzo nel rito penale dovrebbe reputarsi legittimo anche in assenza di indicazioni normative ulteriori. Oltre questo, però, una presa di posizione del legislatore è essenziale e ci si dovrebbe chiedere se, in difetto di essa, un impiego che vada oltre l'identificazione iniziale sarebbe legittimo, nel sistema interno. Il tema è complesso, perché non risulta in questo caso un divieto esplicito, benché esso possa desumersi indirettamente dalla formulazione normativa del regolamento, che considera obbligatoria l'autorizzazione e che sancisce che in sua assenza (*rectius* in caso di rigetto), i dati debbano essere cancellati. La delicatezza del punto, però, oltre alla complessità esegetica dell'assetto italiano in tema di inutilizzabilità, spingono a consigliare una presa di posizione esplicita da parte del legislatore.

Non è di grande aiuto, in questo contesto, la strategia attendista sinora adottata dal legislatore italiano. In un primo momento, sull'onda delle questioni sollevate dal Garante della privacy sul sistema SARI, il d.l. 8 ottobre 2021, n. 139, conv. legge 3 dicembre 2021, n. 205, ha sospeso fino all'entrata in vigore di un'apposita disciplina legislativa sulla materia¹⁴ l'installazione e l'utilizzo di impianti di videosorveglianza muniti di sistemi di riconoscimento facciale in luoghi pubblici o aperti al pubblico, riguardante soggetti sia pubblici che privati. La *ratio*, dichiarata nello stesso tenore normativo, è proprio quella di fare da ponte a una disciplina organica della materia, nel frattempo rispettando i principi fondamentali sanciti in quest'ambito dalle fonti europee¹⁵, con particolare riferimento al principio di proporzionalità *ex art.* 52 Carta dir. fond. UE. Anche qui, però, a rilevare sono proprio le eccezioni, giacché si sottraggono alla moratoria tutti i trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione delle sanzioni penali, che possono proseguire previo parere favorevole del Garante della priva-

¹⁴ E comunque non oltre il 31 dicembre 2025.

¹⁵ Si menzionano il reg. (UE) 2016/679 e la Direttiva 2016/680.

cy, e anche a prescindere da questo, quando siano trattamenti effettuati dall'autorità giudiziaria o giurisdizionale (dunque, sia giudice che pubblico ministero) (art. 9 comma 12 d.l. n. 139 del 2021 conv. legge n. 205 del 2021). La previsione è estremamente inadeguata, non solo perché opera nella sola prospettiva del principio di proporzionalità e del diritto alla privacy, che sono insufficienti a coprire la complessità dei valori in gioco, ma anche perché sembra addirittura autorizzare un'apparente *deregulation* per gli impianti in uso alle autorità di contrasto, che l'attuale disciplina europea invece non tollererebbe. Anche i primi commentatori, del resto, hanno sottolineato come la clausola sia criticabile per le sue lacune, perché non distingue fra riconoscimento *a posteriori* e in tempo reale, per le omissioni proprio in punto di bilanciamento di interessi, visto che non precisa né i canoni dell'impiego per stretta necessità, né il grado di gravità dei reati per cui gli impieghi di tali sistemi sarebbero consentiti, perché non specifica neppure i tempi di conservazione dei dati raccolti¹⁶. La sua censurabile vaghezza, quanto meno, andrebbe letta non come una liberalizzazione indiscriminata all'uso a fini penalistici, ma come mera sottrazione dell'ambito della giustizia penale alla moratoria sancita dal provvedimento, fermi restando i limiti derivanti dal resto della normativa sovraordinata e codicistica¹⁷.

Era lecito aspettarsi di più dalle «disposizioni e deleghe al Governo in materia di intelligenza artificiale», che, *ratione materiae*, erano la sede adatta per dare coordinate visibili alla tematica dei sistemi di identificazione biometrica in genere e di riconoscimento facciale in particolare. Anche in questo caso, però, l'attesa è stata delusa: non solo mancano disposizioni specifiche su questo tema, ma anche il contenuto della delega è del tutto generico, facendo riferimento a un'ampia delega al Governo all'adozione di «uno o più decreti legislativi per l'adeguamento della normativa nazionale a regolamento (UE)2024/1689» (art. 24 legge 23 settembre 2025 n. 132), con un richiamo ai vaghissimi criteri direttivi già contenuti per l'attuazione delle direttive nella legge 24 dicembre 2012, n. 234, e poi a una lunga serie di criteri aggiuntivi, quasi nessuno dei quali applicabili alla materia che qui ci occupa. Solo uno – senza però riferimenti espliciti al tema del riconoscimento facciale – rileverà, pur dicendo l'ovvio, ossia asse-

¹⁶ E. SACCHETTO, *Tecnologie di riconoscimento facciale*, cit., p. 161 s.

¹⁷ J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale*, in I. MICHELI (a cura di), *Ragioni Comuni 2019-2020. Risultati delle attività progettuali realizzate tramite assegni di ricerca finanziati dalla Regione Friuli Venezia Giulia ai sensi della LR34/2015, art. 5, commi 29-33*, EUT Edizioni Università di Trieste, Trieste, 2023, p. 178; nonché E. SACCHETTO, *Tecnologie di riconoscimento facciale*, cit., p. 162 s.

gnando la delega al Governo per l'adozione di una «apposita disciplina per l'utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia» (art. 24 comma 2 lett. *b* legge n. 132 del 2025) che, a tacer d'altro, neppure suona come un vero criterio direttivo, ma piuttosto come un'integrazione contenutistica della delega già attribuita.

Tra le disposizioni che invece sono di immediata applicazione e contengono quindi scelte più nette e già affrontate dal legislatore, l'unica in qualche modo riferibile al sistema penalistico è l'art. 15 legge n. 132 del 2025, che ancora una volta è nebulosa nella sua genericità. La previsione prescrive che, ove vi sia un impiego dei sistemi di intelligenza artificiale nell'attività giudiziaria, «è sempre riservata al magistrato ogni decisione sull'interpretazione e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti». La norma non sembra tracciare nulla di più che una clausola di ampia trasposizione in campo giudiziario del canone di “supervisione umana”, che impone di non lasciare che i sistemi di IA si sostituiscano agli utilizzatori quando si adottino decisioni che spettano alle persone fisiche, quali sono tipicamente tutte quelle che si collocano entro il perimetro di un procedimento penale. Peraltro, nel campo del riconoscimento facciale, non appare presidio sufficiente: i sistemi di identificazione biometrica infatti non sono deputati di per sé ad adottare decisioni o ad influenzare direttamente la valutazione delle prove già in atti o l'esegesi della legge (come avviene invece per gli algoritmi predittivi della recidiva o per quelli che ricostruiscano gli orientamenti giurisprudenziali su una data questione). Si può dire che la previsione, per quanto riguarda ad esempio la valutazione dei fatti, preclude indirettamente che lo strumento di identificazione fornisca un output che da solo fondi la decisione del giudice, che sarebbe altrimenti troppo condizionato e quindi “non autonomo” nell'adozione del provvedimento. Ma è palese che la clausola sia di troppo vasta portata per risultare davvero utile ai nostri fini, rispetto ai quali semmai i divieti già sanciti in sede europea sono assai più chiari.

Da ultimo, va rammentato che anche rispetto all'eventuale impiego nel rito penale di applicativi che verifichino gli stati emozionali, il quadro risulta più complesso di quanto non si potrebbe affermare in prima battuta. Il sistema del regolamento non preclude radicalmente tale uso, che tuttavia non potrebbe che collocarsi nell'ambito di una precisa scelta normativa, giacché condizione essenziale per l'utilizzo di simili applicativi è senz'altro – anche nella prospettiva europea – il rispetto di un bilanciamento tra interessi e uno specifico assetto di tutele stabiliti per legge. Inoltre, la legge dovrebbe comunque tenere conto di divieti e cautele sanciti non direttamente, ma indirettamente, perché riferibili, se non espressamente ai sistemi di riconoscimento delle emozioni, a quelli che comun-

che realizzino scopi di per sé vietati o ad alto rischio. Infine si deve tenere conto del fatto che alcuni divieti discendono dalla normativa interna e comportano sovente preclusioni o standards di garanzia più alti di quelli tracciati a livello europeo. Un esempio delle problematiche appena rammentate è dato dal poligrafo ed analoghi strumenti, che servano a misurare le reazioni emotive alle domande rivolte al dichiarante nel rito penale per stabilire la veridicità delle risposte e il tasso di attendibilità delle dichiarazioni: sono considerati dall'*AI Act* ad alto rischio (All. III, § 6 lett. b), benché non vietati¹⁸, ma andrebbero comunque a collidere con l'art. 188 c.p.p. In altri termini, non potrebbero in ogni caso essere consentiti come forma tecnologicamente avanzata di “macchine della verità”¹⁹. In questa direzione sembra andare anche il rammentato art. 15 legge n. 132 del 2025, che preclude che al magistrato possa essere sottratta la supremazia nella valutazione delle prove, sicché andrebbe riservato comunque alla persona fisica il vaglio finale, ad esempio, sull'attendibilità di un testimone le cui emozioni fossero decifrate da uno strumento di “lettura del volto” basato sull'intelligenza artificiale. Tuttavia, va detto, l'art. 15, a differenza dell'art. 188 c.p.p., non suona come un divieto assoluto: riservare al magistrato la decisione, infatti, non sancisce l'assoluta inutilizzabilità di uno strumento, ma solo che non prenda il sopravvento rispetto al giudicante e quindi, ad esempio, che non sia unico o decisivo elemento di valutazione e che non vada così in alcun modo (neppure indirettamente) a sostituirsi al giudizio umano. Non è questa, però, l'indicazione netta che ci si attendeva e che sarebbe stata utile.

Del resto, è proprio sul versante del riconoscimento delle emozioni, che si possono invece immaginare impieghi possibili degli applicativi oggi disponibili e sempre più sofisticati. Si pensi alla possibilità di verificare in tempo reale, nell'assunzione di sommarie informazioni da parte di un minorenni o di un soggetto vulnerabile, se le domande poste dall'operatore causino disagio, imbarazzo, paura, emozioni negative che consiglierebbero di interrompere l'atto, fare una pausa o persino sostituire l'operatore con un altro più accorto e preparato. Si potrebbe, in altri termini, immaginare di rovesciare la prospettiva, permettendo un uso di tali applicativi per rivelare le possibili violazioni dell'art. 188 c.p.p. commesse

¹⁸ E comunque fatte salve le cautele correlate al grado di rischio, illustrate nel regolamento.

¹⁹ Il tema, peraltro, è più delicato e complesso di quanto non si possa dire a prima lettura: per una analisi problematica, cfr. G. CASONE, *Emotional biometrics: a preliminary analysis of critical aspects concerning the use of the last AI frontier in criminal procedure*, in P. ARRABAL PLATERO, G. CONDE FUENTES, P. GARCIA MOLINA (a cura di), *El proceso en tiempos de cambio*, Editorial Colex, Coruna, 2023, p. 298 s.

dalle persone fisiche attraverso un uso aggressivo, manipolativo o abusante delle domande rivolte ai soggetti fragili. Nulla poi vieterebbe di impiegare questi strumenti in sede di formazione del personale specializzato, per fare “sperimentare” (ovviamente con soggetti non coinvolti nei procedimenti penali) le reazioni degli interrogati alle domande improvvisamente formulate dagli interroganti e persino le “reazioni facciali” e quindi emotive di questi ultimi alle risposte, per verificare come possono influenzare a loro volta coloro che rilasciano dichiarazioni.

Si tratta di una possibilità che rivela un'esigenza di fondo: con uno sforzo di immaginazione, gli strumenti di intelligenza artificiale hanno molto da offrire. L'importante è essere consapevoli delle implicazioni negative e bilanciarne adeguatamente gli impieghi rispetto ai possibili rischi. È una sfida alla quale è praticamente impossibile sottrarsi e che il legislatore dovrà prima o poi affrontare. Meglio che sia prima che un'IA incontrollata si insinui comunque nelle pieghe del sistema e prenda subdolamente il sopravvento.

PARTE SECONDA

USO, CONSERVAZIONE, CIRCOLAZIONE

QUALE FUTURO PER LA PROVA BIOMETRICA? RIFLESSIONI AL CROCEVIA TRA GARANZIE DELL'INDIVIDUO E ACCERTAMENTO PENALE

ELEONORA DEI-CAS

SOMMARIO: 1. Dalla fallacia umana, a quella della macchina. – 2. Il “divieto-non divieto” e “l’alto rischio insufficientemente governato” dell’*AI Act* a proposito di riconoscimento biometrico remoto. – 3. Futuribili per una normativa interna improntata alle garanzie individuali.

1. *Dalla fallacia umana, a quella della macchina*

Con «pareidolia» si definisce la tendenza naturale della psiche umana a ricondurre ogni immagine vaga a cose conosciute e, in special modo, a volti umani¹. Risulta quindi controintuitivo, forse, come, nonostante sia per natura portato a vedere facce nelle forme ignote, la scienza abbia dimostrato l'estrema inabilità dell'uomo nel riconoscere i propri simili, soprattutto se appartenenti a soggetti a lui sconosciuti² e, ancora di più, se di etnia diversa dalla propria³.

Da qui l'inaffidabilità – comunemente data per assodata – del tradizionale mezzo di prova della ricognizione, dovuta alla fallacia della memo-

¹ Sul fenomeno, R. FALCINELLI, *Visus. Storie del volto dall'antichità al selfie*, Einaudi, Torino, 2024, p. 48 ss.

² T.C. BENNETT-H.M.J. SMITH-H.D. FLOWE, *Advances and Future Prospects in Evolving Face Matching Technologies for Crime Prevention and Investigation*, in E. PICA-D. ROSS-J. POZZULO (edited by), *The Impact of Technology on the Criminal Justice System. A Psychological Overview*, Routledge, New York and Abingdon, 2024, p. 77-78, e T.D. ALBRIGHT-B.L. GARRETT, *The Law and Science of Eyewitness Evidence*, in *Boston University Law Rev.*, 102/2(2022), p. 521 ss., cui si rimanda anche per gli studi psicologici citati.

³ C.d. *other race/cross racial effect*, sul quale, per tutti, A. BERNASCONI, *La ricognizione di persone nel processo penale. Struttura e procedimento probatorio*, Giappichelli, Torino, 2003, p. 19, nota 33, e T.D. ALBRIGHT-B.L. GARRETT, *The Law and Science of Eyewitness Evidence*, cit., p. 516 e p. 557.

ria umana⁴, alla suggestionabilità del soggetto effettuatore⁵ e agli effetti che il normale decorso del tempo provoca sulla capacità di ricordare; fattori, questi ultimi, che hanno fatto sì che i “testimoni oculari”⁶, quantunque in perfetta buona fede, siano annoverati fra le principali fonti di errori giudiziari conclamati⁷. Non a caso, il codificatore del 1988-1989 ha tem-

⁴ Fallacia che si estende anche alla diversa, ma contigua, attività di rievocazione delle singole caratteristiche del volto ai fini dell'*identikit*: al riguardo T. ALESCI, *Il corpo umano fonte di prova*, Cedam, Milano, 2017, p. 90.

Con precipuo riferimento all'errore nel riconoscimento, quale causa da cui è scaturito l'interesse verso gli strumenti automatizzati, di recente, G. BORGIA-M. ZONARO, *L'errore nel riconoscimento automatizzato*, in W. NOCERINO (a cura di), *L'errore tecnico e la prova penale*, Pacini giuridica, Pisa, 2025, p. 176 ss.

⁵ M. BONTEMPELLI, *La ricognizione nel processo penale*, Giappichelli, Torino, 2012, p. 2, nota 4. Nella letteratura estera, seppure in relazione a istituti non del tutto sovrapponibili al nostro mezzo di prova, S.M. BOWEN, *Man vs. Machine: Facial Recognition Technology Replacing Eyewitness Identifications*, in *Lincoln Memorial University Law Rev.*, 10/1(2022), p. 21 ss. Proprio per evitare suggestioni, è ricorrente la necessità di avvalersi di agenti che non sappiano quale persona, presente nel *lineup*, sia la sospettata (agente “blind”): si veda il report del National Research Council, *Identifying the Culprit. Assessing Eyewitness Identification*, Washington D.C., The National Academies Press, 2014, p. 106-107. Sulla procedura cieca, B.L. GARRETT, *Eyewitness Identifications and Police Practices: A Virginia Case Study*, in *Virginia Journ. Crim. Law*, 2/1(2014), p. 3, p. 11 e p. 15 ss., nonché T.D. ALBRIGHT-B.L. GARRETT, *The Law and Science of Eyewitness Evidence*, cit., p. 580 ss., Annex A, per una sintesi delle legislazioni statali USA che prevedono *policies* cieche.

⁶ L'espressione viene utilizzata in relazione a ordinamenti diversi dal nostro. A dispetto di letture giurisprudenziali disinvolute, è chiaro come, nel sistema italiano, la ricognizione non possa essere trattata alla stregua di una *species* della testimonianza: per tutti, in tal senso, N. PASCUCCI, *Un nodo ancora da sciogliere nel processo penale: il riconoscimento informale di persona in udienza*, in *Riv. dir. proc.*, 2018, p. 723, con la copiosa dottrina richiamata alla nota 9.

⁷ Sugli errori giudiziari dovuti alla malleabilità della memoria umana – partendo dal grave errore giudiziario inglese nel caso *Malkinson*, costato a un innocente diciassette anni di carcere (*Malkinson v. King* [2023] EWCA Crim 954) –, A. ROBERTS-D. ORMEROD, *Improving Identification Procedures: Time for Devlin 2.0?*, in *Crim. Law Rev.*, 5(2024), p. 328, anche per la dottrina citata a nota 16. Da una prospettiva psicologica, H.M. KLEIDER-OFFUTT-B.B. STEVENS, *Is Facial Recognition Software a Solution to the Negative Effects of Social Media on Eyewitness Testimony?*, in E. PICA-D. ROSS-J. POZZULO (edited by), *The Impact of Technology on the Criminal Justice System. A Psychological Overview*, cit., p. 397 ss. Nel mondo nordamericano, INNOCENCE STAFF, *How Eyewitness Misidentification Can Send Innocent People to Prison*, The Innocence Project, (April 15, 2020), innocenceproject.org/how-eyewitness-misidentification-can-send-innocent-people-to-prison/, nonché T.D. ALBRIGHT-B.L. GARRETT, *The Law and Science of Eyewitness Evidence*, cit., p. 515 ss., e G.L. WELLS, *Psychological Science on Eyewitness Identification and Its Impact on Police Practices and Policies*, in *American Psychologist*, 75/9(2020), p. 1316 ss., spec. p. 1322, ove, muovendo dagli studi psicologici che hanno dimostrato che il rischio maggiore di errato riconoscimento deriva dalla mancata ricomprensione dell'autore del fatto tra i soggetti da riconoscere, raccomanda di mostrare un sospettato nel *lineup* allestito prima del giudizio solo là dove esistano già elementi a suo carico. Per altri esempi, B.L. GARRETT, *Eyewitness Identifications and Police Practices: A Virginia Case Study*, cit., p. 7 ss.

pestatò il mezzo di prova in questione di adempimenti e salvaguardie⁸, volti, almeno nelle intenzioni, a ridurre il rischio di fare entrare nella piattaforma conoscitiva del giudice riconoscimenti errati, sebbene i paletti normativi siano puntualmente aggirati dal diritto pretorio⁹.

A ciò si aggiunge poi la labilità della memoria, soggetta a decadimento irreversibile, essendo «nella natura degli atti ricognitivi consumare in fretta le proprie energie: sono tanto più attendibili quanto più prossimi ai fatti, tanto più credibili quanto meno preceduti da altri riconoscimenti, in qualunque modo effettuati, finanche indiretti od occasionali»¹⁰. Il che, dato i tempi con cui si celebrano oggi giorno i dibattimenti, non può che amplificare le problematicità congenite del mezzo di prova.

Su questo sfondo assai poco tranquillizzante per la bontà dell'accertamento, i prodigi della tecnica hanno fatto breccia, convincendo tecnici e operatori – prima ancora che legislatori¹¹ – che le moderne tecnologie

⁸ Similmente al *case law* americano relativo al *lineup*: United States v. Wade, 388 U.S. 218 (1967) 236, nota 26, in cui viene citato D.E. MURRAY, *The Criminal Lineup at Home and Abroad*, in *Utah Law Rev.*, 3(1966), p. 610 ss., che risente dell'invito alla cautela, volto a ridurre l'errore, proveniente da J.H. WIGMORE, *A Treatise on the Anglo-American System of Evidence in Trials at Common Law. Including the Statutes and Judicial Decisions of All Jurisdictions of the United States and Canada*, vol. III, Third edition, Little, Brown and company, Boston, 1940, p. 164-165. Approccio cauto che Murray (p. 624-625) paragona alla disciplina spagnola del 1882, che a sua volta ricorda quella italiana della ricognizione nel codice del 1930.

⁹ Il riferimento corre, naturalmente, ai riconoscimenti informali in udienza o fotografici, pacificamente ricondotti dalla giurisprudenza alla categoria della prova atipica, sebbene più propriamente da ritenersi irrituali in quanto *contra legem* (M. NOBILI, *Commento all'art. 189 c.p.p.*, in M. CHIAVARIO (coord. da), *Commento al nuovo codice di procedura penale*, vol. II, Utet, Torino, 1990, p. 398-399): sui primi, da ultimo, Cass., Sez. II, 31 marzo 2022, Mannolo, in *C.e.d.*, n. 283392; in dottrina, N. PASCUCCI, *Un nodo ancora da sciogliere nel processo penale: il riconoscimento informale di persona in udienza*, cit., p. 721 ss. Sui secondi Cass., Sez. III, 30 giugno 2016, C.A., in *Riv. it. dir. proc. pen.*, 2017, p. 285 ss., con nota critica di N. PASCUCCI, *La natura controversa della ricognizione fotografica*. Nel senso che l'«atipicità della prova rappresenta un concetto eversivo della legalità processuale», O. MAZZA, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Dir. pen. cont.*, 2013, f. 3, p. 8.

¹⁰ Così, C. CESARI, *Individuazione e dibattito: limiti e rischi dell'uso a fini contestativi di un atto di indagine*, in *Critica dir.*, 1995, p. 142 ss.

¹¹ In molti hanno, negli anni, denunciato l'immobilismo dei legislatori nel normare una materia come quella in discorso, capace di intaccare in modo significativo i diritti fondamentali. Per tutti, sulla sostanziale mancanza in Europa di una cornice giuridica che regolamenti l'uso delle tecnologie in esame: S. KUHLMANN, *Government Use of Facial Recognition Technologies under European Law*, in R. MATULIONYTE-N. ZALNIERIUTE (a cura di), *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge University Press, Cambridge, 2024, p. 127. L'assunto viene tuttavia contestato da chi fa leva sul quadro dei diritti riconosciuti dalla grande e piccola Europa in tema di diritto al rispetto della vita privata e di diritto ai dati personali: F. DI MATTEO, *La riservatezza dei dati biometrici nello spazio europeo dei diritti fondamentali: sui limiti all'utilizzo delle tecnologie di riconoscimento facciale*, in *Freedom, Security & Justice: European Legal Studies*, 1(2023), p. 109.

potessero porre fine ai problemi ravvisati, in ragione di una (più pretesa che reale) infallibilità della macchina¹².

Certo, al fenomeno ha contribuito in misura più che significativa il fatto che le nostre città siano costellate di telecamere¹³, per cui, al verificarsi di un fatto penalmente rilevante, diventa sempre più probabile che gli inquirenti riescano a rinvenire immagini rappresentative di quanto avvenuto sul luogo o in sua prossimità, venendo quindi a disporre di un «ricognitore potenzialmente perenne»¹⁴. A queste si sommano le fotografie che gli utenti stessi caricano sui *social media*, vera e propria miniera di volti per allenare gli algoritmi, come ha dimostrato il caso *Clearview*¹⁵, nonché le riprese fatte da passanti, da droni o da *body-cam*. Aspetto, quest'ultimo, con ogni probabilità destinato a crescere ulteriormente, se si pensa ai fon-

¹² A. FRAERMAN, *Relying on Unreliable Tech: Unchecked Police Use of Algorithmic Technologies*, in *Santa Clara High Technology Law Journ.*, 40/2(2024), p. 128, che tratta l'*automation bias*. Sull'aura di infallibilità, si vedano anche C. CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, 5/3(2019), p. 1183 (anche per il riferimento contenuto nella nota 30); S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, 2020, p. 90, e S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 100.

Per un parallelismo tra strumenti tecnologici in parola e DNA, entrambi considerati «portat[ori] di assunti di verità pressoché assoluta e insuscettibili di essere efficacemente confutati», F. NICOLICCHIA, *Tecniche di riconoscimento biometrico e fisionomia dell'accertamento: i caratteri dell'istruttoria nella procedura penale algoritmica*, in A. CAPPUCCIO-S. RUGGERI (a cura di), *Antichi e nuovi modelli di giustizia partecipata e cultura della giurisdizione. Verso una tutela penale più umana ed egualitaria*, Cedam, Milano, 2024, p. 205.

¹³ T.C. BENNETT-H.M.J. SMITH-H.D. FLOWE, *Advances and Future Prospects in Evolving Face Matching Technologies for Crime Prevention and Investigation*, cit., p. 73 ss. Sull'utilità dei filmati tratti dalle telecamere a circuito chiuso come strumento investigativo, M.P.J. ASHBY, *The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis*, in *Eur. Journ. Crim. Policy and Research*, 23(2017), p. 441 ss.; J. PURSHOUSE-L. CAMPBELL, *Automated facial recognition and policing: a Bridge too far?*, in *Legal Studies*, 42(2022), p. 210.

¹⁴ D. NEGRI, *Videosorveglianza e analisi di immagini a fini identificativi: una introduzione*, in *Videosorveglianza e analisi di immagini a fini identificativi. Atti del Convegno tenutosi a Ferrara il 13 dicembre 2005 presso l'Aula Magna della Facoltà di Giurisprudenza*, Poliziamoderna, 2006, p. 8.

¹⁵ La notizia è leggibile in [nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html](https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html). Alla storia aziendale di *Clearview* è dedicato il libro-inchiesta della giornalista del *New York Times* K. HILL, *La tua faccia ci appartiene* (2023), trad. it. di V. Parodi, Orville Press, Milano, 2024. Sul punto, I. NERONI REZENDE, *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, in *New Journ. Eur. Crim. Law*, 11/3(2020), p. 375 ss.

Come noto, il caso in questione è all'origine del divieto di *scraping* contenuto nel Regolamento europeo sull'I.A.: F. LALA, *Data collection via web scraping: privacy and facial recognition after Clearview*, in *Riv. scienze giur., scienze cognit. e I.A.*, 2023, f. 16, 2, p. 43.

di stanziati dal recente “d.l. sicurezza” per la dotazione di videocamere al personale delle forze di polizia¹⁶.

E così, oramai da anni, gli “atti omologhi” alla ricognizione “vengono compiuti”¹⁷, in diversi ordinamenti, più da software di riconoscimento facciale (FRTs) che da persone in carne e ossa. La qual cosa, come è evidente, sposta l’attenzione dalle questioni attinenti alla credibilità del teste a quella della affidabilità del risultato originato tecnologicamente. Occorre dunque anzitutto focalizzare l’attenzione sulla necessità di rifuggire da ogni tentazione di atteggiamento fideistico nei confronti della macchina: lungi dall’infallibilità, i risultati prodotti, in primo luogo, dipendono direttamente dalla qualità dei dati in entrata. Per cui, fuori dalle condizioni “di laboratorio”¹⁸, in cui l’arnese informatico è stato alimentato utilizzando materiale di buona risoluzione, perfettamente allineato, col soggetto che guarda in macchina, scattato alla giusta distanza¹⁹, il dare in pasto fotogrammi sbiaditi, magari ripresi da lontano, di notte, e raffiguranti persona parzialmente celata da indumenti o dalla stessa posizione assunta²⁰, produce in uscita un risultato assai meno af-

¹⁶ Art. 21 del d.l. 11 aprile 2025, n. 48, recante disposizioni urgenti in materia di sicurezza pubblica, di tutela del personale in servizio, nonché di vittime dell’usura e di ordinamento penitenziario, convertito senza modificazioni in legge 9 giugno 2025, n. 80.

¹⁷ Invero, attenta dottrina evidenzia come non possa propriamente parlarsi di attività ricognitiva compiuta dalla macchina, anziché dall’uomo, perché a cambiare non è solo l’agente, ma anche il percorso di elaborazione che porta al risultato: in questo senso, G. GALUCCIO MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*, in *Cass. pen.*, 2025, p. 647-648.

¹⁸ Lo scarto a livello di affidabilità tra le due condizioni viene sottolineato da W. CRUMPLER-J.A. LEWIS, *How Does Facial Recognition Work? A Primer*, leggibile in *csis.org/analysis/how-does-facial-recognition-work*, 10 giugno 2021, p. 7-8.

¹⁹ Ad esempio, foto segnaletiche. Preme sottolineare come siano queste le condizioni in cui i *software* venivano validati – soprattutto in passato – dal *National Institute of Standards and Technology* (NIST), falsando, di fatto, le carte: a riguardo, B. FRIEDMAN, *Written Testimony Before the House Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security. Facial Recognition Technology: Examining Its Use by Law Enforcement*, July 13, 2021, p. 8-9. Analogamente, A. FRAERMAN, *Relying on Unreliable Tech*, cit., p. 184, il quale raccomanda che in futuro i test vengano condotti su software effettivamente utilizzati dagli organi di *law enforcement* e sulla base di materiale verosimile. Raccomandazione condivisa dalla National Association of Criminal Defense Lawyers, *Policing Technologies At Issue In Proposed Executive Order 14074*, datata 19 gennaio 2024.

²⁰ Il che vale anche quando l’identificazione fotografica viene fatta da umani: sul punto S. RITZ-TIMME-P. GABRIEL-Z. OBERTOVA-M. BOGUSLAWSKI-F. MAYER-A. DRABIK-P. POPPA-D. DE ANGELIS-R. CIAFFI-B. ZANOTTI-D. GIBELLI-C. CATTANEO, *A new atlas for the evaluation of facial features: advantages, limits, and applicability*, in *Int. Journ. of Legal Medicine*, 125(2011), p. 305. Anche in quel caso, l’espressione del soggetto ritratto può inficiare il risultato del riconoscimento. L’impatto delle espressioni facciali sull’identificazione è oggetto di studio nelle scienze forensi: D. GIBELLI-D. DE ANGELIS-P. POPPA-C. SFORZA-C.

fidabile²¹. Inoltre, sempre fuori dalle condizioni ottimali, è assai frequente che l'immagine iniziale abbisogni di una qualche sorta di modifica, prima di poter essere somministrata alla macchina²². Queste forme di *editing* presentano, in concreto, uno spettro amplissimo, che va dal variare la luminosità o il contrasto, oppure ruotare l'immagine, al copia-incollare elementi del volto non visibili, ad esempio gli occhi chiusi o la bocca nascosta dalla posa. In un caso americano noto, si è addirittura passati dalla modifica alla radicale sostituzione dell'immagine: ritenendo che la persona da riconoscere somigliasse a un attore, alla macchina è stata consegnata la foto di quest'ultimo²³. Tralasciando detta ipotesi, auspicabilmente un *unicum*, non sfugge come l'operazione di modifica sia cruciale, giacché può allontanare il risultato da quello che, in assenza di manipolazione, sarebbe stato raggiunto: occorre quindi serbare traccia di quanto compiuto in modo da sottoporre a controllo successivo, rendendolo noto alla difesa²⁴. Qui la questione non può non fare i conti col fatto che a posteriori l'interessato non sa neppure che per identificarlo è stata utilizzata, nelle primissime fasi delle indagini, la tecnologia in parola: spesso dal fascicolo ciò semplicemente non traspare, come denunciano membri dell'*American Bar Association*²⁵ e anche alcuni studiosi eu-

CATTANEO, *An Assessment of How Facial Mimicry Can Change Facial Morphology: Implications for Identification*, in *Journ. of Forensic Sciences*, 62/2(2017), p. 405 ss.

²¹ A. FRAERMAN, *Relying on Unreliable Tech*, cit., p. 115 ss., spec. p. 121, ove chiosa «If a technology is not reliable, evidence generated from its use should be excluded». Assai meno critico sull'uso della tecnologia in discorso in via generale, H.H. PERRITT JR., *Defending Face-Recognition Technology (And Defending Against It)*, in *Journ. of Technology Law & Policy*, 25/1(2021), Article 2, leggibile in *scholarship.law.nfl.edu/jtlp/vol25/iss1/2*, p. 50, che pur riconosce gli attuali problemi di affidabilità.

Nella giurisprudenza nordamericana, per un caso in cui materiale di scarsa risoluzione è stato usato nel riconoscimento che ha portato all'arresto del soggetto individuato, si veda *Williams v. City of Detroit*, No. 2:21 Civ. 10827.

²² C. GARVIE, *A Forensic Without the Science. Face Recognition in U.S. Criminal Investigations*, in *Center on Privacy & Technology at Georgetown Law*, 2022, p. 11 (ove porta l'esempio del sistema DataWorks Plus che presenta opzioni simili a quelle di Photoshop) e p. 34-35.

²³ K. JACKSON, *Challenging Facial Recognition Software in Criminal Court*, in *The Champion*, *nacdl.org*, 2019, p. 15, che dà conto di come in un caso la foto grezza sia stata sostituita con quella dell'attore Woody Harrelson, somigliante, secondo la polizia di New York, al soggetto ritratto.

²⁴ Una proposta di legge statunitense, mai entrata in vigore, indicava tra gli elementi di cui dare copia all'interessato anche le modifiche alla fotografia (c.d. *probe image*): H.R. 9061, «To regulate law enforcement use of facial recognition technology, and for other purposes» (c.d. «Facial Recognition Act of 2022»), sec. 108 (a) (2) (D).

²⁵ K. JACKSON, *Challenging Facial Recognition Software in Criminal Court*, cit., p. 16; G. GARVIE, *What Defense Counsel Should Know About Facial Recognition Technology*, in *The Champion*, *nacdl.org*, 2023, p. 20.

ropei²⁶. Quando la traccia vi è, nella prassi nordamericana viene negata alla difesa la *disclosure* in ordine a elementi fondamentali²⁷, quali – in prima battuta – il nome del software utilizzato, il codice sorgente e il tasso d'errore dello stesso²⁸; elementi che consentirebbero di contrastare l'avvenuta identificazione²⁹. Tra questi, risulta importante conoscere anche quanti volti sono ricompresi nella banca dati di riferimento, dal momento che il risultato restituito a seguito del raffronto non assume la forma “secca” e binaria di un sì/no, ma viene espressa in termini probabilistici organizzati in scala, la quale dipende in modo apprezzabile dal numero di raffronti effettuati³⁰. Ignorare quest'ultimo dato sbarra pertanto la possibilità di un controllo successivo, già reso difficile dall'oggetto stesso da sottoporre a scrutinio.

Infatti, da una parte, l'affidabilità dell'algoritmo, come ormai risaputo, dipende dal materiale tramite il quale lo stesso è stato allenato³¹. Di

²⁶ M. GALIC-L. STEVENS, *Regulating police use of facial recognition technology in the Netherlands: The complex interplay between criminal procedural law and data protection law*, in *New Journ. Eur. Crim. Law*, 14/4(2023), p. 469: «information concerning an operation involving facial recognition technology does not always end up in a case file, particularly when it is not used for an arrest but just as a lead in the earlier stages of an investigation».

²⁷ C. GARVIE, *A Forensic Without the Science*, cit., p. 8, in quanto le *policies* di diversi dipartimenti di polizia specificano a chiare lettere che il riconoscimento non può da solo giustificare un arresto o costituire la *probable cause* alla base di un mandato di perquisizione, ma è un mero *investigative lead*.

Vanno quindi salutati con favore quei provvedimenti normativi statali che impongono obblighi di *disclosure*: si veda, in particolare la legge dello Stato di Washington RCW 43.386.070, § 1, la quale stabilisce che «[a] state or local government agency must disclose their use of a facial recognition service on a criminal defendant to that defendant in a timely manner prior to trial».

²⁸ Si veda, ad esempio, il caso *Arteaga*, riformato da *State of New Jersey v. Arteaga*, Superior Court of New Jersey, Appellate Division, May 15, 2023, Docket no. A-3078-21, 476 N.J.Super. 36. Sul punto, K. JACKSON, *Challenging Facial Recognition Software in Criminal Court*, cit., p. 14 ss.; P. BARRANCO, *Match up: increasing disclosure of facial recognition technology with criminal discovery rules*, in *Duke Journ. of Constitutional Law & Public Policy*, 18(2023), p. 138; B.L. GARRETT, *Defending Due Process. Why Fairness Matters in a Polarized World*, Polity Press, Cambridge UK and Hoboken USA, 2025, p. 148-149. Per un caso in cui il *retrial* è stato negato, sull'assunto che non vi fossero i requisiti per un *Brady trial* (ovvero una ragionevole probabilità che il processo avrebbe avuto un diverso esito se la *disclosure* fosse stata garantita), *Willie Allen Lynch, Appellant, v. State of Florida, Appellee*. No. 1D16-3290 District Court of Appeal of Florida, First District. December 27, 2018.

²⁹ Un elenco dettagliato di tutto ciò che dovrebbe essere reso disponibile è contenuto nelle richieste della difesa *Arteaga*. Si veda poi il *Brief Of Amici Curiae Electronic Privacy Information Center, Electronic Frontier Foundation, And National Association Of Criminal Defense Lawyers*, leggibile al link [eff.org/it/deeplinks/2023/06/victory-new-jersey-court-rules-police-must-give-defendant-facial-recognition](https://www.eff.org/it/deeplinks/2023/06/victory-new-jersey-court-rules-police-must-give-defendant-facial-recognition).

³⁰ S.M. BOWEN, *Man vs. Machine*, cit., p. 46-47.

³¹ Icasticamente, C. GARVIE, *Garbage in, garbage out. Face recognition on flawed data*, in *fla-*

qui la maggiore precisione con cui, nel mondo occidentale³², vengono riconosciuti i maschi caucasici, a discapito delle diverse etnie e delle donne, in forza di un *bias* persistente riconosciuto persino dal NIST³³. Non sorprende quindi che l'intollerabile rischio di errore giudiziario e di ingiuste detenzioni³⁴, seppure comune ai più tradizionali sistemi di riconoscimento biometrici³⁵, per le tecnologie di riconoscimento facciale abbia riguardato principalmente la popolazione afro-americana³⁶. Il che dipende certo dalla minore accuratezza sopra descritta, cui si somma tuttavia la sovra-rappresentazione degli stranieri nelle banche dati di riferimento. Se in nordamerica il tema dei *bias* a danno delle comunità marginalizzate – soggette, più di altri, a perquisizioni, *stop and frisk* e arresti arbitrari, nonché all'uso di strumenti di sorveglianza³⁷ – è ampiamente discusso in dottri-

wedfacedata.com, 16 maggio 2019. Sul fatto che «[t]he quality of what the machines learn depends on the size and representativeness of the exemplars fed into the machines during the learning process through a training database» anche H.H. PERRITT JR., *Defending Face-Recognition Technology*, cit., p. 45.

³² P.J. PHILLIPS-F. JIANG-A. NARVEKAR-J. AYYAD-A.J. O'TOOLE, *An Other-Race Effect for Face Recognition Algorithms*, in *ACM Transactions on Applied Perception*, 8/2(2011), Article 14. Sul maggior tasso di falsi positivi (40% dei falsi positivi) per le persone di colore o asiatiche, ACLU Report, *Amazon's Face Recognition Technology Incorrectly Matched 28 Congress Members with Mugshots*, leggibile in innocenceproject.org/amazon-face-recognition-incorrect-match/; C. RABINOWICZ, *Approaches to Regulating Government Use of Facial Recognition Technology*, in jolt.law.harvard.edu/digest/approaches-to-regulating-government-use-of-facial-recognition-technology, 4 maggio 2023.

³³ I risultati delle analisi più recenti sono leggibili al link pages.nist.gov/frvt/html/frvt_demographics.html.

³⁴ G. GARVIE, *What Defense Counsel Should Know About Facial Recognition Technology*, cit., p. 18, nota come lo strumento in questione combini in sé le due maggiori fonti di errore giudiziario oggi conosciute: «two of the leading factors contributing to wrongful convictions are mistaken eyewitness identification and the use of false or misleading forensic evidence at some stage in the investigation or adjudication. Facial recognition searches reflect the most problematic elements of both of these techniques».

³⁵ Si pensi, in particolare, all'uso delle impronte digitali, che come noto risale agli inizi del secolo scorso. Ciò nondimeno, lo stesso non è ancora immune da rischi, come testimonia l'accusa rivolta nei confronti dell'americano Brandon Mayfield di essere coinvolto nell'attentato di Madrid del 2004, elevata a seguito del riconoscimento di una impronta ritrovata su una busta presente sulla scena da parte degli esperti del FBI. La stessa agenzia governativa fu poi costretta a riconoscere l'errore: si veda United States. Department of Justice. Office of the Inspector General, *A review of the FBI's handling of the Brandon Mayfield case*, 2006.

³⁶ È noto il caso di Robert Williams, arrestato ingiustamente dalla polizia di Detroit nel gennaio del 2020 per furto di orologi, in base al riconoscimento facciale: sul punto A. SANFORD, *Artificial Intelligence Is Putting Innocent People at Risk of Being Incarcerated*, leggibile in innocenceproject.org/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/, 14 febbraio 2024. La vicenda è trattata pure da K. HILL, *La tua faccia ci appartiene*, cit., p. 235 ss.

³⁷ R. LEVINSON-WALDMAN, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, in *Emory Law Journ.*, 66(2017), p. 553-554.

na, anche da noi inizia ad avvertirsi l'urgenza di contenere derive verso forme più o meno apparenti di "diritto processuale penale dello straniero"³⁸. Fenomeno in cui si iscrive anche la procedura di formazione degli archivi di raffronto dei dati biometrici³⁹, giacché – come si evince dal capitolato tecnico del Sistema Automatico Riconoscimento Immagini (SARI) – lo strumento di riconoscimento da remoto *a posteriori* attualmente in uso presso le nostre forze dell'ordine attinge alla banca dati dei soggetti fotosegnalati (SottoSistema Anagrafico AFIS)⁴⁰, popolato per di più da cittadini extra-UE⁴¹.

Ebbene, per anni gli strumenti in questione sono stati utilizzati dalle agenzie di *law enforcement* anche in paesi democratici, in presenza di un sostanziale vuoto normativo⁴². Detta mancanza di base giuridica è stata, come noto, riconosciuta a livello giurisprudenziale nell'ordinamento inglese, nel secondo grado del procedimento *Bridges*⁴³, relativo a *AFR Locate*, una forma di riconoscimento facciale in tempo reale usata dalla polizia inglese e gallese. Per quel che importa adesso, merita rimarcare come i poteri at-

³⁸ E. VALENTINI, *La procedura penale per lo straniero: tratti di specialità al ribasso*, in F. CURI-F. MARTELLONI-A. SBRACCIA-E. VALENTINI (a cura di), *I migranti sui sentieri del diritto. Profili socio-criminologici, giuslavoristici, penali e processualpenalistici*, Giappichelli, Torino, 2021, p. 297 ss.

³⁹ Il fatto che, pure fuori dai nostri confini, i database di riconoscimento facciale siano spesso sovrarappresentati dalle minoranze etniche viene sostenuto da H. RUHRMANN, *Facing the Future: Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement. Case Studies from the United Kingdom and the United States*, Citris Policy Lab, 2019, spec. p. 28 e p. 62-63, e da M. ZALNIERIUTE, *Burning Bridges: the Automated Facial Recognition Technology and Public Space Surveillance in the Modern State*, in *The Columbia Science & Technology Law Rev.*, 22/2(2021), p. 290.

⁴⁰ Ministero dell'interno, Dipartimento della pubblica sicurezza, *Capitolato tecnico. Procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini S.A.R.I. Lotto n° 1*, leggibile in poliziadistato.it/statics/06/20160627-ct-sari-4-.pdf, p. 14.

⁴¹ Volendo, E. DEI-CAS, *Le nuove norme in materia di identificazione degli apolidi e dei cittadini di Paesi terzi*, in P. FELICIONI (a cura di), *Dalle indagini all'udienza preliminare (d.lgs. 10 ottobre 2022, n. 150 – d.lgs. 19 marzo 2024, n. 31)*, Giappichelli, Torino, 2024, p. 140 ss.

⁴² Già *supra* si è detto del Bill del 2022, seguito da un tentativo di moratoria – anch'esso infruttuoso – nel 2023: S. 681, «To prohibit biometric surveillance by the Federal Government without explicit statutory authorization and to withhold certain Federal public safety grants from State and local governments that engage in biometric surveillance», c.d. «Facial Recognition and Biometric Technology Moratorium Act of 2023».

⁴³ R (on the application of Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058. A tale proposito, B. KEENAN, *Automatic Facial Recognition and the Intensification of Police Surveillance*, in *The Modern Law Rev.*, 84/4(2021), p. 886 ss.; N. NI LOIDEAIN, *Lawfulness and Police Use of Facial Recognition in the United Kingdom. Article 8 ECHR and Bridges v. South Wales Police*, in R. MATULIONYTE-N. ZALNIERIUTE (a cura di), *The Cambridge Handbook of Facial Recognition in the Modern State*, cit., p. 165 ss.; J. PURSHOUSE-L. CAMPBELL, *Automated facial recognition and policing: a Bridge too far?*, cit., p. 209 ss.; M. ZALNIERIUTE, *Burning Bridges*, cit., p. 284 ss.

tribuiti in via generica dal *common law* alla polizia sono stati reputati insufficienti – contrariamente a quanto ritenuto in precedenza dalla *High Court*⁴⁴ – a giustificare l'ingerenza nel rispetto della vita privata del ricorrente, sebbene lo stesso non fosse stato in alcun modo attinto dalle attenzioni della polizia a seguito di un *match* (che, nel caso di specie, non vi è stato⁴⁵), dolendosi invece del solo trattamento (di cui non vi era nemmeno traccia, visto i brevissimi periodi di conservazione⁴⁶) dei suoi dati sensibili, in qualità di attivista per le libertà civili. Il che fornisce il destro per sottolineare un ulteriore fattore che ci pare degno di nota, prima di volgere lo sguardo alla regolamentazione europea di recente introduzione, ovvero come la sollecitazione da parte di organizzazioni di attivisti, preoccupate dall'uso del riconoscimento biometrico remoto per interferire con proteste pacifiche poste in essere dalla popolazione civile⁴⁷, abbia portato le stesse *Big-Tech* ad «autonormarsi», ovvero a sfruttare una sorta di moratoria dichiarata sull'impiego e sulla vendita delle tecnologie di riconoscimento⁴⁸, animata da finalità promozionali⁴⁹: quali che siano le reali intenzioni, siamo quindi arrivati al paradosso per cui le aziende multinazionali della *Silicon Valley* si sono mosse prima in direzione della tutela delle salvaguardie, sostituendosi ai parlamenti nazionali, dando luogo al fenomeno da alcuni efficacemente definito «privatizzazione dei diritti fondamentali»⁵⁰.

⁴⁴ Bridges [2019] EWHC (Admin) 2341, sul quale si veda J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Dir. pen. cont.*, 2020, f. 1, p. 231 ss.

⁴⁵ Bridges [2019] EWHC (Admin) 2341, § 101.

⁴⁶ Bridges [2019] EWHC (Admin) 2341, § 37, ove si legge che, in assenza di *match*, i dati vengono cancellati subito in automatico. Del resto, non è nemmeno dimostrato che il volto di Bridges sia stato ripreso: § 51.

⁴⁷ M. CAGLE, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU Northern California (Oct. 11, 2016), leggibile in aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target/; si veda poi Amnesty International, *Ban dangerous facial recognition technology that amplifies racist policing*, 26 January 2021, [amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/](https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/). Per altri esempi, M. ZALNIERIUTE, *Burning Bridges*, cit., p. 298-299.

⁴⁸ IBM, ad esempio, ha rinunciato a fornire questa tecnologia alla polizia: A. HERN, *IBM quits facial-recognition market over police racial-profiling concerns*, leggibile sul sito [theguardian.com](https://www.theguardian.com), ove si nota tuttavia come la società versasse al momento della decisione in un ragguardevole ritardo competitivo rispetto alle concorrenti. Simili decisioni sono state assunte da Amazon e da Microsoft.

⁴⁹ G.A. FOWLER, *Black Lives Matter could change facial recognition forever – if Big Tech Doesn't stand in the way*, in *The Washington Post* (June 12, 2020), ne parla in termini di «corporate public relations stunt [...]».

⁵⁰ In questo senso, sebbene in relazione agli *Internet Service Providers*, M. BASSINI,

2. Il “divieto-non divieto” e “l’alto rischio insufficientemente governato” dell’AI Act a proposito di riconoscimento biometrico remoto

Come già si è accennato, lo strumento investigativo noto come Sistema Automatico di Riconoscimento Immagini (SARI) risulta in uso agli organi di polizia del nostro paese già da quasi due lustri pur in una situazione di anomia⁵¹; la recente introduzione del reg. 2024/1689/UE (d’ora in poi, *AI Act*)⁵² ha quindi avuto – perlomeno – il merito di portare alla ribalta le tecniche di riconoscimento biometrico remoto, seppure dettando norme minime che necessiteranno (per quanto qui importa) di attuazione da parte dei legislatori nazionali⁵³, i quali potranno introdurre discipline più stringenti e perfino vietarle *in toto*.

Fundamental rights and private enforcement in the digital age, in *Eur. Law Journ.*, 25/2(2019), p. 187.

La sempre crescente incidenza delle aziende private sul godimento dei diritti fondamentali viene sottolineata anche da A. LAVORGNA-G. SUFFIA, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell’ambito della giustizia penale*, in *Dir. pen. cont.*, 2021, f. 2, p. 91.

⁵¹ Sottolineano correttamente G. BORGIA, in ID.-M. ZONARO, *L’errore nel riconoscimento automatizzato*, cit., p. 186, nota 61, e E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell’impiego della biometria moderna*, Giappichelli, Torino, 2025, p. 16 e p. 158 ss., che il c.d. decreto “capienze” (d.l. 8 ottobre 2021, n. 139, conv. con modif. dalla legge 3 dicembre 2021, n. 205), nel porre una moratoria all’utilizzo dei sistemi in parola fino alla fine del 2023 (termine poi prorogato di due anni), ai nostri fini non rileva in quanto detto limite non trova applicazione in caso di impiego da parte delle «autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali».

⁵² L. AGOSTINO-G. BORGIA, *La disciplina dei sistemi di IA ad alto rischio: biometria, attività di contrasto e amministrazione della giustizia*, in *Proc. pen. giust.*, 2024, p. 1061 ss.; G. BARONE, *Artificial Intelligence Act: un primo sguardo al regolamento che verrà*, in *Cass. pen.*, 2024, p. 1047 ss.; M. TORRE, *Il Regolamento europeo sull’intelligenza artificiale: i profili processuali*, in *Proc. pen. giust.*, 2024, p. 1534 ss.

Un giudizio severo, ma condivisibile, sull’articolato proviene poi da S. QUATTROCOLO, *Intelligenza artificiale e processo penale: le novità dell’AI Act*, in *Dir. difesa (web)*, 16 gennaio 2025, p. 3, la quale nota come lo stesso «non si distingu[a] per chiarezza, né di linguaggio, né, purtroppo, di concetti, obbligando chi vi fa riferimento a funambolismi interpretativi, per dare senso ad alcune parti del testo».

⁵³ Non compaiono, tuttavia, indicazioni stringenti nella legge 23 settembre 2025, n. 132, Disposizioni e deleghe al governo in materia di intelligenza artificiale, che impegna l’esecutivo a adottare, entro dodici mesi dall’entrata in vigore della legge, uno o più decreti legislativi per l’adeguamento della normativa interna all’*AI Act*. Tra i principi e i criteri direttivi indicati, rilevano ai nostri fini la «previsione di un’apposita disciplina per l’utilizzo di sistemi di intelligenza artificiale per l’attività di polizia» (art. 24 comma 2 lett. b), la «regolazione dell’utilizzo dei sistemi di intelligenza artificiale nelle indagini preliminari, nel rispetto delle garanzie inerenti al diritto di difesa e ai dati personali dei terzi, nonché dei principi di proporzionalità, non discriminazione e trasparenza» (art. 24 comma 5 lett. e), nonché la «modifica, a fini di coordinamento e di razionalizzazione del sistema, della

Difatti, nonostante l'uso oramai consolidato, lo studioso – ma anche il cittadino – che volesse a oggi indagarne modalità di funzionamento e limiti, non potrebbe che rivolgersi, in prima battuta, al capitolato tecnico del software⁵⁴, per poi considerare alcuni noti pronunciamenti dell'autorità garante per la *privacy*⁵⁵. In questo contesto, dunque, ad onta dei diritti di libertà dell'individuo potenzialmente comprimibili, la norma processuale penale – baluardo e scudo a tutela dei galantuomini e degli onesti incappati nella maglie dell'accertamento⁵⁶, che la Carta fondamentale vuole presunti innocenti –, sfuma, riapparendo al più (ammesso che l'operazione sia ortodossa, richiedendo, come noto, la disciplina della prova innominata garanzie per l'accertamento, nonché una specie di contraddittorio⁵⁷) sotto forma di *passepartout* della prova atipica⁵⁸.

Eppure quanto le attività in questione siano foriere di *vulnera*, se non adeguatamente governate, appare in tutta la sua evidenza già da come vengono “etichettate” dal legislatore eurounitario. Le une (riconoscimenti a posteriori, ritenuti, a torto o a ragione, meno invasivi⁵⁹) tra le attività “ad alto rischio”, le altre (quelli in tempo reale) addirittura nelle vietate,

normativa sostanziale e processuale vigente, in conformità ai principi e ai criteri enunciati nelle lettere a), b), c), d) ed e)» (art. 24 comma 5 lett. ff).

⁵⁴ *Capitolato tecnico. Procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini S.A.R.I. Lotto n° 1*, cit.

⁵⁵ Parere sul sistema Sari Real Time, 25 marzo 2021 [9575877], leggibile in garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575877; garante per la protezione dei dati personali, Provvedimento n. 440 del 26 luglio 2018, relativo a Sari Enterprise.

⁵⁶ Pensiero comunemente riferito a Carrara (F. CARRARA, *Il diritto e la procedura penale*, in *Opuscoli di diritto criminale*, 2a ed., Tipografia Giachetti, figlio e c., Prato, 1881, vol. V, p. 19), anche se ascrivibile già a Romagnosi («[l]a procedura è fatta primieramente per la sicurezza della gente onesta [...]»: G.D. ROMAGNOSI, *Se la pubblicità dei giudizi criminali convenga alla monarchia*, in *Opere di G. D. Romagnosi riordinate ed illustrate da A. De Giorgi*, vol. IV, pt. I, *Scritti sul diritto penale*, Perelli e Mariani Editori, Milano, 1841, p. 443). Vedi, sul punto, R. ORLANDI, *Rito penale e salvaguardia dei galantuomini*, in *Criminalia*, 2006, p. 297) e a Ferri (in tal senso, G.D. PISAPIA, *Introduzione*, in *Il codice di procedura penale. Esperienze, valutazioni, prospettive*, Giuffrè, Milano, 1994, p. 26).

⁵⁷ Il punto verrà ripreso *infra*, § 3.

⁵⁸ Espressione utilizzata da R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv. it. dir. proc. pen.*, 2018, p. 553.

⁵⁹ Secondo alcuni invece, queste sarebbero maggiormente invasive, proprio in quanto si attinge a una piattaforma materiale più vasta: EDPB-EDPS, *Joint Opinion 5/2021 on the proposal of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 June 2021, p. 11. Della stessa opinione pure gli autori del Report for the Greens/EFA in the European Parliament, *Behavioural Mass Surveillance in EU member States*, October 2021, p. 11.

Al riguardo anche A. GIANNINI-S. TAS, *AI Act and the Prohibition of Real-Time Biometric Identification: Much ado about nothing?*, VerfBlog, 10 dicembre 2024, in verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification/, DOI: 10.59704/a15aa6e58151c853, sebbene in termini possibilistici.

salvo eccezioni, tra cui rientrano neanche a dirlo le finalità investigative e accertative; eccezione che comporta un *down-grading* da attività vietata ad attività ad alto rischio. Ciò, nonostante autorevoli organismi europei (l'*European Data Protection Board* e l'*European Data Protection Supervisor*) avessero invocato una moratoria generale che vietasse ogni forma di riconoscimento biometrico remoto in spazi accessibili al pubblico⁶⁰.

Prendendo le mosse dalla seconda tra le categorie richiamate, la preoccupazione crescente nei confronti di scenari distopici di sorveglianza di massa negli spazi pubblici, con tutto ciò che ne deriva in termini di *chilling effects*⁶¹ sull'esercizio di diritti di rilievo costituzionale (libertà di movimento, di manifestazione del pensiero, di associazione e riunione, di culto, per dirne alcuni), ha sortito un divieto di massima. Senonché, le eccezioni introdotte sono tali e tante da potersi ragionevolmente dubitare che di esso si tratti⁶², giacché le autorità nazionali potranno ricorrere allo strumento *live* se ritenuto «*strettamente necessario*» in vista della ricerca mirata di vittime specifiche di taluni reati o di persone scomparse; per prevenire minacce – *specifiche, sostanziali e imminenti* – alla vita o all'incolumità fisica di persone oppure di attacchi terroristici (*reali e attuali o reali e prevedibili*: con la prima situazione che pare attagliarsi al c.d. *ticking bomb scenario*); oppure per localizzare o identificare un sospettato di aver commesso un reato contemplato dall'elenco annesso, purché punibile nello Stato membro con una pena di reclusione massima pari ad almeno quattro anni, ai fini dello svolgimento dell'indagine, dell'esercizio dell'azione o dell'esecuzione penale.

A tale ultimo riguardo, non è sfuggito ai primi interpreti⁶³ che, in un contesto di insufficiente armonizzazione dello *ius terribile*, ove le discipline nazionali delle fattispecie incriminatrici e del *quantum* edittale di pena sono oltremodo variegate, il riferimento qualitativo e quantitativo appaia fuorviante di disparità e frammentazioni all'interno dell'Unione⁶⁴.

Invece, volendo mantenersi su un piano generale di analisi, la lettura

⁶⁰ Si veda EDPB-EDPS, *Joint Opinion 5/2021 on the proposal of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, cit., p. 2 e p. 11.

⁶¹ Effetti indagati già da tempo nella monografia di G. DI PAOLO, "Tecnologie del controllo" e *prova penale*. L'esperienza statunitense e spunti per la comparazione, Cedam, Padova, 2008, p. 147.

⁶² Sottolinea la vaghezza di detto divieto pure S. QUATTROCOLO, *Intelligenza artificiale e processo penale: le novità dell'AI Act*, cit., p. 9, richiamando, in seguito (p. 10), gli interpreti al rigore, onde evitare un sostanziale rovesciamento dello stesso.

⁶³ A. LAVORGNA-G. SUFFIA, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale*, cit., p. 95, in relazione al testo della proposta.

⁶⁴ In tal senso anche A. GIANNINI-S. TAS, *AI Act and the Prohibition of Real-Time Biometric Identification*, cit.

complessiva della disposizione produce nello studioso italiano impressioni simili a quelle che si provano in relazione alla disciplina dei *pericula libertatis*, ovvero che il legislatore – eurounitario, in un caso; nazionale, nell’altro – tenti di imprimere certezza a una regolamentazione che sfugge (o che quantomeno non imbriglia l’autorità statuale a sufficienza) mediante la moltiplicazione degli aggettivi e degli avverbi, senza che ne corrisponda un aumento concreto delle garanzie del singolo. Sempre rimanendo sul medesimo piano, appare pure come, affianco a usi prettamente investigativi, figurino forme preventive, andando quindi ad accrescere quell’agglutinamento tra ciò che è procedimentale e ciò che invece vi si antepone – tra repressione e prevenzione – connotante oramai da tempo la nostra procedura, e che va sotto la denominazione di indagini proattive⁶⁵.

Nonostante questa commistione nell’utilizzo consentito, i profili dinamici vengono trattati unitariamente; l’impiego del predetto sistema in tempo reale, per attività di contrasto e in spazi accessibili al pubblico, è subordinato alla riserva di giurisdizione, essendo imposta l’autorizzazione preventiva di una autorità giudiziaria (o di un’autorità amministrativa indipendente), rilasciata a seguito di istanza motivata, a meno che non si versi in una situazione d’urgenza, tale – *more solito* – da consentire un avvio d’uso, prima di richiedere l’autorizzazione entro le ventiquattro ore.

Ricorrono, a proposito della prevista autorizzazione, i richiami ai principi di necessità e di proporzionalità⁶⁶, da valutarsi alla stregua di elementi indicati espressamente che dovrebbero vincolare il sindacato del giudice, chiamato a decidere se utilizzare la tecnologia *real time* per la conferma dell’identità di un determinato soggetto⁶⁷ e non, quindi, per le-

⁶⁵ D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Arch. pen.*, 2016, f. 1, p. 44 ss.; R. ORLANDI, *Il sistema di prevenzione tra esigenze di politica criminale e principi fondamentali*, in *La giustizia penale preventiva. Ricordando Giovanni Conso*, Giuffrè, Milano, 2016, p. 5 ss., spec. p. 15; S. SIGNORATO, *Le indagini digitali*, cit., p. 183, nota 141.

⁶⁶ L. BELVINI, *Principio di proporzionalità e attività investigativa*, Edizioni scientifiche italiane, Napoli, 2022; F. NICOLICCHIA, *Il principio di proporzionalità nell’era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Dir. pen. cont.*, 2018, f. 2, p. 176 ss.; G. UBERTIS, *Prova penale e proporzionalità*, in *Sist. pen. (web)*, 23 gennaio 2025, p. 1 ss.

Sul tema specifico qui d’interesse, G. BORGIA, *Biometría, evolución, tecnológica y proceso penal: urge un cambio de ritmo en nombre de la proporcionalidad*, in S. PEREIRA PUIGVERT-G. BORGIA, *Retos de la prueba en el proceso actual*, Editorial Aranzadi, Madrid, 2024, p. 425 ss.

⁶⁷ Il che sembrerebbe alludere a una forma di verifica, dal rapporto 1:1, piuttosto che a una autentica identificazione (1:n), secondo una distinzione ricorrente nella letteratura in tema di biometria. Si vedano per tutti G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 34-35; J.D. WOODWARD, *Biometric scanning, law & policy: identifying the concerns drafting the biometric blueprint*, in *University of Pittsburgh Law Review*, 59/1(1997), p. 100.

Sulle differenze tecniche tra impiego 1:1 e 1:molti, si veda altresì GIOV. TESSITORE,

gittimare operazioni esplorative⁶⁸. In primo luogo, «a) la natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno che sarebbe causato in caso di mancato uso del sistema; b) 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», nonché il rispetto delle «tutele e le condizioni necessarie e proporzionate in relazione all'uso, conformemente al diritto nazionale che autorizza tale uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali»⁶⁹.

Al di là del richiamo, persino ridondante⁷⁰, ai canoni di proporzione e stretta necessità, sorgono dubbi sulla reale attitudine delle previsioni a garantirne il rispetto, in ragione, da una parte, della loro eccessiva genericità (non si comprende, ad esempio, il vacuo riferimento alle «limitazioni temporali, geografiche e personali»), dall'altra, poiché tendono a dare la stura a un modo di ragionare rischioso e che anzi contraddice l'essenza stessa del principio di proporzione, secondo cui lo stesso possa esser letto non come garanzia ma a scapito dell'indagato/imputato⁷¹: la gravità del reato da accertare o del pericolo (che si ritiene) incombente che giustifica *ex se* la necessità dell'impiego della tecnologia per confermare l'identità del sospettato.

Inoltre la considerazione pare incentrata sul bilanciamento – che a

Riconoscimento automatico del volto e confronto in ambito forense, in P. DI SIMONE-A. MANGIARACINA-L. PARLATO (a cura di), *120 anni di polizia scientifica: l'identificazione personale tra scienza e diritto. Atti del convegno (Palermo, 18-19 aprile 2023)*, Palermo University press, Palermo, 2023, p. 61 ss.

⁶⁸ Di tale avviso anche M. TORRE, *Il Regolamento europeo sull'intelligenza artificiale: i profili processuali*, cit., p. 1543.

⁶⁹ Art. 5 § 2 del Regolamento.

⁷⁰ Richiamo che non caratterizza solamente la fonte in parola, ma pure il Regolamento (UE) 2016/679 (c.d. GDPR) e la Direttiva (UE) 2016/680 (*Law Enforcement Directive*), fatti salvi dall'*AI Act*. Si veda, al riguardo, l'art. 2 § 7, a norma del quale «[il] diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni si applica ai dati personali trattati in relazione ai diritti e agli obblighi stabiliti dal presente regolamento. Il presente regolamento lascia impregiudicati il regolamento (UE) 2016/679 o (UE) 2018/1725 o la direttiva 2002/58/CE o (UE) 2016/680, fatti salvi l'articolo 10, paragrafo 5, e l'articolo 59 del presente regolamento». Merita evidenziare, come nota G. BORGIA, *Biometria, evolución, tecnológica y proceso penal*, cit., p. 429, che la Direttiva (UE) 2016/680, a differenza del Regolamento IA, non prevede alcuna riserva di giurisdizione e che quest'ultimo già comporta un incremento di garanzie, almeno sotto tale profilo.

⁷¹ Mette in guardia da consimile ragionamento D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 2020, p. 4, il quale ricorda come il principio in parola debba rimanere genuina garanzia liberale. Per un esempio di pronunciamento in cui la Corte costituzionale ha consentito alla limitazione di un diritto fondamentale mediante il ricorso al principio di proporzione, F. NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico*, cit., p. 181.

rigore dovrebbe invece rappresentare soltanto il terzo gradino del *test* di proporzionalità⁷² – da condursi alla stregua di una valutazione dei *pro* e dei *contra* dell'utilizzo del mezzo nella situazione data. Al posto della verbosità mostrata, non avrebbe stonato qui l'affermazione netta per cui, a parità di risultato, occorre che sia privilegiato dall'autorità il mezzo meno invasivo⁷³ al fine del raggiungimento dello scopo prestabilito: previsione, quest'ultima, atta, ben più dei proclami a dare corpo al principio di stretta necessità, di cui altrove il legislatore europeo ha dimostrato di sapere fare buon uso⁷⁴.

Notevolmente più sguarnita si mostra invece la disciplina del riconoscimento a posteriori, peraltro sepolta all'interno di una disposizione dalla rubrica che pare eccentrica rispetto al tema di interesse (art. 26 «Obblighi dei deployer dei sistemi di IA ad alto rischio»). In essa si stabilisce una riserva di giurisdizione (autorizzazione *ex ante* o entro 48 ore), tranne quando il riconoscimento statico è utilizzato a fini di identificare alle primissime battute delle investigazioni un potenziale sospettato «sulla base di fatti oggettivi e verificabili direttamente connessi al reato». L'eccezione è relevantissima; eppure l'ultima dizione appare quasi un «superfluo avvertimento didattico»⁷⁵, giacché non si comprende cos'altro possa scomodarsi in quelle prime fasi a giustificare un sospetto, senza un qualche ancoraggio fattuale (es. un fotogramma estrapolato dalle registrazioni effettuate dalle telecamere a circuito chiuso, che mostra un soggetto allontanarsi dal luogo del reato di gran carriera), salvo avvalersi di veggenti e sfere di cristallo.

Pertanto, la garanzia primaria del controllo dell'organo giurisdizionale viene negata in uno scenario che si immagina divenga di frequente utilizzo – specie se pensiamo a quanto detto sopra a proposito dell'esperien-

⁷² Per tutti, F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione della prova tra fonti europee e ordinamenti nazionali*, Cedam, Milano, 2020, p. 122 ss.

⁷³ Similmente a quanto previsto al quinto comma dell'art. 224-bis c.p.p., considerata «una bandiera superba, che non sfignerebbe affatto in apertura del codice» da A. CAMON, *La prova genetica tra prassi investigativa e regole processuali*, in *Proc. pen. giust.*, 2015, p. 169.

⁷⁴ Cfr. l'art. 10 § 3 della direttiva 2014/41/UE relativa all'ordine europeo di indagine penale, a norma del quale «[l']autorità di esecuzione può anche ricorrere ad un atto d'indagine diverso da quello richiesto nell'OEI quando l'atto scelto dall'autorità di esecuzione assicuri lo stesso risultato dell'atto richiesto nell'OEI con mezzi meno intrusivi». A riguardo, in termini critici, L. SCOMPARIN-A. CABIALE, *The Proportionality Test in Directive 2014/41/EU: Present and Future of a Fundamental Principle*, in *Eurojus*, 2022, 2, p. 81-82.

⁷⁵ F. CORDERO, *Procedura penale*, 8^a ed., Giuffrè, Milano, 2006, p. 484, in relazione alla «“personalità (...) desunta da comportamenti o atti concreti o (...) precedenti penali”» all'interno del disposto dell'art. 274 comma 1 lett. c, c.p.p., il quale proseguiva «qualcuno adopera oroscopi, grafologumeni, cabale chiromantiche o fisiognomiche?».

za statunitense e del configurarsi quale *investigative lead* –, ovvero là dove il ricorso allo strumento biometrico serva per l'immediata prosecuzione delle indagini, relegato all'esclusivo appannaggio degli organi inquirenti.

Il richiamo reiterato alla stretta necessità⁷⁶ («Ogni uso è limitato a quanto strettamente necessario per le indagini su uno specifico reato»⁷⁷) permane, insieme alla specificazione per cui non sono ammesse forme di *inquisitio generalis* tecnologica, in quanto l'impiego *ex post* necessita di «collegamento con un reato, un procedimento penale, una minaccia reale e attuale o reale e prevedibile di un reato o la ricerca di una determinata persona scomparsa»⁷⁸. Ebbene, a fronte dell'urgenza che traspare, le tutele apparenziate dal legislatore europeo sono blande⁷⁹, riconducibili in buona sostanza a una insistenza sulla necessità e proporzionalità più apparente che reale.

Pure il richiesto controllo umano significativo⁸⁰ non pare risolvere le perplessità: non impedisce, per un verso, che l'operatore umano si appiattisca sul risultato della macchina in forza del già menzionato *automation bias*; per l'altro, si rischia di aggiungere al *bias* algoritmico quello umano.

Prima di rivolgere lo sguardo alle prospettive future, merita precisare che il regolamento sull'IA prescrive anche obblighi di documentazione delle attività compiute con riguardo alle tecnologie di riconoscimento biometrico remoto con finalità di controllo, da inserire nel fascicolo proce-

⁷⁶ Una precisazione sul canone in parola deriva dalla Corte di Lussemburgo, chiara nel dire che «le finalità del trattamento di dati biometrici e genetici non possono essere designate in termini troppo generici, ma richiedono di essere definite in modo sufficientemente preciso e concreto da consentire di valutare il carattere “strettamente necessario” di detto trattamento» e che «il requisito della necessità è soddisfatto qualora l'obiettivo perseguito dal trattamento di dati di cui trattasi non possa ragionevolmente essere conseguito in modo altrettanto efficace con altri mezzi meno lesivi dei diritti fondamentali delle persone interessate, in particolare dei diritti al rispetto della vita privata e alla protezione dei dati personali garantiti dagli articoli 7 e 8 della Carta»: così Corte giust., sent. 26 gennaio 2023, C-205/21, V.S., rispettivamente § 124 e 126.

⁷⁷ Art. 26 § 10.

⁷⁸ Ancora art. 26 § 10.

⁷⁹ Condivide il giudizio severo sulla formulazione, troppo lasca, adottata J. GARCÍA LUENGO, *Obligations of providers and deployers of high-risk AI systems and other parties* (Chapter III, section 3), in A. HUERGO LORA (a cura di), *The EU Regulation on Artificial Intelligence: a Commentary*, Cedam, Milano, 2025, p. 317.

⁸⁰ In letteratura, il nesso tra dignità umana e decisione robotica viene sondato da S. SIGNORATO, *Il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati: un nuovo diritto derivante dal rispetto della dignità umana*, in *Riv. dir. proc.*, 2021, p. 101 ss. Sul “*human in the loop*” pure G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. pen. cont.*, 2020, f. 4, p. 83 ss.

dimentale o «di polizia»⁸¹. Il che ci pare meritevole di attenzione, se solo si pensa a quanto lamentato dai pratici nord-americani circa la mancanza di trasparenza in ordine all'avvenuto ricorso allo strumento, fronteggiato talvolta là a livello di legislazione statale⁸²: il punto diviene allora l'effettiva possibilità di contraddire sulla bontà dei risultati ottenuti, il che risente dell'opacità algoritmica e dei confini non chiari su quanto debba divenire ostensibile alla difesa.

3. *Futuribili per una normativa interna improntata alle garanzie individuali*

Tratteggiato il telaio minimo di garanzie previste di recente dal legislatore unionale, l'indagine può ora intradarsi sulle vie percorribili dal legislatore domestico, giovandosi dell'opera già compiuta dagli autori occupatisi in Italia, in special modo, di riconoscimento facciale⁸³, che qui fi-

⁸¹ Art. 26 § 10.

⁸² Diversi obblighi di documentazioni sono sanciti, ad esempio, dalle leggi statali di Washington: la già citata RCW 43.386.070 prescrive la tenuta di registri documentanti l'utilizzo dei sistemi di riconoscimento facciale da parte delle autorità statali o locali, mentre RCW 43.386.020 norma l'*accountability report*, che ogni autorità deve stilare prima di sviluppare, procurarsi o utilizzare sistemi di quel tipo, contenente informazioni sul servizio acquisito (ad esempio «name of the facial recognition service, vendor and version; description of its general capabilities and limitations, including reasonably foreseeable capabilities outside the scope of the proposed use of the agency») e sul suo funzionamento (es: «type or types of data inputs that the technology uses; (ii) how that data is generated, collected, and processed; and (iii) the type or types of data the system is likely to generate»).

⁸³ L. BELVINI, *Intelligenza artificiale e circuito investigativo*, Cacucci editore, Napoli, 2025, p. 160 ss.; G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *Leg. pen. (web)*, 11 dicembre 2021; L. CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, in F. BASILE-M. BIASI-L. CAMALDO-G. CANESCHI-B. FRAGASSO-D. MILANI (a cura di), *Intelligenza artificiale. Diritto, giustizia, economia ed etica*, Giappichelli, Torino, 2025, p. 79 ss.; F. DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale*. Tra possibilità di impiego e limiti ordinamentali, Cedam, Milano, 2025; J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.*, 2022, 3, p. 1057 ss.; ID., *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, in G. DI PAOLO-L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Editoriale scientifica, Napoli, 2022, p. 7 ss.; G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 638 ss.; R. LOPEZ, *Riconoscimento facciale tramite software e individuazione del sospettato*, in A. SCALEATI (a cura di), *Pre-investigazioni (Espedienti e mezzi)*, Giappichelli, Torino, 2020, p. 295 ss.; A. MARANDOLA, *Il riconoscimento facciale*, in C. CONTI-A. MARANDOLA (a cura di), *La prova scientifica*, Giuffrè, Milano, 2023, p. 495 ss.; E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit.; EAD., *La prova biometrica*, in C. CONTI-A. MARANDOLA (a cura di), *La prova scientifica*, cit., p. 243 ss.; EAD., *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *Leg. pen. (web)*, 16 ottobre 2020; EAD., *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Dir. pen. cont.*, 2019, f. 2, p. 465 ss.; L. SAPONARO, *Le nuove frontiere*

gura quale archetipo del riconoscimento biometrico remoto, anche in virtù del più avanzato stato di elaborazione che la riflessione ha oramai raggiunto sul punto. Nei contributi editi appare infatti l'urgenza di normare la materia, giacché gli addentellati individuati in più sedi (si pensi a quelli indicati nei già citati pareri dell'autorità garante per la *privacy*), si mostrano insufficienti a disciplinare l'impiego delle tecnologie di riconoscimento remoto, sia nella fase delle indagini, sia durante l'istruzione probatoria.

Senza ripercorrere qui compiutamente i termini del dibattito, basti ricordare come, da un lato, l'art. 349 c.p.p., in tema di identificazione personale, a ben vedere avrebbe poco a che spartire con l'operazione compiuta dall'algoritmo (con buona pace del suddetto garante), se solo si rammenta il significato autentico di *identificazione*, quale ascrizione delle corrette generalità a una persona; operazione diversa dall'*individuazione*, che più si confà allo scenario in discorso in cui occorre designare un soggetto fisico a cui ascrivere in ipotesi il fatto⁸⁴.

Ragioni ancora più pregnanti portano a escludere l'utile richiamo alla categoria della prova innominata, introdotta – come noto – dal legislatore del 1988-1989 con l'intento di coniugare garanzie difensive e necessità di tenere in debito conto il progresso inarrestabile della tecnologia «che estende le frontiere dell'investigazione»⁸⁵. Se l'intento di allora può ritenersi comprensibile e ragionevole, si avverte un disagio – se non un vero assurdo – reputando che un atto atipico, proprio in quanto non previsto né prevedibile nel momento della codificazione, possa soddisfare la garanzia della riserva di legge posta dalle fonti sovranazionali per invadere la sfera intima dell'individuo⁸⁶. Pertanto, quand'anche l'operazione di sus-

tecnologiche dell'individuazione personale, in *Arch. pen. (web)*, 2022, f. 1, p. 1 ss.; M. TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. proc.*, 2021, p. 1042; V. VASTA, *Diritto dell'Unione europea e intelligenza artificiale. Riflessi sul procedimento penale*, in F. BASILE-M. BIASI-L. CAMALDO-G. CANESCHI- B. FRAGASSO-D. MILANI (a cura di), *Intelligenza artificiale. Diritto, giustizia, economia ed etica*, cit., p. 140 ss.

⁸⁴ O. DOMINIONI, *Commento agli artt. 66-68 c.p.p.*, in E. AMODIO-O. DOMINIONI (diretto da), *Commentario del nuovo codice di procedura penale*, vol. I, Giuffrè, Milano, 1989, p. 409-410, il quale precisa come l'*individuazione* dell'imputato sia «una delle componenti dell'imputazione e consiste nel determinare, fra una più o meno definita cerchia di individui, la persona a cui è ascritto il fatto di reato e nei confronti della quale, pertanto, è iniziata l'azione penale»; mentre l'*identificazione* è «l'attribuzione all'imputato dei contrassegni che lo accompagnano nell'ordinaria vita di relazione: cognome, nome e le altre generalità necessarie a rendere univoca la sua designazione, quali la paternità, la maternità, il luogo e la data di nascita [...]».

⁸⁵ Si veda, al riguardo, la *Relazione al progetto preliminare del 1988*, in G. CONSO-V. GREVI-G. NEPPI MODONA (a cura di), *Il nuovo codice di procedura penale. Dalle leggi delega ai decreti delegati*, vol. IV, *Il progetto preliminare del 1988*, Cedam, Padova, 1990, p. 553.

⁸⁶ Di questa opinione, M. DANIELE, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen.*, 2013, p. 370, cui aderisce S. SIGNORATO, *Le indagini digitali*, cit., p. 260.

sunzione dei congegni di riconoscimento biometrico fra le prove atipiche fosse ammessa⁸⁷, difficilmente si porrebbe in linea coi canoni richiesti dall'art. 8 Conv. e.d.u. e, segnatamente, con la necessaria base legale a giustificazione della ingerenza nella riservatezza della persona. E questo nonostante l'esigenza di contemplare pure ordinamenti di *common law* all'interno della famiglia del Consiglio d'Europa faccia sì che detta base non debba essere necessariamente racchiusa in una legge⁸⁸ *scripta et stricta*, ma pure nel diritto giurisprudenziale⁸⁹, purché accessibile e prevedibile agli occhi dei destinatari⁹⁰.

Peraltro, anche la più lassista delle interpretazioni che volesse considerare base legale sufficiente a legittimare lesioni dei diritti fondamentali dell'individuo il richiamo a generici poteri di polizia giudiziaria (artt. 55, 348 e 354 c.p.p.) – in patente spregio del principio di legalità processuale – non potrebbe che scontrarsi con l'inconciliabilità tra *FRTs* e il rispetto dei limiti che il legislatore ha impresso alla prova innominata⁹¹, che viene immancabilmente a tema in virtù della natura di *novel science*⁹².

Senza scomodare acquisizioni ricorrenti⁹³, che muovono dalle risalentissime pronunce Frye e Daubert⁹⁴, e che dovrebbero fungere da ar-

⁸⁷ La gran parte degli interpreti concorda sulla mancata soddisfazione dei criteri richiesti a giustificare invasioni nel diritto alla vita privata e personale qualora ci si trovi dinanzi a una prova innominata: in tal senso, ad esempio, G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato*, cit., p. 19.

⁸⁸ Sul termine "legge" ai sensi dell'art. 8 § 2 Conv. e.d.u., G. UBERTIS, *L'autonomia linguistica della Corte di Strasburgo*, in F. RUGGIERI-T. RAFARACI-G. DI PAOLO-S. MARCOLINI-R. BELFIORE (a cura di), *Processo penale, lingua e unione europea*, Cedam, Padova, 2013, p. 224 ss.

⁸⁹ S. SIGNORATO, *Le indagini digitali*, cit., p. 259 ss.

⁹⁰ Corte e.d.u., 2 settembre 2010, Uzun c. Germania, § 57; Corte e.d.u., 24 aprile 1990, Kruslin c. Francia, § 27 ss.

⁹¹ Nel senso che SARI non è in grado di rispettare i presupposti dell'art. 189 c.p.p., L. BELVINI, *Intelligenza artificiale e circuito investigativo*, cit., p. 175; J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, cit., p. 38 ss.; E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 233.

⁹² M. TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, cit., p. 1052. La tesi per cui il *match* fra due dati biometrici digitalizzati sarebbe sussumibile nella categoria della *digital evidence* è sostenuta da E. SACCHETTO, *La prova biometrica*, cit., p. 257, la quale, in altra sede (EAD, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, cit., p. 475, nota 56), specifica che il *template* è *prova digitale*. Per la riconduzione della *digital evidence* all'interno della nuova prova scientifica, L. MARAFIOTI, *Digital evidence e processo penale*, in *Cass. pen.*, 2011, p. 4510.

⁹³ F. CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2005, p. 3520 ss.; O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005.

⁹⁴ Frye v. United States 293 F. 1013 (D.C. Cir. 1923); Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 113 S. Ct. 2786 (1993). Sul punto, per tutti, M. TARUFFO, *Le*

gine all'ingresso della cattiva scienza nel processo penale, trattandosi di materia già da tempo arata nella letteratura scientifica – al pari (anche se di ben più recente emersione) del tema dell'opacità algoritmica –, basti qui rimarcare come quello dell'affidabilità sia il vero buco nero del congegno in parola. Se già in dottrina è discussa l'attitudine dei riconoscimenti in udienza a garantire l'accertamento dei fatti⁹⁵, l'uso probatorio di algoritmi sui quali la difesa non può efficacemente contraddire, là dove ci si trovi dinanzi a una *black box*⁹⁶, dovrebbe essere radicalmente vietato⁹⁷. Altrimenti opinando, quel controllo umano significativo di cui discorrono le fonti sia di *soft* sia di *hard law* esprimerebbe, in definitiva, null'altro che una regola di facciata⁹⁸, come per altro pare suggerire perfino la Corte di Lussemburgo con qualche timida affermazione espressa in ambito assai diverso da quello in discorso⁹⁹.

prove scientifiche nella recente esperienza statunitense, in *Riv. trim. dir. proc. civ.*, 1996, p. 233 ss. Tornando al nostro tema, nella dottrina americana sottolineano che l'uso delle FRT non è ancora stato sottoposto ai test Frye e Daubert. C. GARVIE, *A Forensic Without the Science*, cit., p. 3 e p. 45-46, e A. FRAERMAN, *Relying on Unreliable Tech*, cit., p. 171, valutazione che, secondo gli autori citati, questi *tools* non passerebbero.

⁹⁵ A.M. CAPITTA, *Ricognizioni e individuazioni di persone nel diritto delle prove penali*, Giuffrè, Milano, 2001, p. 298; N. TRIGGIANI, *Ricognizioni mezzo di prova nel nuovo processo penale*, Giuffrè, Milano, 1998, p. 183 s.; A. TRINCI, *L'attuazione del contraddittorio tra storture della prassi e insostenibilità del sistema*, in D. NEGRI-R. ORLANDI (a cura di), *Le erosioni silenziose del contraddittorio*, Giappichelli, Torino, 2017, p. 221.

⁹⁶ Concordi su tale natura da attribuire ai sistemi di riconoscimento facciale, D. CURTOTTI-A. PROCACCINO, *Perizia e consulenza tecnica: alcune criticità e qualche prospettiva*, in C. CONTI-A. MARANDOLA (a cura di), *La prova scientifica*, cit., p. 922.

Intorno al concetto di *black box*, si veda G. FIORELLI, *Calcolabilità del giudizio giuridico e processo penale*, Giappichelli, Torino, 2025, p. 226 ss., anche per l'ampia bibliografia citata (spec. p. 227, nota 202).

⁹⁷ A questa conclusione, estesa oltre il solo uso probatorio in senso stretto, giunge B.L. GARRETT, *Defending Due Process*, cit., p. 140 ss.

Come si ricorderà, nella vicenda EncroChat, i giudici del Kirchberg hanno già stabilito che «un elemento di prova sul quale una parte non sia in grado di svolgere efficacemente le proprie osservazioni debba essere escluso dal procedimento penale» qualora lo stesso sia atto a «influire in modo preponderante sulla valutazione dei fatti»: Corte giust., sent. 30 aprile 2024, C-670/22, M.N., § 130-131.

⁹⁸ In un quadro più ampio, scettica nei confronti dell'invocato controllo si mostra l'allarmata analisi di O. MAZZA, *Distopia del processo artificiale*, in *Arch. pen. (web)*, 2025, f. 1, p. 17.

⁹⁹ Quando, ad esempio, riconosce che, in modo da soddisfare il diritto a contestare la decisione automatizzata riconosciuto dall'art. 22 GDPR, devono essere fornite all'individuo informazioni trasparenti e facilmente accessibili, specificando che «[n]on può soddisfare tali requisiti né la semplice comunicazione di una formula matematica complessa, come un algoritmo, né la descrizione dettagliata di tutte le fasi di un processo decisionale automatizzato, in quanto nessuno di questi metodi costituirebbe una spiegazione sufficientemente concisa e comprensibile»: così Corte giust., sent. 27 febbraio 2025, C-203/22, CK, § 59.

Continuando a concentrarci sulla dicotomia vietare-non vietare, primo passo che il legislatore domestico dovrà compiere, pare francamente improbabile che questi (specie nella presente temperie culturale) sarà disposto a rinunciare del tutto al contributo delle tecnologie in discorso ai fini di indagine e di accertamento. Consapevoli di ciò, si tratta come sempre di individuare un equilibrio tra diritti individuali ed esigenze repressive e investigative. Operazione da farsi in questo caso scindendo, da una parte, tra riconoscimento a posteriori e in tempo reale, e dall'altra parte, in considerazione del diverso momento procedimentale (o persino pre-procedimentale).

Iniziando dalla tecnologia a posteriori, già in uso nel nostro paese, una prima soluzione apparentemente di buon senso consiste nel relegarne l'utilizzo ai soli fini investigativi¹⁰⁰ (meglio: soltanto per l'immediata prosecuzione delle indagini), senza neppure che il riconoscimento così effettuato possa contribuire a ravvisare il *fumus commissi delicti* richiesto per l'applicazione di una misura cautelare¹⁰¹.

Ciò a patto di non abbassare la guardia, accontentandosi di garanzie minimali e di approcci aformalistici, che tanto altrove hanno caratterizzato gli atti a valenza endoprocedimentale¹⁰².

¹⁰⁰ Caldeggiata, fra gli altri, da G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale*, cit., p. 669.

¹⁰¹ Cass., Sez. I, 7 luglio 2020, n. 21823, in *DeJure*, in cui il giudice per le indagini preliminari, prima, e il tribunale del riesame poi avevano escluso l'esistenza di gravi indizi di colpevolezza, in quanto il riconoscimento facciale effettuato tra fotogramma delle videoriprese sul luogo del fatto e «le effigi presenti su utenze telefoniche di persone coinvolte» (verosimilmente, foto profilo di whatsapp o similari) mediante SARI era stato effettuato su immagini non nitide che non consentivano di riconoscere le fattezze dell'accoltellatore.

I limiti del presente lavoro non consentono di sondare un profilo d'interesse, relativo alla precautelata di recente introduzione, prevista dall'art. 382-bis c.p.p., il quale disciplina la nuova flagranza differita o tecnologica: sul punto G. BORGIA, *Riconoscimento facciale automatizzato e flagranza differita: un connubio possibile?*, in G. GARUTI-E. DEI-CAS-C. TRABACE (a cura di), *Le nuove frontiere della giustizia penale: smaterializzazione e intelligenza artificiale*, Giappichelli, Torino, in corso di pubblicazione.

¹⁰² G. CECANESE, *Aspetti problematici e snodi interpretativi dell'individuazione di persone e di cose*, in *Arch. pen. (web)*, 2018, f. 1, p. 1 ss. Per considerazioni analoghe si veda A. BERNASCONI, *La ricognizione di persone nel processo penale*, cit., p. 116, il quale evidenzia come «[u]na sconcertante anarchia sembra infatti animare il quadro normativo e giurisprudenziale in materia di riconoscimento di persona», giacché «[n]ecessità per l'immediata prosecuzione delle indagini, netta semplificazione delle forme, assenza di garanzie difensive nella fase di svolgimento dell'atto [rappresentano] le coordinate dalle quali si evince la spiccata valenza endoprocedimentale dell'individuazione».

Già Corte cost., sent. 12 giugno 1991, n. 265, escludeva profili di illegittimità costituzionale, per contrasto con l'art. 24, non essendo prevista tra gli atti con diritto di assistenza difensiva, proprio perché l'individuazione è atto endoprocedimentale privo di valenza probatoria.

Eppure, anche qualora si optasse per una soluzione del genere, potremmo davvero dirci tranquillizzati da un uso meramente endoprocedimentale “in vista della immediata prosecuzione delle indagini”? Non si rischia che nel ricognitore umano, al quale venga fatto sapere che il suo responso collima con quello della macchina, si radichi il ricordo in modo inscalfibile – anche se errato –, amplificando di converso pure l’effetto *tunnel* degli inquirenti?¹⁰³ Il problema diviene allora portare in emersione l’utilizzo della tecnologia di riconoscimento in modo da verificare se lo stesso ha “inquinato”, con la propria forza suggestiva, i passaggi susseguenti.

Insomma, neppure l’uso come mera “pista investigativa” appare privo di pericoli: trattandosi di tecnologia dal funzionamento oscuro per la generalità dei consociati – a cui però gli stessi attribuiscono fiducia cieca – la stessa sposta gli equilibri, già sbilanciati, tra individuo e autorità, venendo il primo a sentirsi ancor più sotto scacco, giacché un algoritmo ha riconosciuto *in lui* l’autore del reato ritratto in video. Che non ci si situi meramente sul terreno delle ipotesi è testimoniato dall’esperienza nordamericana, dove risulta documentato almeno un caso¹⁰⁴ in cui un soggetto, arrestato ingiustamente dopo il riconoscimento automatico, aveva persino pensato di optare per un epilogo negoziato con cui gli sarebbero stati comminati anni di carcere, pur di non accettare l’*alea* di un dibattimento già, per quanto sentiva, fortemente pre-giudicato.

Da queste battute si comprende come la posizione di chi scrive sia *a fortiori* contraria all’utilizzo probatorio in senso stretto dei sistemi di riconoscimento biometrico¹⁰⁵, finché non sia garantita la completa trasparenza algoritmica e quindi l’effettività del contraddittorio.

Non pare idonea a scalfire la prefata impostazione la consapevolezza che, lungi dal riferirsi direttamente al *thema* principale della partecipazione dell’imputato al reato, il *match* positivo restituito da una tecnologia di riconoscimento biometrico, in relazione a un soggetto ritratto, ad esempio, mentre si allontana dal luogo di commissione del delitto, consente solo di inferire l’esistenza del fatto principale in base al consueto percorso logico-deduttivo, configurando quindi al più un mero indizio¹⁰⁶.

¹⁰³ S.M. BOWEN, *Man vs. Machine*, cit., p. 52, riporta che «the National Institute of Standards and Technology’s research shows that humans are likely to believe the computer-generated results».

¹⁰⁴ È quanto avvenuto a Nijeer Parks, della cui vicenda dà conto P. BARRANCO, *Match up*, cit., p. 135 ss.

¹⁰⁵ Rilievo probatorio – fra plurimi elementi di riscontro – del riconoscimento tramite SARI riconosciuto da Cass., Sez. II, 20 marzo 2025, n. 18099, in *DeJure*, seppure la percentuale di somiglianza superasse di poco il 50%.

¹⁰⁶ Al riguardo E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit.,

Non mina la convinzione, anzi accresce lo scetticismo, in quanto non sembra improbabile che la pratica sarà portata a ignorare lo iato, similmente a quello che accade, *mutatis mutandis*, in tema di DNA, ritenuto comunemente – ma a torto – prova del *thema probandum*¹⁰⁷, anziché del solo fatto secondario della presenza del soggetto sul luogo. Pare allora concreto il rischio che, come già in parte avvenuto, l'accertamento possa venire fagocitato dalla identificazione biometrica, vero terreno su cui la causa verrebbe a giocarsi¹⁰⁸.

Ritornando al nodo cruciale della trasparenza, non è ozioso ricordare come in letteratura si sia soliti distinguere tra opacità estrinseca (o giuridica)¹⁰⁹, alludendo al segreto commerciale che avvolge i dettagli tecnici relativi all'algoritmo prodotto da imprese private, e opacità intrinseca (o tecnica)¹¹⁰, che invece pertiene ai sistemi di *machine learning*, idonei in quanto tali a sfuggire alla comprensione dei loro stessi programmatori. Distinzione di interesse ai nostri fini poiché SARI *Enterprise* non è oggi un software capace di autoapprendere¹¹¹. Certo, ciò non esclude, un domani, l'impiego di *tools* più sofisticati¹¹², per i quali non basterebbe quindi l'accesso – anche nella forma della «disclosure "garantita"»¹¹³ – al codice sorgente per poterne de-

p. 248 ss. e p. 262, la quale sottolinea che, anche nel caso in cui a venire ritratta fosse l'azione criminosa, il *match* dovrebbe essere inteso come «prova rappresentativa (debole) dell'identità dell'autore del reato perché direttamente riferita» e «mero indizio rispetto al fatto principale, oggetto dell'imputazione» (citazione tratta da p. 251).

¹⁰⁷ Lo ricorda, di recente, O. MAZZA, *Distopia del processo artificiale*, cit., p. 11. Sul punto, E.M. CATALANO, *La prova indiziaria*, in *Prova penale e metodo scientifico*, Utet, Torino, 2009, p. 71; P. FELICIONI, voce *Prova scientifica*, in *Dig. disc. pen., Agg. VIII*, Utet, Torino, 2014, p. 638.

A riprova di quanto sostenuto dalla dottrina circa il valore attribuito al DNA dal diritto pretorio, Cass., Sez. II, 6 luglio 2022, p.m. in c. Cospito, in *C.e.d.*, n. 283904; Cass., Sez. II, 1 giugno 2016, Syziu, *ivi*, n. 268161; Cass., Sez. II, 5 febbraio 2013, Mariller, *ivi*, n. 255257; Cass., Sez. I, 30 giugno 2004, Rizzetto, *ivi*, n. 231182.

¹⁰⁸ Sul punto, F. NICOLICCHIA, *Tecniche di riconoscimento biometrico e fisionomia dell'accertamento: i caratteri dell'istruttoria nella procedura penale algoritmica*, cit., p. 205-206, che condivisibilmente paventa l'espansione di simili fallacie logiche anche alla biometria.

¹⁰⁹ G. FIORELLI, *Calcolabilità del giudizio giuridico e processo penale*, cit., p. 227, nota 204.

¹¹⁰ G. FIORELLI, *Calcolabilità del giudizio giuridico e processo penale*, cit., p. 228-229. Una tripartizione tra opacità tecnica, giuridica e intrinseca viene invece proposta da L. BELVINI, *Intelligenza artificiale e circuito investigativo*, cit., p. 36 ss.

¹¹¹ Questo quanto è emerso durante il *workshop* «Dati biometrici e procedimento penale. Tra profili operativi ed esperienze giudiziarie», tenutosi a Ferrara il 24 marzo 2025, nel corso dell'intervento del dott. Giovanni Tessitore, del Servizio polizia scientifica di Roma.

Contra, L. BELVINI, *Intelligenza artificiale e circuito investigativo*, cit., p. 175 e 177.

¹¹² E. SACCHETTO, *La prova biometrica*, cit., p. 66, richiama l'uso di tecniche di *deep learning* applicate altrove al riconoscimento facciale (si veda, in particolare, nota 114).

¹¹³ Soluzione ipotizzata, fra gli altri, da S. QUATTROCOLO, *Processo penale e rivoluzione digitale: da ossimoro a eniadi*, in *Media Laws*, 24 dicembre 2020, p. 132. Cfr. G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., p. 79 il quale nota come im-

cifrare il concreto funzionamento. Assumerebbe allora rilievo il monito, proveniente dalla dottrina americana, di privarsi delle *black boxes* applicate al mondo della giustizia penale, a favore dei soli algoritmi che garantiscano una effettiva trasparenza (evocativamente, *glass boxes*)¹¹⁴.

L'obiezione è prevedibile: e se tramite questi *tools* opachi fosse raggiungibile la prova d'alibi?¹¹⁵ Di primo acchito, verrebbe da dire, ricordando una fra le più celebri citazioni tratte dalla nostra dottrina, che «l'accertamento dell'innocenza è una posta troppo importante, per essere sacrificata agli idoli della procedura»¹¹⁶. Del resto, un tentativo di impiego *in favor* è documentato pure nelle banche dati giurisprudenziali, in un caso ove la difesa aveva richiesto la rinnovazione dell'istruttoria per consentire l'utilizzo di SARI come prova a discarico (ossia, per dimostrare che la persona ritratta nelle videoriprese mentre era intenta a coltivare canapa indiana non era l'imputato), ma la Suprema Corte aveva rigettato il ricorso, non avendo il difensore documentato la valenza scientifica dello strumento dei cui risultati si chiedeva l'ammissione¹¹⁷... seppure il medesimo fosse in uso alle forze dell'ordine già da qualche tempo. Questo a riprova del potenziale pregiudizio della parità delle armi che vi si annida; preoccupazione principale che non a caso circonda questa tecnologia (come, del resto, le altre a elevata specializzazione), giacché costi e asimmetrie conoscitive rendono un miraggio il paritario accesso agli strumenti disponibili, in

porre la completa accessibilità del *source code* potrebbe consentire ai malintenzionati di modificare il loro comportamento.

¹¹⁴ Si allude a B.L. GARRETT, *Defending Due Process*, cit., p. 140 ss., il quale propone di superare l'attuale impostazione, incentrata sulla spiegabilità dell'IA, a favore della interpretabilità. In sintesi, mentre la prima si limiterebbe a fornire spiegazioni su cosa l'algoritmo potrebbe aver fatto, la seconda consentirebbe di comprendere la causa dell'*output* e di rendere quest'ultimo replicabile.

Sulle differenze tra *interpretable A.I.* e *explainable A.I.*, C. RUDIN-J. RADIN, *Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson From an Explainable AI Competition*, in *Harvard Data Science Rev.*, 1.2(2019), p. 3 ss. Cfr. E. SACCHETTO, *La prova biometrica*, cit., p. 143-146.

Sostengono l'impellente necessità di bandire dal sistema penale ogni uso potenzialmente pregiudizievole di *black boxes*, B.L. GARRETT-C. RUDIN, *The Right to a Glass Box: Rethinking the Use of Artificial Intelligence in Criminal Justice*, in *Cornell Law Rev.*, 109/3(2024), p. 561 ss.; ID., *Interpretable algorithmic forensics*, in *PNAS*, 120/41(2023), p. 1 ss.

¹¹⁵ J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, cit., p. 17.

Più in generale, sulle potenzialità difensive offerte dall'IA., G. LASAGNI, *Difendersi dall'intelligenza artificiale o difendersi con l'intelligenza artificiale? Verso un cambio di paradigma*, in G. DI PAOLO-L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, cit., p. 63 ss.

¹¹⁶ F. CORDERO, *Prove illecite*, in *Tre studi sulle prove penali*, Giuffrè, Milano, 1963, p. 171.

¹¹⁷ Cass., Sez. IV, 18 giugno 2019, n. 39731, in *DeJure*.

astratto, alla stragrande maggioranza degli accusati – poco abbienti e non sempre ben difesi – che animano il mondo della giustizia penale.

Escludendo l'uso delle tecniche di riconoscimento biometrico anche là dove richieste dalla difesa per dimostrare un alibi, si riproporrebbe, dunque, l'annosa *querelle* dottrinale tra coloro che sostengono non sia possibile scindere i divieti probatori a seconda degli effetti – favorevoli o sfavorevoli – prodotti¹¹⁸, e chi invece reputa che «l'inutilizzabilità della prova va intesa come divieto di valutare i risultati conseguenti all'assunzione di una prova vietata unicamente quando tali risultati giustifichino un giudizio di responsabilità dell'imputato, mentre il divieto non vale se dal risultato probatorio emerge l'innocenza»¹¹⁹. Senonché, il divieto di cui si caldeggia l'introduzione si mostra funzionale non solo a restituire effettività alla difesa e al contraddittorio, ma pure a espungere dalla piattaforma conoscitiva risultati prodotti da sistemi della cui reale attendibilità è doveroso dubitare¹²⁰.

Se l'introduzione di una vera e propria *exclusionary rule* valevole per ogni algoritmo insondabile¹²¹ costituisce la via più lineare e condivisibile, occorre riconoscere l'improbabilità che il legislatore, un domani, intervenendo a normare la materia in attuazione della delega contenuta nella legge nazionale sulla intelligenza artificiale¹²², sia disposto a privarsi di ogni ausilio offerto dalla tecnologia di riconoscimento biometrico, anche in tempo reale, potendo muoversi a tale ultimo proposito negli ampi spazi concessi dall'*AI Act*, al fine di localizzare o identificare un

¹¹⁸ Ad esempio, A. CABIALE, *I limiti della prova nella procedura penale europea*, Cedam, Milano, 2019, p. 73-74; M. DANIELE, *Regole di esclusione e regole di valutazione della prova*, Giappichelli, Torino, 2009, p. 157; G. ILLUMINATI, *L'inutilizzabilità della prova nel processo penale italiano*, in *Riv. it. dir. proc. pen.*, 2010, p. 526.

¹¹⁹ Testualmente G. LOZZI, *Lezioni di procedura penale*, 11^a ed., Giappichelli, Torino, 2016, p. 195. Più cauto F. CAPRIOLI, *Verità e giustificazione nel processo penale*, in *Riv. it. dir. proc. pen.*, 2013, p. 613, nel ritenere impresa non agevole dimostrare che le regole di esclusione probatoria valgano anche *contra reum*.

¹²⁰ Come ammonisce A. CAMON, *Le prove*, in A. CAMON, C. CESARI-M. DANIELE-M.L. DI BITONTO-D. NEGRI-P.P. PAULESU, *Fondamenti di procedura penale*, 5^a ed., Cedam, Milano, 2025, p. 353, «pure le prove favorevoli devono avere una certa dignità sul piano epistemologico», ricordando la distinzione già ipotizzata in N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Cedam, Padova, 1992, p. 77-78, la quale discerne tra vizi riconducibili alla violazione di regole poste a garanzia di interessi extraprocedurali o alla inosservanza delle modalità di assunzione, da un lato, e prova ammessa o assunta in violazione dei divieti stabiliti a tutela dell'accertamento, dall'altro lato, portando ad esempio le regole dettate per la testimonianza indiretta.

¹²¹ Opinione a cui accede, fra gli altri, L. BELVINI, *Intelligenza artificiale e circuito investigativo*, cit., p. 146.

¹²² Legge n. 132 del 2025, già citata.

indagato, imputato o condannato per reati non bagatellari, di ricercare in modo mirato specifiche vittime di reato o persone scomparse, oppure in presenza di minaccia reale e attuale di attacco terroristico. Nel farlo, si pone l'esigenza primaria di dare effettività ai proclami contenuti nel regolamento europeo quanto al rispetto dei canoni di proporzione e di stretta necessità.

Pare istruttivo a tale ultimo riguardo rivolgere l'attenzione a una recente pronuncia del *Bundesverfassungsgericht* in tema di controlli occulti continuativi¹²³, nella quale la Corte costituzionale federale tedesca ha specificato che l'utilizzo di mezzi particolarmente intrusivi di registrazione delle immagini è consentito soltanto a fronte di un pericolo specifico o, almeno, di un pericolo identificabile nel caso concreto, non potendosi ravvisare una valida ragione per l'ingerenza derivante da sole regole d'esperienza. Dal momento che più l'interesse minacciato pesa e più gravi sono le conseguenze temute, minore è il grado di certezza relativa alla verifica di esse richiesto per consentire l'intrusione, nel caso in cui si tema un attacco terroristico, il livello di prevedibilità può essere anche inferiore¹²⁴. Tuttavia, la base legale che autorizza la sorveglianza deve essere sufficientemente specifica e chiara¹²⁵; ciò deve fungere da monito per il legislatore che volesse sobbarcarsi l'onere – certo non agevole – di tradurre in legge in modo rigoroso i dettami di quella Corte costituzionale che da decenni si distingue per l'elaborazione più matura del principio di proporzione¹²⁶, muovendosi all'interno delle maglie assai lasche tracciate dal legislatore eurounitario.

Se davvero si vuole garantire l'applicazione in concreto del baluardo eretto a garanzia dell'individuo¹²⁷, posta l'indispensabilità di un provvedimento motivato dell'organo giurisdizionale – prescritto come si è visto dal Regolamento europeo –, dovrebbe essere normativamente imposta, a pena di nullità dello stesso, l'individuazione specifica delle circostanze del caso; degli elementi già acquisiti indicativi o dell'esistenza di gravi indizi in capo al soggetto bersaglio per uno dei reati tassativamente previsti che consentono l'utilizzo della tecnologia *in real time*, da restringere rispet-

¹²³ *Bundesverfassungsgericht*, 14 novembre 2024, 1 BvL 3/22, spec. § 76.

¹²⁴ *Bundesverfassungsgericht*, 14 novembre 2024, 1 BvL 3/22, cit., § 78.

¹²⁵ *Bundesverfassungsgericht*, 14 novembre 2024, 1 BvL 3/22, cit., § 85.

¹²⁶ F. NICOLICCHIA, *I limiti fissati dalla Corte costituzionale tedesca agli strumenti di controllo tecnologico occulto: spunti per una trasposizione nell'ordinamento italiano*, in *Arch. pen. (web)*, 2017, f. 2, p. 1 ss.; R. ORLANDI, *Uso poliziesco dell'intelligenza artificiale. L'insegnamento del Bundesverfassungsgericht*, in *Cass. pen.*, 2023, p. 2167 ss.

¹²⁷ D. NEGRI, *Diritto costituzionale applicato: destinazione e destino del processo penale*, in *Proc. pen. giust.*, 2019, p. 554, chiarissimo nel ribadire «l'ispirazione garantista».

to a quelli indicati in modo largheggiante nel regolamento¹²⁸, o dell'esistenza di una minaccia reale e attuale di attacco terroristico; la durata (anch'essa commisurata allo scopo che si intende raggiungere) e l'ambito spaziale del controllo, nonché le ragioni dell'impossibilità di raggiungere il medesimo risultato con l'ausilio di uno strumentario meno invasivo¹²⁹.

Certo, l'utilizzo di categorie sfuggenti è eventualità che non può dirsi remota; ciò che si impone, tuttavia, è una stretta rispetto a quel minimo, più evocato che descritto, dal legislatore sovranazionale.

¹²⁸ Critiche al novero troppo ampio provengono giustamente da E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 183-184.

¹²⁹ L. BELVINI, *Intelligenza artificiale e circuito investigativo*, cit., p. 180-181, per una impostazione simile.

I WEARABLES NEL PROCESSO ITALIANO

LAURA BARTOLI *

SOMMARIO: 1. Introduzione. — 2. Dal sensore alla sentenza: un percorso tortuoso. — 3. Livello 1: il dato grezzo. — 4. Livello 2: l'informazione elaborata. — 5. I mezzi di acquisizione: le intercettazioni — 6. *Segue*. Il sequestro di oggi... — 7. ... e di domani. — 8. Livello 3: gli ordini di produzione. — 9. Livello 4: i dati resi manifestamente pubblici. — 10. Interpretazione. — 11. Valutazione. — 12. Conclusioni

*Se mai le cose potessero parlare —
ma se parlassero, potrebbero anche mentire*

(Wisława Szymborska, *Se mai*, in *Racconto Antico*, Adelphi, 2025)

1. *Introduzione*

Nel tracciare le coordinate generali¹, siamo incappati in una sorta di stallo alla messicana tra tre diversi poli: le grandi aziende del digitale, che raccolgono, elaborano e stoccano dati personali per profitto, con un grado di garanzie variabile e divieti non sempre pregnanti; l'Unione Europea, che cerca di rallentare (o quantomeno controllare) l'erosione della riservatezza, dettando una serie di limiti; il sistema penale, che è fondato su una contraddizione: ha bisogno della maggior quantità possibile di informazioni per ricostruire i fatti e applicare il diritto, ma deve avere limiti — e, quindi, rinunciare a qualcosa — per non torcersi in uno strumento d'oppressione.

In questo capitolo, studieremo le ripercussioni di questo intreccio sul

* Il lavoro è uno sviluppo delle premesse poste, insieme ad Alberto Camon, in *Dispositivi elettronici indossabili e prova penale*. La redazione è solitaria; la riflessione resta condivisa.

¹ *Dispositivi elettronici indossabili e prova penale*, in *questo volume*.

processo italiano attraverso il prisma dei dispositivi elettronici indossabili. Per farlo, descriveremo brevemente le caratteristiche degli apparecchi e dei dati che generano; esamineremo poi il loro ingresso nel processo, soffermandoci tanto sulle opportunità inedite che offrono, quanto sulle distorsioni, sulle imprecisioni; insomma: sulle trappole nascoste in ciò che si rischia di scambiare per un'algida captazione della realtà.

2. *Dal sensore alla sentenza: un percorso tortuoso*

L'informazione prodotta dai dispositivi indossabili non è una semplice rilevazione registrata e archiviata. Il dato è semmai frutto di una lunga serie di trasformazioni impercettibili: il sensore avverte una grandezza e la trasforma in bit; gli algoritmi elaborano il materiale per estrarre i parametri desiderati — il numero dei passi, il battito cardiaco e così via. Una volta completata l'operazione, le misure sono ormai cristallizzate: non subiscono più modifiche o ricalcoli; vengono semplicemente inviate appena possibile a uno o più apparecchi che le preservano finché l'utente vi consente. La prima tappa del viaggio è generalmente lo *smart phone*: riceve e cataloga i dati che gli vengono trasmessi normalmente via *bluetooth*, quando i due dispositivi si trovano fisicamente vicini; il telefono consente di visualizzarli tramite una *app* in una veste grafica gradevole e chiara, facile da afferrare². Normalmente, l'accesso al programma è subordinato all'apertura di un profilo, cosa che consente di stoccare tutte le informazioni nei server dell'impresa; l'interessato può accedere al materiale in qualsiasi momento, ma non è detto che sia fisicamente salvato sulla memoria del dispositivo: più probabilmente, l'apparecchio è solo un "portale" che consente di vedere quello che è salvato altrove, in un *cloud* aziendale.

Dietro al dato del *wearable*, insomma, c'è un'architettura digitale labirintica che complica a sua volta il problema che affrontiamo qui: di cosa parliamo quando parliamo di informazioni tratte dagli indossabili? Che dati, esattamente, possiamo avere davanti? Da quale memoria sono estratte? Quella del *fitness tracker*, quella del cellulare o quella dell'archivio *cloud*?

² Quasi tutti i modelli commerciali di *fitness tracker* hanno bisogno di sincronizzarsi a un telefono cellulare per la configurazione iniziale; senza, non possono iniziare a funzionare. Una volta compiuto il passaggio, però, il collegamento non è più strettamente necessario: molte delle funzionalità che ci interessano (per esempio: il contapassi) sono disponibili anche senza che i risultati debbano essere periodicamente condivisi con altri dispositivi. A quel punto, la decisione spetta all'utente: almeno in teoria, potrebbe utilizzare l'indossabile in modalità aereo e accontentarsi dei (pochi) dati ospitati nella memoria dell'apparecchio, destinati a essere sovrascritti a stretto giro.

Con quali strumenti giuridici e con quali garanzie minime si possono apprendere? E, infine, quali precauzioni si devono utilizzare nell'interpretarle? Possiamo credere a quello che ci dicono? Per azzardare qualche risposta, esamineremo uno a uno i gradi di elaborazione che abbiamo appena descritto, come se fossero i livelli di un videogioco. Cercheremo così di tracciare una mappa che mostri forze e debolezze del materiale estratto in ciascuna fase, nonché gli strumenti giuridici più utili per ottenerlo e sfruttarlo al meglio.

Prima di proseguire, però, è bene chiarire i limiti del nostro studio, tendenzialmente circoscritto ai *wearable* commerciali più comuni: la probabilità che i loro dati facciano capolino in un processo penale sono più alte. Non ci dedicheremo a un modello in particolare, né a sensori utilizzati nelle ricerche biomedicali o ai dispositivi medici. Di tanto in tanto, useremo questi ultimi come pietre di paragone: essi servono scopi molto diversi da quelle di un ordinario *fitness tracker*; la raccolta e il trattamento dei dati sono quindi organizzati di conseguenza. Toccheremo così con mano gli effetti del GDPR: come abbiamo visto, i principi di limitazione della finalità e di minimizzazione dei dati condizionano irrimediabilmente la quantità e la qualità delle informazioni disponibili, che sono strettamente correlate all'obiettivo del prodotto³.

3. *Livello 1: il dato grezzo*

Nella filiera che trasforma l'azione umana in informazione da salvare, vendere o condividere, il primo passo riguarda necessariamente i sensori, cioè: quei dispositivi «in grado di rilevare dati fisici dall'ambiente circostante e trasmetterli a un sistema di controllo»⁴; in sostanza, percepiscono segnali meccanici e li trasformano in grandezza digitale, generando un tracciato tendenzialmente difficile da leggere, quasi impossibile da interpretare senza conoscenze specialistiche.

L'immagine che riportiamo⁵, per esempio, contiene i segnali registra-

³ V. *retro*, L. BARTOLI-A. CAMON, *Dispositivi elettronici indossabili e prova penale*, parte II, § 3.

⁴ Questa la definizione del dizionario Sabini-Coletti.

⁵ Ringraziamo il Dott. Luca Palmerini e il Dott. Marcello Sicbaldi, rispettivamente ricercatore e dottorando in bioingegneria, per averci messo a disposizione l'immagine e, più in generale, per il prezioso supporto che ci hanno fornito nel corso del progetto. Per lo studio condiviso delle questioni più tecniche v. M. SICBALDI-L. BARTOLI-J.L. ALBITES-SANABRIA-I. D'ASCANIO-A. SILVANI-L. CHIARI-A. CAMON-L. PALMERINI, *Is my smartwatch a valid witness? A systematic review and meta-analysis*, in *Forensic Science International* (in corso di pubblicazione).

Gli apparecchi più studiati raccolgono diversi dati dei sensori nel data base delle app

ti da due sensori (l'accelerometro e il sensore ottico) di un dispositivo indossabile durante 20 secondi di camminata di un adulto sano. Osservando la rilevazione, una persona impreparata non riuscirebbe nemmeno a comprendere qual è l'attività osservata; ottenere informazioni vere e proprie — distanza percorsa, numero di passi, frequenza cardiaca — sarebbe impossibile senza l'aiuto di un tecnico.

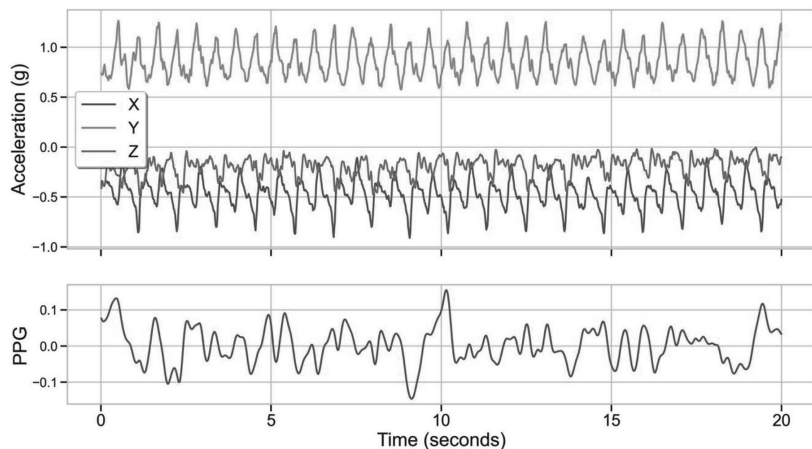


Fig. 1 — Rilevazione dell'indossabile 'Empatica' di 20 secondi di camminata di un adulto sano

Tracciati simili sono continuamente formati dai sensori del telefono cellulare e dei dispositivi indossabili: costituiscono il materiale grezzo che è alla base di ogni elaborazione successiva. In altre parole, questi arabeschi sono il punto di partenza, quello che la convenzione di Budapest e la legge 18 marzo 2008 n. 48 qualificherebbero come 'originale': i testi normativi e le migliori pratiche dell'informatica forense ci obbligherebbero a preservarlo e a trattarlo con tutti i riguardi. Le cautele sono sparse per tutto il codice di procedura penale: le troviamo nella disciplina delle ispezioni (art. 244 comma 2 c.p.p.), delle perquisizioni (art. 147 comma 1-bis c.p.p.), dei sequestri (artt. 254, 254-bis, 259 c.p.p.); insomma: si tratta quasi

'Salute'; non tutte le informazioni sono visualizzate, ma sono comunque estraibili dal dispositivo. Per qualche esempio, con le relative illustrazioni, v. J.P. VAN ZANDWIJK-K. LENSEN-A. BOZTAS, *Have you been upstairs? On the accuracy of registrations of ascended and descended floors in iPhones*, in *Forensic Science Int.l — Digital investigation*, 47 (2023), n. 301660; L. JENNINGS-M. SORELL-H.G. ESPINOSA, *The provenance of Apple Health data: A timeline of update history*, in *Forensic Science International: Digital Investigation*, 50 (2024), n. 301804.

di un *mantra* dell'indagine digitale, e lo è per un'ottima ragione. Se il materiale fosse perduto o alterato, non si potrebbe saggiare la solidità dell'esame successivo: quella che porta a estrarre una informazione precisa da una massa di bit.

Eppure, nel mondo degli indossabili, l'originale scompare quasi immediatamente. È il passaggio fondamentale, ma anche il più effimero: è dunque rarissimo che arrivi sul banco del giudice, per tre ordini di ragioni. Vi abbiamo già accennato⁶, ma è bene riprenderle sinteticamente: sul piano informatico, è difficile pensare di poter salvare e conservare tutti i tracciati di tutti i sensori di tutti i dispositivi. Il monitoraggio costante di diversi parametri per milioni di persone produrrebbe costi di archiviazione giganteschi. Dal punto di vista giuridico, una scelta simile striderebbe con i principi del GDPR, che esige la raccolta e la conservazione della quantità minima di dati, per il tempo strettamente necessario ad assolvere una funzione predefinita: una volta estratto il parametro che interessa — per esempio: il numero di passi — l'originale non serve più, e deve essere eliminato. Il pericolo per la *privacy*, infine, sarebbe ancora più consistente considerando il basso livello di sicurezza degli apparecchi. Molto meglio, quindi, lavorare il materiale grezzo sul posto, direttamente all'interno del dispositivo indossabile, e trasmettere solo il risultato finito: si isola l'informazione che interessa — quella da contabilizzare nella *app* Salute delle diverse case di programmazione — e la si trasmette; tutto il resto è sovrascritto a stretto giro, cioè: è perso per fare spazio alle nuove registrazioni dei sensori.

L'operazione comporta la perdita di una grande quantità di dati, magari decisivi per l'accertamento penale. Prendiamo per esempio la rilevazione dei piani di scale percorsi che, come abbiamo visto, sono talvolta utilizzati dai giudici per ricostruire l'accaduto⁷. L'informazione è costruita a partire dai tracciati di diversi sensori: il barometro e l'accelerometro. Un piano viene contabilizzato soltanto se l'apparecchio registra un dislivello di pressione atmosferica pari a circa tre metri in ascesa, accompagnato da un movimento del corpo; la salita, da sola, non basta: se la persona non si muovesse — per esempio: perché è in ascensore o su una scala mobile — la *app* non mostrerebbe alcuna rilevazione. Lo stesso succede per i differenziali registrati in discesa: semplicemente, non compaiono. Se il programma ci dicesse che l'indossabile di Tizio ha registrato tre piani di scale, non sapremmo se egli si è spostato dal piano terra al terzo; se è sceso in garage e risalito per tre volte; o se ancora ha percorso le prime tre rampe e

⁶ V. *Dispositivi elettronici indossabili*, cit., Parte II, § 3.

⁷ V. *Dispositivi elettronici indossabili*, cit., Parte I, § 5.

poi, stanco, ha preso l'ascensore fino al settimo. L'enigma sarebbe facilmente risolto dal tracciato integrale: i sensori, infatti, captano continuamente sia la pressione, sia l'accelerazione. L'algoritmo seleziona però solo ciò che serve in base a parametri predefiniti: il mondo dei *wearable* commerciali è di solito attento a monitorare lo sforzo fisico, quello che fa consumare calorie; sulla base della finalità dichiarata, quindi, fa una cernita e lascia che il resto sia sovrascritto.

Quando abbiamo, quindi, la possibilità di incontrare i dati grezzi nel processo? Qualcosa si potrebbe recuperare se l'apparecchio fosse sequestrato molto rapidamente, nel breve lasso di tempo che separa l'annotazione dalla sua eliminazione automatica. Se gli investigatori fossero tempestivi, riuscirebbero a congelare lo stato delle cose con una copia forense: a quel punto, le informazioni sarebbero salvate in una memoria immutabile e sottratte al ciclo incessante di scritture e cancellature. Un consulente tecnico esperto, che sa dove cercare, potrebbe trovare almeno parte delle informazioni volatili — nel nostro esempio: avrebbe più elementi per stabilire se Tizio si trovava al primo, al terzo o al settimo piano⁸.

I tracciati puri si potrebbero recuperare con più facilità anche se il *wearable* in questione fosse un dispositivo medico: un *pacemaker* connesso, per esempio, non dà ragguagli solo sulle aritmie, ma fornisce il dettaglio di tutta l'attività cardiaca. Le finalità per cui è progettato sono diverse — permette il monitoraggio da parte di un professionista specializzato — e raccoglie quindi tutte le informazioni che servono a raggiungerle.

4. Livello 2: l'informazione elaborata

Arriviamo al secondo passaggio, che ci porta all'interno dei processori: ricevono il lavoro dei sensori, assemblano i pezzi che servono, calcolano e producono un risultato. Dall'incomprensibile ricamo dei tracciati, gli algoritmi estraggono un'informazione: riconoscono una specifica attività e, come abbiamo visto, la quantificano. È questo il materiale che cade più di frequente nelle mani degli investigatori e dei giudici: è già elaborato, è di più facile lettura e soprattutto è molto più semplice da reperire. Prodotto dall'indossabile, può essere raccolto direttamente dal *wearable*, dal telefono o dai server in cui è normalmente stoccato: il contenuto informativo è esattamente lo stesso; vive contemporaneamente in conteni-

⁸ Per alcuni esempi v. J.P. VAN ZANDWIJK-K. LENSEN-A. BOZTAS, *Have you been upstairs?*, cit., p. 2 s.; J.P. VAN ZANDWIJK- A. BOZTAS, *The phone reveals your motion: Digital traces of walking, driving and other movements on iPhones*, *ivi*, 37 (2021), 301170, p. 4 ss.

tori diversi⁹, che gli investigatori possono raggiungere con atti d'indagine differenti.

Prima di esaminare la disciplina nel dettaglio, conviene fermarsi ad affrontare due problemi che riguardano la qualità del materiale confezionato a questo stadio, e che restano costanti a prescindere dall'istituto giuridico che viene in rilievo. Il primo: non sappiamo come funzionano gli algoritmi che trattano i dati grezzi. Si tratta spesso — meglio: quasi sempre — di software proprietari che non sono mai stati validati da studi indipendenti o certificati da altri laboratori: le sole persone capaci di spiegarne esattamente il funzionamento sono i programmatori che li hanno scritti; salvo rare eccezioni¹⁰, gli unici test di affidabilità che hanno dovuto superare sono quelli interni, se previsti dalle stesse aziende produttrici. Questo significa che vagliare la loro tenuta è complesso: il metodo utilizzato per ottenere una risposta precisa dalla massa di materiale non è noto, e non sono noti nemmeno i suoi limiti. In uno dei rari documenti in cui una casa produttrice ha dovuto condividere qualche dettaglio in più, l'azienda ha evidenziato i difetti e i punti ciechi del dispositivo confrontando l'esattezza di una specifica rilevazione con il migliore standard disponibile: la corrispondente apparecchiatura di monitoraggio ospedaliero¹¹. Un resoconto simile manca per la maggior parte delle funzionalità. Il quadro è ulteriormente complicato da un elemento: non sappiamo quante e quali operazioni sono affidate a intelligenze artificiali; l'Apple Watch, per esempio, vanta un sistema di notifiche pensato per chi soffre di ipertensione

⁹ La comunicazione tra dispositivi può causare duplicazioni di dati o marche temporali diverse, ma le informazioni rilevate restano le stesse.

¹⁰ Apple ha richiesto l'approvazione della Food and Drug Administration (FDA) americana per due caratteristiche del suo orologio connesso: il riconoscimento della fibrillazione atriale e il monitoraggio dell'ipertensione arteriosa; v. rispettivamente FDA, *De Novo Classification Request for Irregular Rhythm Notification Feature*, in *fdagov*, 8 agosto 2018; e FDA, *Hypertension Notification Feature (HTNF)*, *ivi*, 11 e 12 settembre 2025 (corrispondenza tra S. Browning dell'agenzia federale e Bonnie Wu di Apple in cui si riconosce formalmente l'equivalenza tra il *wearable* e un dispositivo medico già approvato). Le domande sono pubbliche, insieme alla documentazione allegata. Non si tratta di pubblicazioni particolarmente compromettenti, ma disegnano almeno una (piccolissima) area di relativa trasparenza.

Questo accade però soltanto per le caratteristiche da certificare secondo lo standard del 'dispositivo medico'; la stessa FDA ha affermato di non avere alcun potere di regolamentazione quanto alle funzionalità che permettono agli individui di «annotare, registrare, tracciare, valutare, prendere decisioni o [ricevere] suggerimenti comportamentali relativi allo sviluppo o al mantenimento della loro forma fisica, della loro salute o del loro benessere»: FDA, *Policy for Device Software Functions and Mobile Medical Applications. Guidance for Industry and Food and Drug Administration Staff*, in *fdagov*, 28 settembre 2022, p. 19.

¹¹ FDA, *De Novo Classification Request*, cit., p. 2.

basato sul *machine learning*¹²: quasi certamente non è l'unico calcolo in cui sono impiegate tecnologie simili. L'opacità che avvolge i programmi, insomma, ci impedisce di sapere non solo come vengono trattati i dati grezzi, ma anche quali passaggi siano spiegabili o interpretabili.

In secondo luogo, anche le verifiche in concreto non appaiono semplici: con l'eliminazione sistematica delle tracce prodotte dai sensori, non si può procedere a un controllo *ex post* dei risultati. Anche se avessimo l'algoritmo — o se ne avessimo uno equivalente — l'operazione non sarebbe comunque ripetibile: non riusciremmo a ripercorrere la catena logica che ha portato all'informazione perché mancherebbe il punto di partenza; avremmo il piatto finito e la ricetta, ma non gli ingredienti.

Ciò non significa che i dati generati dai *wearables* debbano rimanere fuori dal processo; lo scenario dovrebbe però indurre a un'estrema prudenza nella valutazione degli esiti: l'unico modo per sondarne i limiti è lo studio sperimentale, da condurre con lo stesso dispositivo usato nel caso concreto e con lo stesso software; un semplice aggiornamento del sistema operativo potrebbe cambiare il metodo di computo e saremmo d'accapo¹³.

Esistono studi che hanno svolto sperimentazioni più generali, ma si tratta spesso di ricerche condotte ad altri fini: per esempio, la letteratura è ricca di analisi sull'accuratezza di un determinato parametro, per come rilevato da un indossabile "commerciale", per la verifica dei progressi di un paziente nella riabilitazione post-operatoria; o per misurare il deterioramento della camminata in soggetti affetti da malattie neurodegenerative. Certo, non mancano lavori utili anche in campo forense¹⁴, ma non sono stati concepiti a quel fine: la distanza degli obiettivi dovrebbe comunque suggerire qualche cautela.

Le disamine nate per il processo penale non sono molte, ma esistono

¹² Lo si desume da FDA, *Hypertension Notification Feature*, cit.

¹³ Per poter compiere tali verifiche, l'Istituto olandese di scienze forensi (NIF) cerca di procurarsi almeno una copia di ogni dispositivo, così da poter caricare di volta in volta l'applicativo che serve e procedere a una sorta di esperimento mirato, tagliato sulla specifica funzione che serve verificare in quel momento. Ringraziamo della condivisione Jan Peter Van Zandwijk, ricercatore del NIF, che ci ha spiegato con grande generosità le difficoltà e le soddisfazioni quotidiane del lavoro forense sui *wearables*.

¹⁴ Per esempio, la letteratura di medicina dello sport ha approfondito il tema dell'affidabilità della misura del ritmo cardiaco e dello sforzo profuso durante l'esercizio fisico, cosa che può avere una certa rilevanza anche nella ricostruzione svolta a fini penali. Per un esempio v. A.R. JAGIM-N. KOCH-GALLUP-C.L. CAMIC-L. KROENING-C. NOLTE-C. SCHROEDER-L. GRAN-J.L. ERICKSON, *The accuracy of fitness watches for the measurement of heart rate and energy expenditure during moderate intensity exercise*, in *Jour. Sports Med. Phys. Fitness*, 61 (2021) f. 2, p. 205-211.

e sono destinate a diventare più numerose: la diffusione degli apparecchi porterà a interrogarli di frequente; saperne saggiare la precisione tornerà utile sempre più spesso, in una moltitudine di occasioni diverse. Non tutte le funzioni (e non tutti i modelli di mercato) sono però state esaminate con la stessa dovizia¹⁵.

Anche le condizioni delle ricerche, infine, sono da considerare: tanto quelle di ambito medico quanto quelle pensate a uso forense si svolgono spesso in ambienti protetti, in modo da garantire il pieno controllo delle variabili rilevanti. Gli studi sono preziosi perché consentono di gettare luce sul funzionamento di sistemi quasi completamente chiusi, ma non è detto che le conclusioni restino le stesse anche fuori dal laboratorio¹⁶. La misurazione potrebbe essere falsata o addirittura impedita, per esempio, dal sangue che sporca il sensore, o da uno spostamento repentino del dispositivo¹⁷.

5. I mezzi di acquisizione: le intercettazioni

Chiariti i limiti strutturali del materiale, vediamo come può essere prelevato. Uno degli strumenti utilizzabili, almeno in teoria, passa dalla disciplina delle intercettazioni. Come abbiamo visto, l'indossabile si sincronizza di norma con un telefono cellulare e registrare i segnali in transito non solo è tecnicamente possibile ma è anche abbastanza semplice¹⁸. Questo spiega perché molti studiosi statunitensi si stiano interrogando sulla disciplina applicabile all'intercettazione delle trasmissioni fatte da questi strumenti¹⁹.

¹⁵ Per esempio, l'Istituto olandese di scienze forensi ha studiato il pattern di rilevazioni prodotte dagli indossabili a ridosso della morte del soggetto per verificare l'accuratezza nella determinazione dell'ora del decesso: *Smart watches can help solve murders by determining time of death more precisely*, in *nltimes.nl*, 22 febbraio 2025. Per lo studio di altre funzionalità v. J.P. VAN ZANDWIJK-A. BOZTAS, *The phone reveals your motion: Digital traces of walking, driving and other movements on iPhones*, in *Forensic Science Int.l: Digital Investigation*, 37 (2021), n. 301170.

¹⁶ Lo segnalano, per esempio, J.P. VAN ZANDWIJK-A. BOZTAS, *The phone reveals your motion*, cit., p. 10.

¹⁷ M. SCHLUSCHE-K. YEN-S. KNÖDLER-K. FELD, *Digitale Spuren in einem Mordprozess*, in *Rechtsmedizin*, 35 (2025), p. 448.

¹⁸ L. BARMAN, *Every Byte Matters: Traffic Analysis of Bluetooth Wearable Devices*, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2015, scaricabile da dl.acm.org/doi/10.1145/3463512; A.G. FERGUSON, *The "Smart" Fourth Amendment*, cit., p. 563 s.; P. ROBERTS, *BitDefender Finds Phone to Smart Watch Communications easy to Snoop*, in *securityledger.com*, 10 dicembre 2014.

¹⁹ E. HABER, *The Wiretapping of things*, cit., p. 748 s.; G. JOHNSON, *Privacy and the Internet*

Anche se, con ogni probabilità, non sarà la strada battuta più spesso, non si può escludere che, in particolari circostanze, gli organi dell'indagine cerchino di registrare i dati proprio mentre sono trasmessi; in tal caso, bisognerebbe applicare le regole sulle intercettazioni? Nel nostro ordinamento si tratterebbe di capire se l'oggetto dell'intercettazione possa essere soltanto una comunicazione fra individui, oppure se gli artt. 266-271 c.p.p. si prestino ad abbracciare anche lo scambio d'informazioni fra apparecchi elettronici; pur con molte incertezze, la giurisprudenza è al riguardo abbastanza possibilista²⁰.

Il mezzo sarebbe senz'altro efficace e rispetterebbe le garanzie che esige la Corte di giustizia per il trattamento dei dati sensibili²¹. Esso, però, non sembra destinato ad avere un grande rilievo pratico: i requisiti per autorizzare le intercettazioni sono i più stringenti ed esse non sembrano assicurare vantaggi apprezzabili. Se la tecnica non sembra particolarmente attraente per l'autorità giudiziaria, lo è per i malintenzionati: la scarsa sicurezza dei dispositivi consente non solo di esfiltrare dati (autentici), ma anche di introdurne dei nuovi (falsi). Per quanto si tratti di un'ipotesi marginale, conviene tenere a mente che è possibile²².

6. Segue. *Il sequestro di oggi...*

Il modo più facile per acquisire le informazioni che servono è porre l'apparecchio sotto sequestro per copiarne ed esaminarne la memoria. Ma quale accessorio è meglio prelevare? Paradossalmente, vincolare l'indossabile non è l'opzione migliore per consultarne il contenuto: è possibile, ed è sicuramente meglio di niente; in un caso di (sospetto) omicidio, per esempio, il telefono della vittima non è stato ritrovato, ma il *fitness tracker* sì; ci si è accontentati di quello che, insieme ad altri elementi, ha aiutato gli investigatori a ricostruire gli ultimi momenti di vita della persona²³. La memoria del *wearable*, però, è limitata: non contiene l'archivio particolar-

of Things, cit., p. 370; A.N. KITCHEN, *Smart devices and criminal investigations*, cit., p. 49 s.; A.G. FERGUSON, *The Internet of Things*, cit., p. 807 s.; ID., *The "Smart" Fourth Amendment*, cit., p. 549 s.

²⁰ Analisi della questione e citazione di precedenti in A. CAMON, *I confini mobili delle intercettazioni*, cit., p. 9 ss.

²¹ V. *Dispositivi elettronici indossabili*, cit., Parte II, § 8.

²² Avvertono del pericolo anche M. SCHLUSCHE-K. YEN-S. KNÖDLER-K. FELD, *Digitale Spuren in einem Mordprozess*, cit., p. 449 riferendosi al problema dell'interpretazione dei dati in un contesto forense.

²³ M. BICCIATO, *Femminicidio Giada Zanola, il giallo del telefonino: dopo 86 giorni resta introvabile*, in *corriere.it*, 25 agosto 2024. Il dibattito è tuttora in corso presso la Corte d'Assise di Padova.

mente esteso che si potrebbe invece consultare altrove. Sequestrare l'apparecchio potrebbe invece essere necessario per svolgere approfondimenti sull'affidabilità delle rilevazioni: come abbiamo visto, non possono che essere fatti *ex post*, e non è inaudito che i tecnici sperimentino vari scenari proprio con il dispositivo dell'autore o della vittima²⁴.

Per raccogliere il materiale, invece, è meglio prendere il dispositivo secondario, cioè: il telefono con cui l'apparecchio si sincronizza; di solito, è proprio per suo tramite che le informazioni prodotte dagli indossabili arrivano al processo²⁵, e per buone ragioni. L'affidabilità del materiale è la medesima, la quantità è maggiore, l'estrazione dei dati è più semplice. Lo *smart phone*, poi, è a sua volta dotato di sensori: le sue rilevazioni possono intrecciarsi con quelle dei *wearable* e costituire un primo raffronto per la teoria che si sta elaborando. Quindi, secondo quali regole lo si può sequestrare?

Il tema, oggi, è tra i più delicati e incerti. Il codice di procedura penale prevede lo stesso assetto varato nel 1988, mentre le Corti europee — in particolare quella di Lussemburgo — premono verso equilibri diversi, che la giurisprudenza sta metabolizzando con fatica. Secondo la disciplina vigente, il sequestro può essere disposto per tutti i reati, quando occorre assicurare al processo il corpo del reato e le cose pertinenti al reato «necessarie per l'accertamento dei fatti» (art. 253 c.p.p.). È disposto con decreto motivato dell'autorità giudiziaria (art. 253 c.p.p.) — quindi, in indagini, del pubblico ministero — o addirittura, nei casi d'urgenza, può essere eseguito direttamente dalla polizia giudiziaria e sottoposto successivamente alla convalida del magistrato (art. 355 c.p.p.).

Da qualche anno a questa parte, l'assetto è parso eccessivamente generoso se calato nell'ambito di un'indagine digitale. La Corte di cassazione, sempre più sensibile allo sviluppo tecnologico, ha cercato di dettare regole più esigenti almeno rispetto alla quantità di materiale informatico che è lecito prelevare. Anche su impulso della Corte e.d.u.²⁶, ha valorizzato al massimo il requisito della necessità e ha chiarito che la proporzione tra dati acquisiti ed esigenze investigative deve essere chiara dall'adozione all'estinzione della misura; se venisse meno in un momento successivo, la restituzione del materiale diventerebbe doverosa. Se lo *smart phone* è prelevato senza una disamina delle ragioni che legittimano l'acquisizione

²⁴ V. per esempio il caso narrato in M. SCHLUSCHE-K. YEN-S. KNÖDLER-K. FELD, *Digitale Spuren in einem Mordprozess*, cit., che racconteremo meglio oltre: § 9.

²⁵ J.P. VAN ZANDWIJK-A. BOZTAS, *Digital traces and physical activities: opportunities, challenges and pitfalls*, in *Science&Justice*, 63 (2023), p. 370 s.

²⁶ V. *Dispositivi elettronici indossabili*, cit., Parte II, § 5.

della «totalità dei messaggi, filmati e fotografie ivi contenuti», il decreto è nullo perché il sacrificio per i diritti del singolo sarebbe ingiustificato²⁷. Lo schema si deve applicare anche ai dati prodotti dai *wearables*: sono una tra le mille categorie di informazioni intime raccolte nel telefono cellulare; non godono delle stesse tutele garantite alle comunicazioni per effetto dell'art. 15 Cost., ma non possono sfuggire al controllo basato sul principio di proporzionalità, con tutti i limiti che abbiamo già visto. È sempre bene rammentare che le esigenze (investigative e difensive) possono portare al sequestro dell'intera memoria per garantire l'autenticità dell'elemento, così come la sua contestualizzazione. Il rapporto di proporzione, ad ogni modo, deve sempre essere presente ed esplicito.

La giurisprudenza ha quindi lavorato sull'estensione del potere del pubblico ministero, ma non ne ha mai discusso la legittimazione: come abbiamo visto, il dato normativo non dà spiragli. Il Parlamento, come vedremo, stava lavorando a qualche correttivo, ma la Corte di giustizia dell'Unione Europea è stata più veloce: la sentenza *Bezirkshauptmannschaft Landeck* ha inequivocabilmente affermato che il sequestro di un telefonino è un atto troppo intrusivo per essere gestito unicamente dall'organo d'accusa; ha la potenzialità di ledere la sfera informativa più intima e deve essere assoggettato ai parametri di giudizio più severi: quelli dell'art. 10 LED sui dati "sensibili"²⁸. L'atto deve essere dunque previsto solo in un numero limitato di casi e non può prescindere da una valutazione di proporzionalità svolta *ex ante* da un giudice o da un'autorità amministrativa indipendente²⁹.

Una presa di posizione tanto netta ha preso in contropiede i giudici nazionali, che sono ora stretti tra incudine e martello: il codice stabilisce una procedura semplice; il diritto dell'Unione Europea ne pretende una articolata e ricca di elementi che sarebbe meglio far stabilire al legislatore, come per esempio le classi di reati per cui la misura dovrebbe essere esclusa. Intanto, però, la decisione esiste e la Corte di cassazione si è dovuta pronunciare più volte sulla legittimità di un decreto di sequestro emesso dal pubblico ministero. Una pronuncia ha liquidato la questione giocando sul ruolo del magistrato inquirente: è organo d'accusa, ma è anche «ente amministrativo autonomo» che adempie alla sua funzione pub-

²⁷ Questa la conclusione di Cass., Sez. VI, 26 novembre 2025, n. 38331, in *italgiure.giustizia.it/sncass/*, cui si rinvia anche per la ricostruzione del complesso iter giurisprudenziale che ha portato all'approdo.

²⁸ V. *Dispositivi elettronici indossabili*, cit., Parte II, § 8.

²⁹ Questo, in breve, il precipitato di Corte giust., Grande sezione, 4 ottobre 2024, C-548/21, *Bezirkshauptmannschaft Landeck*.

blica «secondo le specifiche regole dettate dal legislatore idonee a garantire anche i diritti dell'indagato»³⁰. Stando a questa lettura, egli sarebbe quindi pienamente autorizzato a trattare dati sensibili senza bisogno di particolari controlli. La soluzione pare però fraintendere un punto: la Corte di giustizia non pone l'accento sull'indipendenza esterna di chi autorizza l'atto; pretende piuttosto l'intervento di un soggetto capace di mediare tra i delicati interessi in gioco: il dovere di indagare da un lato e la riservatezza dell'individuo dall'altro³¹. Per quanto autonomo, non si può chiedere al pubblico ministero di essere terzo rispetto a sé stesso³².

La Cassazione ha poi battuto un'altra via, apparentemente più deferente verso la decisione lussemburghese. Ha affermato che, a norma del diritto dell'Unione, il sequestro dei dispositivi elettronici è subordinato alla previa autorizzazione di un giudice³³; tuttavia, ha ritenuto che i dati raccolti grazie al sequestro del pubblico ministero fossero comunque utilizzabili: la LED non impone sanzioni processuali precise e nel diritto italiano nulla proibisce al magistrato inquirente di disporre il vincolo. L'art. 191 c.p.p., quindi, non verrebbe in rilievo: l'inutilizzabilità consiste nella violazione di un divieto di legge e qui, ha detto la Corte, non ne esiste uno. Tutt'al più, prosegue la motivazione, si potrebbe invocare la categoria delle nullità, ma il pregiudizio risulterebbe comunque sanato dal controllo giurisdizionale del riesame, che nel caso concreto aveva confermato la misura ed escluso ogni violazione dei diritti fondamentali dell'indagato³⁴. Nemmeno questo equilibrio sembra soddisfacente, non foss'altro perché, con un piccolo gioco di prestigio, trasforma un vaglio giurisdizionale obbligatorio ed *ex ante* in una verifica eventuale *ex post*. Lo stratagemma sembra tradire una difficoltà, ma anche una consapevolezza: questa volta non si può supplire alle mancanze del dato normativo grazie a una ragnatela di decisioni sagge; serve un intervento strutturale che riorganizzi la materia. Il Parlamento, nel frattempo, ne ha messi in cantiere due.

³⁰ Cass., Sez. V, 28 gennaio 2025, n. 8376, in *C.e.d.*, n. 287976-01.

³¹ Corte giust., Bezirkshauptmannschaft Landeck, cit., § 103.

³² Inoltre, la stessa Corte di giustizia, pur decidendo ad altri fini, aveva affermato che il requisito può essere soddisfatto solo da una autorità che abbia «la qualità di terzo rispetto a quella che chiede l'accesso ai dati, di modo che la prima sia in grado di esercitare tale controllo in modo obiettivo e imparziale»: Corte giust., Grande sezione, 2 marzo 2021, C-746/18, Prokuratuur, § 54.

³³ Cass., Sez. VI, 1 aprile 2025, n. 13585, in *C.e.d.*, n. 287867-01, anche in *Sist. pen.* (web), 19 maggio 2025, con nota di A. MALACARNE, *La Cassazione sul sequestro dello smartphone: la disciplina italiana non è conforme al diritto dell'UE (... ma il materiale raccolto è comunque utilizzabile)*.

³⁴ Cass., Sez. VI, 1 aprile 2025, n. 13585, in *C.e.d.*, n. 287867-02.

7. Segue. ... e di domani

Un primo disegno di legge, approvato dal Senato e trasmesso alla Camera dei deputati l'11 aprile 2024, prevede l'introduzione dell'art. 254-*bis* c.p.p. intitolato «sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviata e ricevuta»³⁵. Se approvata, la disposizione introdurrebbe una procedura nuova e complessa, illustrata in ben diciannove commi: innanzi tutto, il sequestro dei dispositivi dovrebbe essere disposto con decreto del giudice per le indagini preliminari, su richiesta del pubblico ministero. L'atto dell'inquirente potrebbe bastare soltanto per le urgenze, «quando non è possibile [...] attendere il provvedimento» del giudice e dovrebbe essere poi sottoposto a convalida nelle successive 48 ore. Si prevede poi che la copia del dispositivo avvenga secondo una procedura simile a quella dell'accertamento tecnico irripetibile³⁶; una volta ottenuto il clone, si dovrebbe procedere alla perquisizione, che consentirebbe a quel punto di trovare il materiale utile.

Il progetto, però, è già in qualche modo obsoleto: la Corte di giustizia ha infatti prescritto un livello di tutela superiore. Il disegno di legge non prevede alcun limite oggettivo al vincolo dei dispositivi e alla loro duplicazione: il procedimento sarebbe più garantito, ma sarebbe comunque possibile esperirlo per tutti i reati; come abbiamo visto, l'art. 10 LED non lo consente. Anche per questa ragione, probabilmente, il testo sembra essere stato in qualche modo abbandonato, tanto che il legislatore ha aperto un diverso sentiero per raggiungere la meta. Nel disegno di legge di delegazione europea 2025³⁷, l'odierno articolo 6 è dedicato esattamente

³⁵ Camera dei deputati, Proposta di legge approvata dal Senato della Repubblica il 10 aprile 2024 d'iniziativa dei senatori Zanettin e Bongiorno, «Modifiche al codice di procedura penale in materia di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali», Atto Camera n. 1822, XIX legislatura, disponibile al sito *camera.it*.

³⁶ Salvo alcune eccezioni, i soggetti avrebbero diritto a essere avvisati del conferimento dell'incarico: vi potrebbero partecipare insieme ai consulenti tecnici eventualmente nominati, che potrebbero altresì prender parte alle operazioni di copia. L'unico elemento di discontinuità rispetto all'art. 360 c.p.p. è la riserva di incidente probatorio, che non potrebbe qui essere proposta. La norma, se venisse approvata, troncherebbe l'annoso dibattito sulla natura della creazione della copia forense come atto ripetibile o irripetibile: al momento, la giurisprudenza di legittimità afferma la piena ripetibilità dell'operazione (Cass., Sez. II, 27 novembre 2020, n. 5283, in *C.e.d.*, n. 280618-02), mentre la dottrina sostiene perlopiù il contrario (v. M. DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, p. 441 e ss.).

³⁷ Senato della Repubblica, Disegno di legge presentato dal ministro per gli affari europei, il PNRR e le politiche di coesione e approvato dalla Camera dei deputati il 3 dicembre 2025, «Delega al Governo per il recepimento delle direttive europee e l'attuazione

te al problema che ci riguarda: il primo comma delega al Governo il compito di garantire il «corretto recepimento» della direttiva 2016/680. Il secondo comma autorizza invece la modifica del d.lgs. n. 51 del 2018 e del codice di procedura penale così da adeguarli alla sentenza *Bezirkshauptmannschaft Landeck*, espressamente citata nell'articolo³⁸. Nello specifico, il testo chiede al legislatore delegato di varare una nuova disciplina sull'accesso e sull'acquisizione dei «dati contenuti in dispositivi, sistemi informatici o telematici o memorie digitali» rispettosa dell'art. 10 LED e che mostri quindi almeno tre caratteristiche. Dovrebbe assicurare il rispetto del principio di proporzionalità; dovrebbe prevedere il necessario controllo preventivo del giudice, salvo «i casi di urgenza debitamente giustificati»; e dovrebbe infine definire le categorie di reato per cui è ammesso il prelievo delle informazioni.

L'impianto, se fosse confermato, introdurrebbe divieti precisi: il legislatore dovrebbe avere la cura di sanzionarne l'elusione con un'indicazione simile a quella dell'art. 271 c.p.p., che vieta l'uso del materiale captato da intercettazioni eseguite fuori dai casi previsti o senza previa autorizzazione. Anche se non ci fosse una norma espressa, due argomenti militerebbero per l'inutilizzabilità. Per prima cosa, la legge deve stabilire i casi in cui l'atto può essere disposto; ciò significa che in tutti gli altri dovrebbe essere precluso: la violazione del divieto dovrebbe innescare l'art. 191 c.p.p. Inoltre, le regole sono state espressamente introdotte dalla Corte di giustizia per garantire la tutela di un diritto fondamentale: se fosse possibile aggirarle senza conseguenze, i giudici di Lussemburgo rileverebbero probabilmente un contrasto con l'art. 10 LED.

8. Livello 3: gli ordini di produzione

Saliamo ancora di un gradino per trovare una diversa porta d'accesso alle informazioni prodotte dai dispositivi indossabili, che sono quasi sempre inviate a un *cloud* proprietario per essere archiviate (o, se il servizio lo prevede, anche ulteriormente elaborate). Nel modello consacrato dal legislatore, a quel materiale si accede tramite una procedura di poco diversa dall'ordinario. Gli investigatori potrebbero inoltrare alle aziende una richiesta di consegna dei dati necessari (art. 248 c.p.p.). Se venissero prodotti, non ci sarebbe bisogno di utilizzare poteri coercitivi; altrimenti si

di altri atti dell'Unione europea — Legge di delegazione europea 2025», Atto Senato 1737, XIX legislatura, disponibile al sito senato.it.

³⁸ Camera dei deputati, *Dossier sulla legge di delegazione europea 2025*, 1 dicembre 2025, disponibile al sito camera.it, p. 57 s.

potrebbe ricorrere all'art. 254-*bis* c.p.p. che regola il sequestro di dati presso i fornitori di servizi informatici, telematici e di telecomunicazioni. La norma, introdotta nel 2008 in ossequio alla Convenzione di Budapest, pensa all'ingresso fisico degli inquirenti nella sede del *provider* e si preoccupa di conciliare i bisogni dell'accertamento — mettere le mani sulle informazioni contenute nei server — con quelli imposti dalla necessità di fornire un servizio: dispone che il prelievo possa avvenire senza vincolare necessariamente tutte le apparecchiature, ma mediante la copia della porzione di dati rilevante. Intende, insomma, scongiurare che l'autorità vincoli tutte le memorie dell'impresa digitale, impedendole di funzionare.

Lo schema sembra lineare, ma risente di un limite fatale: è legato alla cultura (anche politica e costituzionale) del secolo scorso, abituata a pensare a uno Stato grande, dal potere soverchiante, e un privato piccolo, che ha bisogno di essere difeso da interferenze arbitrarie. L'autorità, in quel disegno, torreggia, proprio come nell'illustrazione della copertina del *Leviatano* di Thomas Hobbes: *non est potestas super terram qui comparetur ei*. Una forza tanto spaventosa può tutto, tanto che, per essere tollerabile, deve essere contenuta, condizionata e in qualche misura frenata dalle forme del codice di procedura penale; senza, i singoli sarebbero inghiottiti, più che governati. In quell'orizzonte, lo Stato è sempre autonomo nella persecuzione dei reati commessi dai suoi cittadini, nel suo territorio: ha bisogno di limiti, non certo di aiuti. Eppure, lo scenario è cambiato. Nel volgere di pochi lustri, i giganti del digitale si sono affermati e hanno consolidato il loro ruolo di «poteri universali» cresciuti in una «bolla d'immunità»³⁹: godono di possibilità e risorse che alcuni stati sovrani possono solo invidiare⁴⁰, senza le preoccupazioni e le responsabilità sociali che derivano dall'amministrazione della cosa pubblica; sono onnipresenti: offrono servizi in paesi dove non hanno nemmeno sedi di rappresentanza — figuriamoci vere e proprie infrastrutture; raccolgono dati da ogni dove e li convogliano verso uno o più *data center* collocati altrove, spesso fuori dai confini nazionali. L'ubicazione degli elementi, per di più, è indefinita e mutevole: può variare a seconda del momento, sulla base di calcoli che puntano (legittimamente) a minimizzare i costi. In un panorama simile, la spada del potere statale è un'arma spuntata: l'autorità giudiziaria può

³⁹ Le espressioni sono di S. CASSESE, *I giganti del digitale e gli Stati*, in *corriere.it*, 16 aprile 2024.

⁴⁰ La capitalizzazione di mercato di Apple è di 4.000 miliardi di dollari: più del PIL di tutti i paesi del mondo eccetto Cina, Germania, Giappone e Stati Uniti. Il valore combinato di Nvidia, Apple e Microsoft si aggira intorno ai 12.000 miliardi di dollari: *Apple's Market Value Exceeds 186 Countries, Ranks Among Top 4 Economies Globally*, in *aiinvest.com*, 14 dicembre 2025.

chiedere i dati e ottenerli per gentile concessione; altrimenti, non ha necessariamente un ufficio in cui recarsi o un server da sequestrare. Gli elementi di prova sarebbero molto probabilmente custoditi fuori dalla sua giurisdizione: l'art. 254-*bis* c.p.p. non si potrebbe utilizzare, e chiedere aiuto tramite i canali della collaborazione giudiziaria sarebbe spesso troppo complicato. Individuare l'interlocutore giusto non sarebbe scontato; ricevere una risposta in tempo utile, prima dell'inesorabile cancellazione dei dati, ancora meno⁴¹.

È quindi intervenuta l'Unione europea che, per ridare efficacia agli strumenti degli stati, ha adottato tre atti normativi. Il primo è il *Digital Services Act* (DSA)⁴², un regolamento poderoso, applicabile a tutte le imprese che forniscono servizi digitali ai cittadini europei a prescindere dalla collocazione geografica delle sedi. Tra le previsioni d'apertura, disciplina gli «ordini di fornire informazioni» (art. 10), che obbligano i *provider* a collaborare con le «autorità amministrative e giudiziarie nazionali» in cui senza dubbio ricade anche la magistratura penale.

La disposizione conferisce un potere che, sul piano del processo, è meglio definito dal regolamento 2023/1543 e dalla direttiva 2023/1544 (cd. "Pacchetto e-Evidence"), precisati e recepiti dal legislatore italiano in due decreti legislativi emanati dal Governo l'11 dicembre 2025⁴³. Il quadro è assai complesso: ancora una volta non potremo esaminarlo nel dettaglio; ci limiteremo a tratteggiarne le tre linee principali.

La prima addossa un ulteriore dovere ai *provider*: si tratta di una sorta di elezione di domicilio ai fini dell'invio degli ordini⁴⁴. La direttiva 2023/1544 e il d.lgs. 216 del 2025 obbligano i prestatori di servizi a indicare uno «stabilimento designato» o un «rappresentante legale» in uno o più paesi dell'Unione europea (art. 4 l'a.g. n. 330 del 2025)⁴⁵. Essi si dovranno oc-

⁴¹ Per un quadro d'insieme, sia consentito il rinvio a L. BARTOLI, *Digital evidence for the criminal trial: limitless cloud and state boundaries*, in *Big data and Public Law: new challenges beyond data protection*, *Eurojus* — numero speciale, 2019, p. 96 ss.

⁴² Regolamento 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE, "Digital Services Act". Per un commento al testo v. F. WILMAN-S.L. KALEDA-P. LOEWENTHAL (a cura di), *The EU Digital Services Act*, Oxford University Press, Oxford, 2024; HOFMANN-B. RAUE (a cura di), *Digital Services Act. Article-by-Article Commentary*, Nomos, Baden-Baden, 2025.

⁴³ Comunicato stampa del Consiglio dei ministri n. 151, in *governo.it*, 11 dicembre 2025.

⁴⁴ L'art. 3 comma 2 d.lgs. 30 dicembre 2025, n. 216 esime i *provider* italiani che prestano servizi esclusivamente in Italia: per loro bastano gli artt. 248 e 254-*bis* c.p.p.

⁴⁵ Non basta che sia un paese membro qualsiasi: deve trattarsi di uno stato soggetto agli strumenti giuridici del pacchetto *eEvidence* (art. 4 comma 2 d.lgs. 216 del 2025); resta

cupare della «ricezione, dell'ottemperanza e dell'esecuzione» degli ordini (art. 3 comma 2 d.lgs. 216 del 2025). Il disegno è chiaro: anche se l'amministrazione aziendale non si trova sul territorio europeo, le imprese devono rendersi visibili; non può essere l'autorità giudiziaria a rincorrerle.

La direttiva prepara il terreno su cui si colloca il secondo segmento della novella, che introduce gli ordini di conservazione e gli ordini di produzione di prove elettroniche disciplinati dal regolamento 2023/1543 e, sul piano interno, dal d.lgs. 30 dicembre 2025, n. 215. Il primo dei due atti — l'ordine di conservazione — serve a preservare gli elementi utili all'accertamento, così che non vengano cancellati dagli archivi o modificati. È propedeutico a una futura richiesta di trasmissione, ma di per sé non permette all'autorità giudiziaria di accedere ai dati: vuole solo sottrarli alle vicissitudini che rendono volatile la prova digitale. Il d.lgs. n. 215 del 2025 ne disciplina due versioni: una destinata all'ordinamento nazionale, cristallizzata nell'art. 263-*bis* c.p.p. (art. 9 comma 3 d.lgs. n. 215 del 2025); l'altra rivolta alle imprese che si trovano all'estero (art. 3 d.lgs. n. 215 del 2025). La loro disciplina è del tutto analoga: durante le indagini, possono essere emessi per tutti i reati dal pubblico ministero, con l'effetto di congelare i dati per un lasso di tempo non superiore a 90 giorni (prorogabili fino a un massimo di sei mesi).

Gli ordini di produzione europei consentono invece di ottenere il materiale informatico stoccato oltre confine. Non tutte le richieste però si equivalgono: i presupposti per la corretta formazione dell'atto variano in base al tipo di dati che l'autorità vuole ottenere. Un conto è chiedere all'impresa di fornire un indirizzo IP al fine di identificare qualcuno; altro è domandare la copia dei file che si trovano su un dispositivo. Per dosare al meglio le tutele, il regolamento ha diviso le informazioni in quattro categorie⁴⁶: quelle relative agli abbonati, quelle richieste al solo scopo di identificare l'utente «in una specifica indagine penale» (art. 3 n. 10 regolamento 2023/1543), quelle sul traffico e quelle di contenuto.

Per le prime due classi, le garanzie sono meno intense: quei dati consentono di ricollegare un nome a un avatar, agevolando lo svolgimento delle indagini. Gli ordini di produzione che si limitano a questo possono essere emessi durante le indagini dal pubblico ministero, per tutti i reati: la loro disciplina è analoga a quella dettata per gli ordini di conservazione.

Le norme si fanno invece più stringenti per i dati di traffico — tra cui spiccano i metadati e i file di log — e per quelli di contenuto: ottenere i

quindi esclusa la Danimarca, che non ha partecipato all'adozione degli atti normativi (v. considerando n. 101 del regolamento 2023/1543).

⁴⁶ Sul punto, il d.lgs. n. 215 del 2025 opera un rinvio diretto alle definizioni del dell'art. 3 regolamento 2023/1543.

primi consente di tracciare le attività di un individuo con una precisione inquietante; procurarsi i secondi equivale spesso (ma non sempre) a mettere le mani sul dispositivo sbloccato⁴⁷. Il regolamento, quindi, ne restringe l'ambito di applicazione: possono essere autorizzati soltanto nei procedimenti per reati puniti con la reclusione non inferiore nel massimo a tre anni. L'art. 2 comma 3 d.lgs. n. 215 del 2025 stabilisce poi che l'autorità deputata a emetterli prima dell'esercizio dell'azione penale è il giudice per le indagini preliminari, su richiesta del pubblico ministero (eventualmente sollecitata dalle parti private). Il comma 7 chiarisce infine che il materiale ottenuto grazie a un ordine emesso fuori dai casi o senza le condizioni previste è inutilizzabile.

L'assetto, come dicevamo, potrebbe costituire una falsariga utile per l'esercizio di una eventuale delega legislativa sul sequestro di dispositivi informatici: le esigenze da assicurare, gli effetti degli atti e l'impatto sui diritti fondamentali non sembrano essere molto diversi. Ad ogni modo, nonostante la molteplicità degli strumenti, la linea di tendenza sembra ormai omogenea: l'accesso ai dati da parte delle forze dell'ordine non può avvenire senza una valutazione di stretta proporzionalità, nei casi previsti dalla legge e previa autorizzazione di un giudice. Il paradiso, insomma, è davvero perduto.

9. *Livello 4: i dati resi manifestamente pubblici*

Abbiamo fin qui passato in rassegna una serie di strumenti che servono a prelevare ciò che è privato, nascosto agli occhi della collettività. Come acquisire invece i dati che l'utente ha volontariamente reso pubblici, condividendoli su blog, forum online o piattaforme senza filtri all'accesso? La questione è affascinante: da un lato, la natura dell'informazione non cambia: è sempre materiale personale o addirittura appartenente a categorie protette. Dall'altro, però, è arduo sostenere che l'elemento debba essere tutelato esattamente come se non fosse mai stato diffuso: sarebbe difficile chiedere agli investigatori di ignorare ciò che tutti possono conoscere grazie a un semplice collegamento internet⁴⁸. Sul piano giuridico,

⁴⁷ La quantità degli elementi dipende dalle impostazioni di condivisione dell'utente e dallo spazio di memoria che ha disposizione nel *cloud*.

⁴⁸ Diverso il caso degli investigatori che, per accedere a materiale almeno in parte riservato, creano un falso profilo su una piattaforma e raccolgono di lì informazioni. La pratica è ormai affermata: già nel 2021, Facebook ha scritto al capo della polizia di Los Angeles chiedendo di porre fine al compimento sistematico di operazioni "sotto copertura" online: L. BHUIYAN-S. LEVIN, *Facebook demands LAPD end social media surveillance and*

come abbiamo visto, anche l'art. 10 LED ammette uno standard meno severo.

Resta comunque un problema: il codice di procedura italiano non prevede distinzioni tra dati personali e “sensibili”, che godono invece di garanzie rafforzate nel diritto dell'Unione. Per la prima classe, l'ordinamento italiano prevede garanzie sufficienti: l'art. 4 LED impone la proporzionalità e la rilevanza del prelievo, già contemplate nel nostro ordinamento dalle disposizioni generali sulle prove. Se invece il materiale appartiene a categorie particolari, la direttiva pretende qualcosa in più: deve essere raccolto sulla base di una valutazione di stretta necessità e con le garanzie appropriate. Nessuna norma di diritto interno sembra declinare meglio tali requisiti: nell'ambito di una delega concessa per tradurre meglio le garanzie della LED, il legislatore potrebbe intervenire.

I dati, oggi, possono invece entrare a processo secondo la disciplina del documento, cioè a norma dell'art. 234 e 234-*bis* c.p.p.

10. Interpretazione

Visto come si formano e come si acquisiscono i dati prodotti dai *wearables*, non resta che chiedersi che contributo, di preciso, possono dare, prima, alla formulazione di un'ipotesi d'accusa e, poi, alla decisione.

Incorporare le informazioni nella propria ricostruzione senza alcuna verifica preliminare, infatti, potrebbe risultare azzardato. Innanzi tutto, occorre tenere ben presente che il dispositivo non è inseparabile dall'individuo: tendenzialmente è indossato dall'utente, ma questi può toglierlo, smarrirlo, prestarlo... non è detto che a una traccia digitale su quell'apparecchio corrisponda necessariamente un'attività (o un'inattività) della persona⁴⁹. Per trovare un esempio, basta guardare alla cronaca: un orologio connesso si è sfilato dal polso del proprietario mentre questi passeggiava nel bosco. L'oggetto ha registrato una caduta traumatica e ha avvertito automaticamente il numero d'emergenza: i soccorritori hanno cercato l'uomo per sei ore prima di trovarlo illeso a casa sua⁵⁰. Quel dato, pro-

use of fake accounts, in *theguardian.com*, 18 novembre 2021. Per una ricostruzione v. Congressional Research Service, *Law Enforcement and Technology: Using Social Media*, in *crsreports.congress.gov*, R47008, 11 gennaio 2022; R. LEVINSON-WALDMAN, *Principles for Social Media Use by Law Enforcement*, in *brennancenter.org*, 7 febbraio 2024. Il punto meriterebbe un approfondimento, ma ci porterebbe probabilmente troppo lontano.

⁴⁹ Anche qui, molto dipende dal tipo di dispositivo con cui abbiamo a che fare: se il *pacemaker* impiantato ci offre una certezza, non si può dire lo stesso per gli orologi, gli anelli, le spille, gli auricolari, i telefoni.

⁵⁰ M. TOTARO, *Lo smart watch lascia l'Sos: decine di soccorritori lo cercano per ore nei boschi, ma dormiva a casa*, in *repubblica.it*, 17 agosto 2025.

tabilmente, non dovrà mai essere interpretato nell'ambito di un processo; in circostanze diverse, però, la rilevazione avrebbe facilmente potuto spingere gli investigatori verso una conclusione fuorviante: per esempio, avrebbero potuto leggere il dato come la prova di un episodio violento subito dalla persona. Inoltre, i dispositivi possono essere ingannati: la luce verde del sensore che misura l'attività elettrodermica non è riflessa solo dalla pelle umana, ragion per cui alcuni indossabili rilevano una frequenza cardiaca anche se indossati da una tazza di caffè, un rolo di carta igienica o addirittura una banana⁵¹.

Ma mettiamo che non ci siano dubbi sulla paternità delle informazioni: la "testimonianza" dell'indossabile sarebbe comunque da scrutinare con attenzione, perché gli algoritmi che la formano leggono le rilevazioni dei sensori secondo determinate euristiche, cioè: sulla base di ciò che più comunemente accade, che non necessariamente corrisponde a quanto è avvenuto. Riprendiamo l'esempio dei piani di scale, contati a partire dall'idea che un livello equivalga all'altezza di circa 3 metri. Se il fatto da ricostruire si fosse svolto in un palazzo storico, con sale nobili dai soffitti altissimi e stanze ricavate in ammezzati asfittici, l'informazione sarebbe da leggere con cautela: segnalerebbe uno spostamento verso l'alto, ma non servirebbe a collocare la persona all'interno dell'edificio⁵². Lo stesso accade per il numero di passi, che alcuni dispositivi calcolano in base al moto delle braccia: qualunque oscillazione contribuisce ad aumentare la conta, e gli stessi produttori nel sono al corrente. La guida di alcuni modelli di FitBit indica per esempio che impastare il pane a mano accresce il conteggio, così come guidare. Allo stesso modo, il numero di passi di chi cammina a braccia ferme sarà sottostimato⁵³. O ancora: un movimento troppo netto può essere letto come un segnale di pericolo; la polizia del Leicestershire ha per esempio raccomandato agli avventori di un festival musicale di spegnere o togliere gli *smart watches* perché i gesti, i salti e le spinte, del tutto fisiologici in quel contesto, innescano spesso le chiamate di sicurezza⁵⁴.

Poniamo di aver superato anche questo ostacolo: resta il dilemma dell'affidabilità delle informazioni. La verifica soffre di tutti i limiti che

⁵¹ V. la deliziosa fotografia in M. SCHLUSCHE-K. YEN-S. KNÖDLER-K. FELD, *Digitale Spuren in einem Mordprozess*, cit., p. 448, che mostra un indossabile mentre comunica i valori del battito di una banana lievemente tachicardica.

⁵² Per un esempio in questo senso, v. J.P. VAN ZANDWIJK-A. BOZTAS, *Digital traces and physical activities*, cit., p. 372 s.

⁵³ M. SCHLUSCHE-K. YEN-S. KNÖDLER-K. FELD, *Digitale Spuren in einem Mordprozess*, cit., p. 447.

⁵⁴ *Se si vuole pogare è meglio spegnere lo smartwatch*, in *ilpost.it*, 15 giugno 2025.

abbiamo già esaminato: gli algoritmi sono segreti; i dati originali sono quasi sempre inattingibili; gli studi di validazione non sono esaurienti sia perché le condizioni di laboratorio non replicano il caos della vita reale, sia perché il profluvio di funzioni, modelli e programmi complica le cose. Se lo guardiamo in termini assoluti, il problema è quasi irrisolvibile; non è però detto che il punto di vista sia l'unico, o quello più proficuo.

Un caso tedesco può aiutarci a chiarire il punto⁵⁵: un uomo ha chiamato il numero di emergenza dicendo di avere appena trovato la moglie, pugnalata a morte, riversa in una pozza di sangue; in seguito, ha detto agli investigatori che lui si trovava fuori con i figli: aveva salutato la donna poco prima per ritrovarla senza vita al rientro. La vittima, però, indossava un FitBit, e i dati hanno subito fatto supporre un decorso diverso: il dispositivo aveva smesso di registrare passi a partire da un orario incompatibile con la versione del marito; la rilevazione del ritmo cardiaco mostrava crescite e decrescite di intensità in momenti che, ancora una volta, stridevano con l'ipotesi di partenza. Per capire quanto ci si potesse fidare di quelle informazioni, i consulenti tecnici incaricati hanno svolto una serie di simulazioni con il dispositivo originale: l'hanno fatto indossare a una persona simile alla vittima per peso e altezza; inoltre, si sono contemporaneamente avvalsi di uno strumento di misurazione più preciso: una fascia toracica che dovrebbe misurare il battito con la stessa accuratezza di un vero e proprio elettrocardiogramma. Gli esperti hanno così verificato che il numero di passi può essere senz'altro inesatto, ma il conteggio a zero corrisponde quasi certamente all'assenza di movimento delle braccia; l'apparecchio non è risultato preciso nemmeno nella misura delle pulsazioni, ma si è mostrato in grado di segnalare fedelmente l'andamento dell'attività cardiaca⁵⁶, rivelando così i suoi momenti di crescita, decrescita ed estinzione. L'inaffidabilità dell'apparecchio è stata in qualche modo certificata dagli esperimenti dei tecnici: nessuna delle due conte si è rivelata esatta. Ciò non ha però impedito di considerarle utili: per la specifica ipotesi da approfondire — le cose sono andate come ha detto il marito? — un risultato indicativo si è rivelato più che sufficiente.

In altre parole, molto dipende dal quesito investigativo cui si vuole rispondere tramite le rilevazioni: se qualcuno dicesse di aver dormito tutta la notte e il suo indossabile, in quel lasso di tempo, avesse contato 20.000 passi, non avremmo bisogno di sapere se ha percorso 10 o 15 chilometri

⁵⁵ L'indagine è riportata nel dettaglio in M. SCHLUSCHE-K. YEN-S. KNÖDLER-K. FELD, *Digitale Spuren in einem Mordprozess*, cit., p. 446 ss.

⁵⁶ M. SCHLUSCHE-K. YEN-S. KNÖDLER-K. FELD, *Digitale Spuren in einem Mordprozess*, cit., p. 447 ss.

per affermare che qualcosa non torna. Anche con un margine di incertezza gigantesco — 5 chilometri — il dato sarebbe utile. Se invece il sospettato sostenesse di aver fatto visita al dirimpettaio della vittima, ci sarebbe bisogno di una misura esatta al metro per dimostrare che mente; se non ci si riuscisse, bisognerebbe accontentarsi di due scenari altrettanto conciliabili con la stessa traccia informatica: per capire quale dei due è il più plausibile, bisognerebbe cercare altrove. Da tale confronto possiamo trarre due insegnamenti; per prima cosa, più la teoria da verificare e le informazioni registrate appaiono compatibili, maggiore è il bisogno di misurare l'accuratezza del dispositivo. Inoltre, sembra utile prendere in prestito un argomento che riguarda di solito gli esperimenti giudiziali: come le simulazioni, anche i dati dei *wearables* sono epistemologicamente più forti quando permettono di escludere una certa ricostruzione dei fatti. Certo, potrebbero essere impiegati anche per affermare la verosimiglianza di un certo decorso o per formulare una prima teoria sugli eventi, ma in quei casi sarebbe meglio prendere le informazioni con tutto lo scetticismo che meritano: difficilmente si riuscirà a provare alcunché sulla sola base di quegli elementi. Illudersi quindi di avere una fotografia perfetta di tutto ciò che accaduto, cristallizzata istantaneamente e senza possibilità di errore, sarebbe a dir poco ingenuo: presentare le informazioni al giudice come se fossero verità irrefutabili sarebbe del tutto irresponsabile⁵⁷. È qui fondamentale tenere a mente la norma dell'art. 7 LED, quella che invita a distinguere i fatti dalle opinioni: la distanza tra la traccia informatica e il significato che la parte desidera attribuirle dovrebbe essere sempre chiara.

Nell'interpretazione investigativa, infine, non è fuori luogo guardare con qualche diffidenza anche agli strumenti di analisi: i software che raccolgono, esaminano, organizzano e illustrano gli elementi elettronici sono sempre più diffusi, e non per caso. Consentono di passare da una matassa di bit inerte, che l'agente medio magari fatica a esaminare con profitto, a una serie di informazioni "preconfezionate", classificate in categorie omogenee e disposte secondo una linea del tempo immediatamente leggibile. Anche quegli algoritmi (proprietary), però, mostrano tassi d'errore. Secondo un recente studio, uno dei software più utilizzati opererebbe semplificazioni addirittura nocive per la solidità dell'indagine: presenterebbe difetti fuorvianti nell'etichettare i dati, nel visualizzare le marche temporali, nella presentazione del contesto in cui calare il singolo elemento. La ricerca ha concluso che sarebbe sempre meglio servirsi di almeno

⁵⁷ La preoccupazione di esaminare la traccia rigorosamente, così da rendere «forensically responsible statements» è esplicita in J.P. VAN ZANDWIJK- A. BOZTAS, *The phone reveals your motion*, cit., p. 2.

due strumenti diversi, così da studiare le convergenze e le divergenze nell'esibizione del prodotto finito⁵⁸.

11. *Valutazione*

Davanti a uno scenario così complesso, come può orientarsi il giudice? È armato del suo libero convincimento, ma non è detto che abbia grande dimestichezza con il funzionamento dei dispositivi o con nozioni di statistica tali comprendere fino in fondo il resoconto dei tecnici, specie se essi hanno confrontato la verosimiglianza di due scenari comunque plausibili⁵⁹.

Se fosse necessario andare per il sottile — quindi: fuori dai casi in cui le discrepanze sono talmente ovvie da rendere superfluo un vaglio approfondito sull'affidabilità — il compito di guidare il giudicante spetterebbe innanzi tutto alla parte che introduce il materiale, incalzata all'occorrenza dall'avversaria. Un contraddittorio tecnico di buon livello può portare alla luce gran parte dei problemi che abbiamo passato in rassegna, laddove sia necessario esplorarli: l'impossibilità di verificare autonomamente l'affidabilità delle rilevazioni, l'alea che spesso le accompagna, gli errori di analisi e presentazione, l'esistenza di condotte alternative plausibili che potrebbero facilmente spiegare lo stesso risultato.

Per farlo, occorre che tanto l'accusa quanto la difesa (tramite i suoi consulenti) abbiano accesso ai dati, agli strumenti di analisi e al dispositivo (o a un apparecchio equivalente) in modo da testare le diverse ipotesi: abbiamo visto che, per stabilire il significato delle informazioni di un singolo FitBit, il pubblico ministero tedesco ha commissionato approfondimenti accurati ai suoi consulenti, cosa che ha consentito al giudice di sapere cosa dimostrasse esattamente quel materiale. Dal canto suo, il giudicante dovrebbe fare tesoro degli insegnamenti della Corte europea dei diritti dell'uomo: è vitale che le obiezioni e le rimozioni di ciascuno dei soggetti siano ascoltate e trattate con l'attenzione che meritano. Possono essere respinte, anche con motivazioni molto nette; quel che il giudice non può fare è fingere che non siano mai esistite⁶⁰.

⁵⁸ D.B. ANDERSEN-N. SUNDE-K. PORTER, *Tool induced biases? Misleading data presentation as a biasing source in digital forensic analysis*, in *Forensic Science Int.l: Digital Investigation*, 52 (2025), n. 301881, p. 8.

⁵⁹ Per uno studio scoraggiante v. W.C. THOMPSON-R. HOFSTEIN GRADYA-G.S. MORRISON, *Does explaining the meaning of likelihood ratios improve lay understanding?*, in *Science & Justice*, 65 (2025), f. 6, n. 101352.

⁶⁰ V. *Dispositivi elettronici indossabili*, cit., Parte II, § 6.

E se le parti non si facessero carico del necessario lavoro di chiarimento? Il materiale potrebbe comunque essere prodotto — pare difficile negargli la qualifica di documento — e il decisore dovrebbe affrontare il problema con i mezzi che gli sono affidati. Ancora una volta, le distinzioni tracciate dalla Corte e.d.u. suggeriscono la strada da percorrere⁶¹. Il magistrato si troverebbe di fronte a un elemento “di bassa qualità”: sarebbe prudente considerarlo come un elemento scarsamente convincente e attribuirgli tutt'al più un ruolo secondario nell'economia della decisione.

Se invece ritenesse di non poter fare a meno di quelle informazioni, dovrebbe resistere alla tentazione di improvvisarsi esperto: correrebbe il rischio di sottovalutare il grado di complessità della questione e di guardare alle approssimazioni di un *fitness tracker* come se fossero una registrazione impassibile della realtà⁶². Farebbe meglio a disporre d'ufficio tutti gli accertamenti necessari nella forma della perizia: il suo ausiliario, debitamente formato, potrebbe chiarire i limiti di affidabilità del materiale e illustrargli nel rispetto del contraddittorio qual è lo scenario che gli elementi sembrano supportare, posto che è quasi impossibile — giova ripeterlo — ricostruire interamente un evento sulla sola base dei dati degli indossabili. Anche se il giudice ritenesse la prova particolarmente persuasiva, l'impossibilità pratica di validare il dato dovrebbe comunque far scattare l'obbligo convenzionale dei riscontri; insomma: condannare l'imputato soltanto in base alle percezioni del *wearable* appare epistemologicamente insostenibile; la possibilità, quindi, dovrebbe essere preclusa.

12. Conclusioni

Nonostante il ritardo e nonostante la fatica, l'ordinamento sta finalmente reagendo allo strappo provocato dalla tecnologia: la riflessione intorno ai “nuovi” diritti è sempre più matura e il caso dei dispositivi indossabili consente di osservare da un punto di vista privilegiato uno dei fenomeni normativi più interessanti e attesi degli ultimi anni: la ritessitura di una trama ormai logora, troppo fragile per servire allo scopo.

L'insufficienza è ormai conclamata e il sistema sembra averne preso

⁶¹ Per l'esame dei precetti e i necessari riferimenti giurisprudenziali v. *Dispositivi elettronici indossabili*, cit., Parte II, § 6.

⁶² Secondo J.P. VAN ZANDWIJK-A. BOZTAS, *Digital traces and physical activities*, cit., p. 370, «una delle questioni principali che occorre affrontare riguarda il valore probatorio delle tracce [degli indossabili] per gli scenari in esame, cioè: cosa può dirci il materiale e, cosa altrettanto importante, cosa *non* può dirci sulle ipotesi investigative» (corsivo nel testo, traduzione nostra).

atto: il bisogno di limitare per legge l'accesso ai dati è stato avvertito in maniera trasversale: lo rintracciamo nella giurisprudenza della Corte e.d.u., nelle prese di posizione della Corte di giustizia e nei progetti del legislatore italiano. Allo stesso modo, l'attenzione a un vaglio di proporzionalità serio, che sappia distinguere le intrusioni indispensabili da quelle di cui si può fare a meno, interseca tutti i livelli: se oggi il custode dell'equilibrio è il pubblico ministero, domani la sua valutazione non basterà più e cederà il passo a quella di un giudice terzo.

Il livello di garanzie, insomma, sta crescendo: sarebbe forse esagerato parlare di una vera e propria riserva di legge e di giurisdizione, ma il risultato finale dell'elaborazione sembra somigliarle abbastanza. Ciò che cambia è la fonte dei doveri: non li troviamo direttamente nella Costituzione repubblicana, magari grazie a un'estensione spericolata della nozione di 'comunicazione'; li ricaviamo da un'elaborazione lunga, incerta e complessa che arriva dalle Corti europee e dagli atti normativi dell'Unione. Le posizioni assunte in quelle sedi stanno penetrando, quasi goccia a goccia, nell'ordinamento italiano, consentendogli di rinnovarsi e di darsi geometrie nuove. Se tutte le riforme che abbiamo riassunto vedranno la luce, il nostro ordinamento si avvicinerà molto a quell'insieme di cerchi concentrici descritto tanto dalla LED, quanto dalla Corte e.d.u. Il sequestro di cose continuerà a essere appannaggio della pubblica accusa; quello di informazioni no: al livello più esterno troveremo gli ordini di produzione e il sequestro di memorie digitali; a quello più interno troveremo le intercettazioni. L'intensità delle tutele non varierà in base al tipo di dato, ma sarà graduata rispetto alla profondità dell'intrusione. Certo, l'assetto è complesso e deve ancora essere varato: sarà senz'altro messo a punto dal legislatore delegato prima e dalla giurisprudenza poi, ma sembra una prima bozza di risposta al *translation problem* da cui siamo partiti. Almeno sul piano dei diritti.

Le soluzioni, invece, sembrano ancora lontane su un altro versante: quello del dialogo tra giuristi e tecnici. Gli elementi di prova elettronici non sono destinati a rarefarsi, anzi: saranno sempre più numerosi. I *wea-rables*, da questo punto di vista, sono soltanto l'inizio: l'unico limite al piazzamento dei sensori è ormai la fantasia dei progettisti; le case, gli elettrodomestici e le automobili contengono una mole di informazioni impressionante. Perché tale patrimonio conoscitivo sia più utile che insidioso, servono criteri trasparenti per la sua analisi, strumenti più affilati per la sua comprensione e coordinate condivise per impostare un confronto. A quel punto, parleremo tutti la stessa lingua: di tradurre non ci sarà più bisogno.

L'INCESSANTE ESPANSIONE DELLA BANCA DATI BIOMETRICA EURODAC CONSULTABILE (ANCHE) PER FINALITÀ DI CONTRASTO

LORENZO AGOSTINO

SOMMARIO: 1. Origini ed evoluzione della banca dati Eurodac. – 2. Le (blande) procedure di accesso a Eurodac per finalità di contrasto. – 3. Riconoscimento facciale tramite Eurodac. – 4. Eurodac in un contesto di interoperabilità: rischi di elusione delle (già inadeguate) garanzie.

1. *Origini ed evoluzione della banca dati Eurodac*

Eurodac, acronimo di *European Asylum Dactyloscopy Database*, è una banca dati biometrica unionale istituita nel 2000 e operativa a partire dal 2003¹.

Essa nacque come strumento utile allo svolgimento delle procedure di asilo, con particolare riferimento alla determinazione dell'ordinamento competente per l'esame delle relative domande secondo le regole previste dalla allora vigente convenzione di Dublino². A tal fine, era indispensabile mettere nelle condizioni lo Stato sul cui territorio fosse illegalmente entrato uno straniero di verificare se questi avesse precedentemente presentato domanda in un altro Paese. Per farlo, si ritenne opportuno implementare un sistema capace di confrontare informazioni particolarmente rile-

¹ L'atto costitutivo è il reg. 2000/2725/CE «che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino». Per un'analisi della banca dati sotto il vigore di tale regolamento, v. M. GIALUZ, *Principio di accessibilità e banche dati di "primo pilastro"*, in F. PERONI-M. GIALUZ (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, EUT, Trieste, 2009, p. 145 ss.

² «Convenzione sulla determinazione dello Stato competente per l'esame di una domanda di asilo presentata in uno degli Stati membri delle comunità europee», firmata a Dublino il 15 giugno 1990.

vanti nella determinazione dell'identità della persona, vale a dire le impronte digitali.

Fu così messa a punto una banca dati centralizzata in cui raccogliere le impronte dei richiedenti asilo e di coloro i quali avessero attraversato irregolarmente le frontiere esterne, in modo tale da poter operare un confronto con quelle di volta in volta trasmesse da uno Stato in quanto appartenenti a uno straniero illegalmente presente sul suo territorio.

Ma questa embrionale forma di banca dati biometrica era naturalmente destinata a evolversi, tanto da essere – ancora oggi – “in movimento”.

Il reg. 2013/603/UE³, subentrato all'atto primigenio e vigente fino al giugno 2026⁴, ha inciso profondamente sulle caratteristiche del *database*, accrescendone le funzioni⁵: esso è divenuto impiegabile non più soltanto per l'individuazione dello Stato competente nell'ambito delle procedure di asilo, ma anche per finalità – molto distanti⁶ – di *law enforcement*⁷. Premesso che «[n]ella lotta al terrorismo e ad altri reati gravi è essenziale che le

³ Regolamento «che istituisce l'“Eurodac” per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il regolamento (UE) n. 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (rifusione)».

⁴ L'art. 62 del reg. 2024/1358/UE ne prevede infatti l'abrogazione a decorrere dal 12 giugno 2026.

⁵ Come osservato da N. VAVOULA, *The Recast Eurodac Regulation. Are Asylum Seekers Treated as Suspected Criminals?*, in C. BAULOZ-M. INELI-CIGER-S. SINGER-V. STOYANOVA (a cura di), *Seeking Asylum in the European Union. Selected Protection Issues Raised by the Second Phase of the Common European Asylum System*, Brill, Leiden, 2015, p. 252, «[t]he Recast Regulation brings about a significant change in the nature and objective of the Eurodac database».

⁶ Talmente distanti che, secondo l'*European Data Protection Supervisor, Opinion on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [...]/... (Recast version)*, 5 settembre 2012, § 27, «[t]he assessment as to the necessity and proportionality of the creation of EURODAC would have been completely different if law enforcement access was envisaged from the outset». In proposito, v. anche le considerazioni di V. FERRARIS, *Eurodac e i limiti della legge: quando il diritto alla protezione dei dati personali non esiste*, in *Dir. imm. citt.*, 2017, n. 2, p. 2 ss., che richiama il suddetto parere.

⁷ L'ampliamento è un chiaro portato di quel «cambio di passo della cultura investigativa che, spinta in questa direzione dalla capacità intrusiva e dalla straordinaria “plasticità” degli strumenti messi a disposizione dall'informatica, è andata vieppiù abbracciando istanze preventive tutte impennate su un controllo diffuso e generalizzato delle informazioni che possano essere ritenute utili a difendere la sicurezza dello Stato e della collettività

autorità di contrasto dispongano delle informazioni più complete e aggiornate possibili per poter svolgere i loro compiti» e che «[l]e informazioni contenute nell'Eurodac sono necessarie a fini di prevenzione, accertamento o indagine»⁸, se ne è allargato l'accesso alle autorità designate dai Paesi membri, nonché a Europol.

Il campo di applicazione di Eurodac, infine, è stato esteso quanto a tipologia di dati conservati. Una delle principali novità del reg. 2024/1358/UE⁹, adottato nell'ambito del c.d. «patto sulla migrazione e l'asilo»¹⁰ e sostitutivo dell'atto del 2013, è costituita dall'inclusione all'interno del sistema delle immagini del volto dei soggetti attenzionati¹¹ – la platea dei quali è stata peraltro a sua volta ampliata¹² –, anche nella prospettiva di installare nella banca dati un applicativo di riconoscimento facciale¹³. La possibilità di usufruire di un maggior numero di identificatori biometrici è stata infatti ritenuta essenziale per una migliore gestione dei flussi di persone alle frontiere¹⁴ e, dunque, data la censurabile «convergenza tra

da ogni minaccia o aggressione criminale o terroristica». In questi termini, B. GALGANI, *Giudizio penale, habeas data e garanzie fondamentali*, in *Arch. pen. (web)*, 2019, n. 1, p. 13 s.

⁸ Così il considerando n. 8 del reg. 2013/603/UE.

⁹ Regolamento «che istituisce l'«Eurodac» per il confronto dei dati biometrici ai fini dell'applicazione efficace dei regolamenti (UE) 2024/1351 e (UE) 2024/1350 o del Parlamento europeo e del Consiglio e della direttiva 2001/55/CE del Consiglio e ai fini dell'identificazione dei cittadini di paesi terzi e apolidi il cui soggiorno è irregolare, e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, che modifica i regolamenti (UE) 2018/1240 e (UE) 2019/818 del Parlamento europeo e del Consiglio e che abroga il regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio».

¹⁰ Cfr. «Un nuovo patto sulla migrazione e l'asilo» (COM(2020) 609 final), il cui § 2.6 poneva l'accento sulla necessità di implementare una nuova banca dati sulla migrazione e l'asilo al fine di garantire «una gestione adeguata delle informazioni necessarie».

¹¹ L'elenco dei dati ospitati da Eurodac è ripetuto per tutte le categorie di soggetti interessate dal reg. 2024/1358/UE.

¹² Mentre in precedenza venivano registrati solo i richiedenti asilo e i cittadini di Paesi terzi coinvolti in un attraversamento irregolare delle frontiere, la nuova disciplina abbraccia anche i dati dei cittadini di Paesi terzi che soggiornano irregolarmente, delle persone reinsediate, delle persone sbarcate a seguito di operazioni di ricerca e soccorso, nonché dei beneficiari di protezione temporanea. Inoltre, rispetto al passato, il limite di età al di sopra del quale è obbligatorio rilevare i dati è stato abbassato da 14 a 6 anni (art. 23 § 1 reg. 2024/1358/UE). Si domandano «se l'aumento delle categorie registrate, dei dati raccolti e dei tempi di conservazione dei dati sia necessario e proporzionato rispetto agli obiettivi perseguiti dal legislatore europeo, tenuto conto del fatto che la banca dati è nata con il solo scopo di individuare gli Stati competenti all'esame della domanda di asilo», E. CELORIA-V. FERRARIS, *Eurodac: dalla gestione delle domande di protezione internazionale al controllo della mobilità*, in *Quaderni AISDUE - Rivista quadrimestrale*, 2024, Fascicolo speciale n. 4, p. 22.

¹³ Cfr. *infra*, § 3.

¹⁴ Cfr., sul punto, l'«Agenda europea sulla migrazione» (COM(2015) 240 final), p. 15, a cui rinvia il considerando n. 18 del reg. 2024/1358/UE.

controllo delle migrazioni e controlli di “sicurezza”¹⁵ sottesa alla disciplina di Eurodac, della criminalità.

La nuova normativa, pertanto, comporterà per gli Stati membri il dovere di raccogliere gli elementi richiesti e di trasmetterli entro 72 ore a Eurodac tramite un'apposita infrastruttura di comunicazione affinché siano immagazzinati all'interno del sistema centrale¹⁶. Dopodiché, sarà possibile interrogare il *database* per effettuare, pure a fini di contrasto, confronti con i dati ivi conservati.

La notevole rilevanza di siffatte operazioni di comparazione per le indagini penali¹⁷, così come l'ampiezza della banca dati e le caratteristiche delle informazioni incamerate, suggeriscono di analizzare le procedure che, in base al regolamento del 2024, permettono di consultare Eurodac, onde verificarne l'idoneità a proteggere i diritti fondamentali¹⁸, troppo spesso messi «tra parentesi» nell'ambito del «*crimmigration process*»¹⁹.

2. Le (blande) procedure di accesso a Eurodac per finalità di contrasto

Il reg. 2024/1358/UE dedica un apposito Capo – l'XI – alla «procedura per il confronto e la trasmissione dei dati a fini di contrasto». Composto di quattro articoli, il Capo in questione si preoccupa, in particolare, di regolare modalità e condizioni di accesso a Eurodac da parte, per un verso, delle autorità designate dagli Stati membri, intendendosi per tali, «le autorità degli Stati membri responsabili della prevenzione, dell'accertamento o dell'indagine di reati di terrorismo o di altri reati gravi», di cui ciascun Paese deve conservare un elenco²⁰, così come anche «delle

¹⁵ In questi termini, E. CELORIA-V. FERRARIS, *Eurodac*, cit., p. 10.

¹⁶ L'architettura di Eurodac è descritta nel dettaglio dall'art. 3 reg. 2024/1358/UE.

¹⁷ ... ricavabile dallo stesso regolamento del 2024, là dove, al considerando n. 34, specifica che «[l]a possibilità di confrontare un'impronta digitale latente con i dati relativi alle impronte digitali conservati nell'Eurodac, nei casi in cui si può ragionevolmente ritenere che l'autore o la vittima di un reato potrebbero rientrare in una delle categorie contemplate dal presente regolamento, rappresenterebbe, per le autorità designate degli Stati membri, uno strumento utilissimo per la prevenzione, l'accertamento o l'indagine di reati di terrorismo o di altri reati gravi, quando per esempio l'unica prova disponibile sul luogo del reato consiste nelle impronte digitali latenti».

¹⁸ Del resto, come sottolineato da D. NEGRI, *Introduzione*, in ID. (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Aracne, Roma, 2007, p. VIII, «la circolazione incontrollata delle informazioni raccolte nelle banche dati» impone di apprestare «adeguati limiti giuridici».

¹⁹ In questi termini, G.L. GATTA, *La pena nell'era della 'crimmigration': tra Europa e Stati Uniti*, in *Riv. it. dir. proc. pen.*, 2018, p. 716.

²⁰ Cfr. art. 5 reg. 2024/1358/UE.

unità operative in seno alle sue autorità designate che sono autorizzate a chiedere il confronto con i dati Eurodac»²¹; e, per l'altro, di Europol, che individua a tale scopo una o più delle sue unità operative²².

Lungi dal poter agire in autonomia, ai sensi dell'art. 32, le autorità designate devono rivolgersi a un'autorità di verifica con una richiesta motivata in cui dare conto della sussistenza dei requisiti necessari per il confronto, in presenza dei quali quest'ultima inoltra la domanda al punto di accesso – nazionale o di Europol a seconda dei casi –, che la trasmette a Eurodac. In ipotesi di eccezionale urgenza, «ove sia necessario per prevenire un pericolo imminente associato a reati di terrorismo o ad altri reati gravi», l'organo di verifica può immediatamente rivolgersi al punto d'accesso salvo dover effettuare il *check ex post*, con l'obbligo di cancellazione di tutti i dati qualora esso dia esito negativo.

Dal punto di vista soggettivo, l'autorità di verifica statale è definita in modo analogo a quella designata²³, tanto che esse possono addirittura «far parte della stessa organizzazione se il diritto nazionale lo consente»²⁴. La scelta è confermata anche per l'Agenzia europea, che designa al suo interno «un'unità specializzata unica composta di funzionari di Europol debitamente autorizzati ad agire in qualità di autorità di verifica»²⁵.

In buona sostanza, dunque, siamo in presenza di uno strumento²⁶ nell'ambito del quale il vaglio circa il rispetto dei parametri a cui è subordinato il confronto dei dati ben può essere rimesso a un organo di polizia, anche appartenente alla stessa struttura di quello richiedente. È quanto, ad esempio, ha scelto di fare proprio l'Italia, che – seppure ovviamente nella vigenza del reg. 2013/603/UE – ha individuato l'autorità di verifica nel Servizio per la cooperazione internazionale di polizia²⁷, ossia un'«artico-

²¹ Cfr. art. 5 § 3 reg. 2024/1358/UE.

²² Cfr. art. 7 § 1 reg. 2024/1358/UE.

²³ In base all'art. 6 § 1 reg. 2024/1358/UE, è «l'autorità dello Stato membro responsabile della prevenzione, dell'accertamento o dell'indagine di reati di terrorismo o di altri reati gravi».

²⁴ Cfr. art. 6 § 2 reg. 2024/1358/UE.

²⁵ Cfr. art. 7 § 2 reg. 2024/1358/UE.

²⁶ Qualificato, non a caso, di «cooperazione di polizia» dal considerando n. 34 del regolamento.

²⁷ Lo si apprende dall'«[e]lenco delle autorità competenti notificate alla Commissione ai sensi dell'articolo 43 del regolamento (UE) n. 603/2013 che istituisce l'Eurodac per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il regolamento (UE) n. 1077/2011 che

lazione” della Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza del Ministero dell’Interno²⁸.

Certo, l’art. 6 § 2 reg. 2024/1358/UE si preoccupa di precisare che l’ente di verifica «agisce indipendentemente nello svolgimento dei propri compiti», dovendo altresì essere «distint[o] dalle unità operative di cui all’articolo 5, paragrafo 3», da cui «non riceve istruzioni [...] in merito al risultato della verifica»²⁹.

Nondimeno, la quantità e la delicatezza degli elementi raccolti – come le impronte digitali –, protetti come sono dall’art. 10 direttiva 2016/680/UE sul trattamento di categorie particolari di dati personali³⁰, oltre al carattere automatizzato del confronto delle informazioni biometriche prescritto dall’art. 27 del regolamento medesimo, inducono a dubitare circa l’adeguatezza delle garanzie da apprestare affinché, ai sensi del suddetto art. 10, il trattamento possa essere autorizzato.

Sebbene la direttiva non chiarisca la portata di dette garanzie³¹, rimettere un controllo così denso di contenuti, sotto il profilo della proporzionalità della limitazione del diritto alla vita privata³², all’autorità di polizia, ammettendo peraltro l’appartenenza di richiedente e “supervisore” a una medesima organizzazione, rischia concretamente di renderlo ineffettivo³³, oltretutto di attentare alla tenuta delle condizioni a cui l’accesso a Eurodac è subordinato³⁴.

istituisce un’agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia» (2021/C 45/01).

²⁸ Si tratta di una delle molte conferme del «ruolo dominante acquisito dalla polizia nell’attuale scenario di reazione al fenomeno terroristico, a tutto discapito delle figure del pubblico ministero e del giudice» (così, D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Arch. pen. (web)*, 2016, n. 1, p. 1).

²⁹ Indicazioni simili sono previste, con riferimento a Europol, dall’art. 7 § 2, secondo cui l’autorità di verifica «è pienamente indipendente dall’autorità designata di Europol nello svolgimento dei suoi compiti a norma del presente regolamento», «è distinta dall’autorità designata di Europol e non riceve istruzioni dalla stessa in merito al risultato della verifica».

³⁰ Così, i dati dattiloscopici rientrano nella nozione di dati biometrici di cui all’art. 3 n. 13 della direttiva, le cui definizioni, ai sensi dell’art. 2 § 4, si applicano al reg. 2024/1358/UE «nella misura in cui i dati personali sono trattati dalle competenti autorità degli Stati membri a fini di contrasto».

³¹ A sottolinearlo è P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, in S. SICA-V. D’ANTONIO-G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Cedam, Milano, 2016, p. 341, il quale nota come, al considerando n. 37 della direttiva, vi sia un elenco esemplificativo di presidi di tutela, tra cui figura l’approntamento di «norme più severe riguardo all’accesso ai dati da parte del personale dell’autorità competente».

³² Cfr., al riguardo, i considerando da 32 a 35 reg. 2024/1358/UE.

³³ Sul punto, si vedano le considerazioni critiche di N. VAVOULA, *The Recast Eurodac Regulation*, cit., p. 266.

³⁴ Cfr. il considerando n. 35 reg. 2024/1358/UE, dove si allude al «rigore» delle con-

Tra i presupposti fissati dall'art. 33 § 1 reg. 2024/1358/UE per le autorità designate statuali³⁵ ne figurano alcuni – comunque da verificare – che potremmo definire “formali”, come la preventiva consultazione delle banche dati nazionali e dei sistemi d'identificazione dattiloscopica di tutti gli altri Stati membri ai sensi della decisione 2008/615/GAI (lett. a). Altri, invece, sottendono una valutazione molto diffusa, concernente la necessità del confronto con i dati Eurodac per accertare reati di terrorismo o altri reati gravi, da intendersi come esistenza di «un interesse prevalente di sicurezza pubblica tale da rendere l'interrogazione [...] proporzionata all'obiettivo perseguito» (lett. b); l'indispensabilità del raffronto nell'ambito di «un caso specifico riguardante persone specifiche» (lett. c); e la sussistenza di «fondati motivi per ritenere che il confronto contribuisca in misura sostanziale» all'indagine «di reati di terrorismo o di altri reati gravi in questione» (lett. d).

Tali parametri – secondo l'interpretazione offerta dalla Corte di giustizia³⁶ del lemma «strettamente necessario» di cui all'art. 10 direttiva 2016/680/UE³⁷, lemma che «definisce condizioni rafforzate di liceità del trattamento dei dati sensibili» – «dovrebbero essere valutat[i] in modo particolarmente rigoroso»³⁸.

Un rigore che difficilmente potrebbe essere garantito dall'autorità di polizia. Infatti, quando si tratta di ingerenze gravi nei diritti fondamentali – gravità dipendente, tra l'altro, «dalla natura e dalla sensibilità dei dati»³⁹ considerati e, dunque, sussistente in presenza delle categorie particolari di informazioni regolate dall'art. 10⁴⁰ – i giudici lussemburghesi, a tutela dei

dizioni d'accesso, giustificato dalla circostanza che la banca dati «registra i dati biometrici e alfanumerici di persone che non si presume abbiano commesso un reato di terrorismo o un altro reato grave».

³⁵ L'art. 34 § 1 è invece la disposizione di riferimento per Europol.

³⁶ Le cui affermazioni, a opinione di R. BENASSAI, *La disciplina dei dati biometrici nella gestione dei flussi migratori: nuove prospettive alla luce del “Patto sulla migrazione e l'asilo”*, in DPCE online, 2025, n. 2 - Sezione Monografica “Decisori ed emergenze”, p. 794, dovrebbero essere tenute in debita considerazione nell'applicazione, in generale, del patto sulla migrazione e l'asilo e, in particolare, del regolamento Eurodac.

³⁷ Lemma che ritroviamo, per quanto riguarda Europol, al § 2 dell'art. 30 reg. 2016/794/UE, introdotto con reg. 2022/991/UE, secondo cui il trattamento dei dati biometrici è autorizzato «solo se strettamente proporzionato e necessario».

³⁸ Corte giust., sent. 26 gennaio 2023, C-205/21, V.S., §§ 117-118. Per un'ampia analisi delle argomentazioni sviluppate dalla Corte di giustizia nella sentenza in esame a proposito del parametro della stretta necessità del trattamento dei dati di cui all'art. 10, v. G. BORGIA, *Biometría, evolución tecnológica y proceso penal: urge un cambio de ritmo en nombre de la proporcionalidad*, in G. BORGIA-S. PEREIRA PUIGVERT, *Retos de la prueba en el proceso actual*, Aranzadi, Madrid, 2024, p. 427 s.

³⁹ Così, Corte giust., sent. 4 ottobre 2024, C-548/21, CG, § 90.

⁴⁰ In proposito è utile rammentare la pronuncia con cui la Corte di giustizia, nel de-

diritti riconosciuti dagli artt. 7 e 8 Carta dir. fond. UE, richiedono l'intervento di figure di ben altra caratura: il giudice o, quantomeno, un organo amministrativo indipendente⁴¹, il quale ultimo «deve godere di uno status che [gli] permetta di agire nell'assolvimento dei propri compiti in modo obiettivo e imparziale, e deve a tale scopo essere al riparo da qualsiasi influenza esterna»⁴². Tutte caratteristiche della cui esistenza, nel caso di specie, è lecito dubitare.

Evidentemente consci della posta in gioco, alcuni ordinamenti hanno deciso di individuare l'autorità di verifica non già in un organo di polizia, ma nella procura⁴³, per quanto anch'essa – com'è noto – non offra adeguate garanzie sotto il profilo dell'indipendenza⁴⁴.

cidere una questione pregiudiziale concernente la conservazione da parte dell'autorità di polizia di dati biometrici e genetici riguardanti soggetti condannati in via definitiva sino alla loro morte, ha messo in risalto la «particolare sensibilità» di quei dati là dove trattati per finalità di *law enforcement* (Corte giust., sent. 30 gennaio 2024, C-118/22, NG, § 47). In buona sostanza – come osservato da C. CONTI, *Il corpo dell'imputato come prova: il diritto di non collaborare tra prospettive sovraordinate, suggestioni storiche e polifunzionalità dei dati*, in *Dir. pen. proc.*, 2024, p. 121 – «il principio di proporzionalità si scarica non tanto sul modo in cui l'acquisizione si effettua [...], bensì sull'individuazione del tipo di dato acquisibile».

⁴¹ Corte giust., sent. 21 dicembre 2016, C-203/15 e C-698/15, Tele2 Sverige AB, § 120. In controtendenza rispetto a una siffatta impostazione sembrerebbe tuttavia porsi una decisione concernente il soggetto chiamato a effettuare il vaglio di stretta necessità di cui all'art. 10 direttiva 2016/680/UE allorché la normativa nazionale preveda la raccolta sistematica dei dati biometrici e genetici di persone accusate di certe tipologie di reati, vaglio che è stato rimesso all'«autorità competente» a raccogliergli come definita dall'art. 3 n. 7 della direttiva, ricomprendente anche l'autorità di polizia (Corte giust., sent. 28 novembre 2024, C-80/23, V.S.). Più di recente, v. Corte giust., sent. 20 novembre 2025, C-57/23, JH, § 104, secondo cui «la circostanza che la necessità di mantenere la conservazione di dati biometrici e genetici è valutata dai servizi di polizia sulla base di norme interne [...] non è, di per sé, contraria all'articolo 8, paragrafo 2, della direttiva 2016/680, purché tali norme interne impongano a dette autorità di garantire il rispetto della condizione relativa all'esistenza di una stretta necessità di conservare tali dati e il margine di discrezionalità di tali autorità sia sufficientemente inquadrato dal diritto nazionale». Per una critica a questo genere di conclusioni, v. L. PARODI, *Dati personali e procedimento penale nel sistema UE: un mosaico di garanzie in costante evoluzione*, in *Proc. pen. giust.*, 2025, p. 1295, ad avviso del quale esse destano perplessità nella misura in cui «l'ingerenza conseguente all'acquisizione dei dati biometrici e genetici è certamente qualificabile come grave, anche solo per la particolare sensibilità di tali informazioni».

⁴² Corte giust., sent. 2 marzo 2021, C-746/18, H.K., § 53.

⁴³ Il riferimento è all'Estonia, che ha incaricato il *Prosecutor's Office* con sede a Tallin, e alla Lituania, che ha a sua volta indicato una serie di uffici della procura. Al riguardo, cfr. l'«[e]lenco delle autorità competenti notificate alla Commissione ai sensi dell'articolo 43 del regolamento (UE) n. 603/2013», cit.

⁴⁴ ... come si ricava da Corte giust., sent. 2 marzo 2021, C-746/18, H.K., cit., § 55. Per un commento alla pronuncia, v. E. ANDOLINA, *La sentenza della Corte di giustizia UE nel caso H.K. c. Prokuratuur: un punto di non ritorno nella lunga querelle in materia di data retention?*, in *Proc. pen. giust.*, 2021, p. 1211, la quale sottolinea che «solo l'intervento preventivo di un organo [...] come quello giurisdizionale, può garantire un sindacato effettivo e rigo-

Di certo, lasciare alla discrezionalità dei vari Stati – dai quali è comunque lecito attendersi un cambio di passo specie alla luce delle modifiche apportate a Eurodac⁴⁵ – la selezione del soggetto a cui demandare valutazioni tanto delicate sotto il profilo del rispetto dei diritti fondamentali non può che destare perplessità in termini di uguaglianza.

3. Riconoscimento facciale tramite Eurodac

Come anticipato, una delle principali innovazioni apportate dal reg. 2024/1358/UE è rappresentata dall'inclusione, tra i dati conservati all'interno di Eurodac, delle immagini del volto.

Benché configurato come *extrema ratio*, in quanto il ricorso alle impronte digitali deve essergli preferito là dove possibile⁴⁶, gli artt. 28 e 32 § 3 dell'atto⁴⁷ aprono le porte al confronto automatico, anche per finalità di contrasto, tra le immagini conservate nel *database* e quelle inviate al bisogno dagli Stati membri⁴⁸.

In particolare, l'idea è quella di consentire una siffatta operazione attraverso la tecnologia di riconoscimento facciale, dal momento che, entro il 12 giugno 2027, l'agenzia eu-LISA – a cui è affidata la gestione di Eurodac – dovrà condurre uno studio circa la fattibilità tecnica dell'inserimento all'interno della banca dati di un apposito *software*⁴⁹, testandone

roso sul provvedimento invasivo della sfera privata, idoneo a circoscrivere l'accesso ai dati conservati entro il limite di razionalità imposto dal canone di proporzione e, dunque, ad arginare il pericolo di abusi e/o interferenze arbitrarie».

⁴⁵ In questa direzione, è aspicabile un aggiornamento dell'elenco delle autorità competenti.

⁴⁶ Cfr. il considerando n. 19 del regolamento, nonché l'art. 28 § 1, ai sensi del quale occorre eseguire la comparazione delle impronte digitali fintantoché «lo stato dei polpastrelli non consent[a] un rilevamento delle impronte digitali di qualità tale da assicurare un confronto appropriato» o esse «non s[iano] disponibili».

⁴⁷ Nel dettaglio, l'art. 32 § 3, rimandando all'art. 28 § 1, abilita il «confronto tra un'immagine del volto e altri dati relativi ad immagini del volto conservati nell'Eurodac a fini di contrasto», purché «tali dati siano disponibili al momento della presentazione della richiesta motivata in formato elettronico da parte delle autorità designate degli Stati membri o dell'autorità designata di Europol».

⁴⁸ Le insidie poste da questa come da altre disposizioni che, a livello eurounitario, permettono di sfruttare tale tecnologia su una particolare categoria di soggetti sono evidenti: «FRT employed en masse will further deepen and systematise the cloak of suspicion with which third-country nationals and generally people on the move are viewed» (in questi termini, N. VAVOULA, *Towards Artificially Intelligent EU Migration, Asylum and Border Management? The AI Act, Interoperable Large-Scale IT Systems and the Role of Agencies: AI for EU Migration, Asylum and Border Control*, in M. BERGSTRÖM-V. MITSILEGAS (a cura di), *EU Law in the Digital Age*, Hart, Oxford, 2025, p. 326).

⁴⁹ Cfr. art. 57 § 4 reg. 2024/1358/UE. In base all'art. 63 § 5, «[i]l software di ricono-

«attendibilità» e «accuratezza»⁵⁰. Ne deriva la necessità di analizzare la procedura che vede coinvolte le autorità designata e di verifica alla luce del reg. 2024/1689/UE sull'intelligenza artificiale, delle cui indicazioni, del resto, si deve obbligatoriamente tenere conto «nella valutazione di ciascun sistema IT su larga scala istituito dagli atti giuridici elencati nell'allegato X»⁵¹, dove figura proprio il reg. 2024/1358/UE⁵².

Ricorrendo alla classificazione del reg. IA, occorre innanzitutto domandarsi quale tipologia di riconoscimento facciale sia realizzabile tramite Eurodac. Poiché quello scandito dal reg. 2024/1358/UE è un *iter* a cui partecipano diversi soggetti e composto da diverse fasi, la prima interna all'ordinamento richiedente o a Europol (iniziativa dell'autorità designata, vaglio dell'autorità di verifica e inoltro dell'istanza al punto di accesso), la seconda volta a ottenere un *output* dalla banca dati (trasmissione del dato a Eurodac, che ne deve confermare la ricezione⁵³, comparazione con quelli «archiviati» – la quale deve essere effettuata, di norma, entro 24 ore, secondo l'ordine di arrivo delle richieste⁵⁴ – e comunicazione di un riscontro al richiedente⁵⁵), sembra possibile affermare come il tutto avvenga con un'apprezzabile soluzione di continuità. In altre parole, il rilevamento del dato biometrico, il confronto e l'identificazione hanno luogo «con un ritardo significativo», tale da escludere l'operatività della disciplina dettata per i sistemi in tempo reale e da rendere, dunque, applicabile quella relativa ai congegni *a posteriori*⁵⁶.

La normativa di riferimento, condensata nell'art. 26 § 10 reg. IA, permette di procedere, «nel quadro di un'indagine per la ricerca mirata di una persona sospettata o condannata per aver commesso un reato», a identificazione biometrica «statica» a patto che il *deployer* ottenga un'autorizza-

scimento facciale è introdotto nell'Eurodac entro un anno dalla conclusione dello studio» da parte di eu-LISA».

⁵⁰ A proposito della scarsa qualità dei risultati forniti dalle tecnologie di riconoscimento facciale, v. G. BORGIA-M. ZONARO, *L'errore nel riconoscimento facciale automatizzato*, in W. NOCERINO (a cura di), *L'errore tecnico e la prova penale*, Pacini Editore, Pisa, 2025, p. 175 ss.

⁵¹ Così recita l'art. 111 § 1, secondo periodo, reg. IA.

⁵² V., in particolare, il n. 3 dell'allegato X.

⁵³ Cfr. art. 37 reg. 2024/1358/UE.

⁵⁴ Cfr. art. 38 § 2 reg. 2024/1358/UE.

⁵⁵ Cfr. art. 38 §§ 4 e 5 reg. 2024/1358/UE.

⁵⁶ Cfr. il considerando n. 17 e l'art. 3 nn. 42 e 43 reg. IA. Per una critica a una siffatta distinzione, v. L. CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, in *Riv. it. dir. proc. pen.*, 2024, p. 246, il quale si chiede se «il ritardo temporale» su cui si fonda «sia sufficiente a giustificare [una] tale differenza di regolamentazione», considerato che «anche i programmi di identificazione «a posteriori» rappresentano una grave minaccia per la *privacy* e potrebbero facilmente trasformarsi in strumenti potenti per effettuare una sorveglianza di massa».

zione, «*ex ante* o senza indebito ritardo ed entro 48 ore», da parte dell'autorità giudiziaria o amministrativa, la cui decisione è «soggetta a controllo giurisdizionale».

Suscettibile di assicurare «l'indipendenza e l'imparzialità del provvedimento adottato»⁵⁷, l'apparato di garanzie in questione va però incontro a una rilevante eccezione allorché il sistema di riconoscimento sia «utilizzato per l'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato»⁵⁸.

Si tratta di un'ipotesi derogatoria che interessa molto da vicino i confronti effettuati attraverso il *database* Eurodac, pensato com'è per agevolare il riconoscimento di categorie di persone rispetto alle quali si riscontrano sovente lacune informative. Lo confermano gli stessi requisiti in presenza dei quali è possibile interrogare la banca dati, su tutti quello legato alla sussistenza di «fondati motivi per ritenere che il confronto contribuisca in misura sostanziale alla prevenzione, all'accertamento o all'indagine di reati di terrorismo o di altri reati gravi», integrato – specifica l'art. 33 § 1 lett. *d* – quando vi sia «il sospetto fondato che l'autore presunto o effettivo oppure la vittima di un reato di terrorismo o di un altro reato grave rientri in una delle categorie contemplate dal [...] regolamento»; nonché il presupposto a cui è subordinata la comparazione delle immagini facciali, vale a dire, come accennato, la sostanziale impossibilità di addivenire all'identificazione sfruttando le impronte digitali.

Alla luce di ciò, sembra probabile che, anche rispetto alla forma più “estrema” di riconoscimento – il riconoscimento facciale tramite *software* basato sull'intelligenza artificiale – l'autorità di polizia potrà accedere a Eurodac senza particolari vincoli e controlli⁵⁹, con inevitabili riverberi negativi sui diritti dei soggetti le cui immagini saranno sottoposte a confronto.

⁵⁷ Testualmente E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna*, Giappichelli, Torino, 2025, p. 192.

⁵⁸ Su tale clausola e, in particolare, sulla difficoltà di «cogliere l'effettiva consistenza dei “fatti oggettivi e verificabili”», con il pericolo «che nella stragrande maggioranza dei casi in cui si voglia procedere all'identificazione iniziale della persona sospettata di aver commesso un reato si possa» agire in libertà, v. F. DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale tra possibilità di impiego e limiti ordinamentali*, Cedam, Milano, 2025, p. 181.

⁵⁹ ... vincoli e controlli la cui importanza è stata messa in risalto dalla Corte di Strasburgo proprio nel contesto delle tecnologie di riconoscimento facciale, dove «*it is essential to have [...] strong safeguards against the risk of abuse and arbitrariness*» (Corte e.d.u., 4 luglio 2023, Glukhin c. Russia, § 82).

4. Eurodac in un contesto di interoperabilità: rischi di elusione delle (già inadeguate) garanzie

Come anticipato, la riforma del 2024 è parte integrante del patto sulla migrazione e l'asilo, in cui si sottolineava la necessità di rendere Eurodac «pienamente interoperabile con le banche dati per la gestione delle frontiere nell'ambito di un sistema globale e integrato di gestione della migrazione e delle frontiere»⁶⁰. In questa direzione, l'art. 3 reg. 2024/1358/UE, nel disegnare l'architettura del *database*, ha incluso tra i suoi componenti l'archivio comune di dati di identità (CIR⁶¹) istituito dal reg. 2019/818/UE⁶², ossia uno degli atti emanati «per rendere interoperabili i sistemi d'informazione per la gestione della sicurezza, delle frontiere e della migrazione al fine di aumentare l'efficacia e l'efficienza della gestione dei dati nell'UE» e «proteggere meglio le frontiere esterne e rafforzare la sicurezza interna»⁶³.

Nell'ambito di un'infrastruttura volta a collegare tra loro diversi sistemi di gestione dell'identità⁶⁴, i quali possono così essere interrogati una sola volta senza necessità di svolgere ricerche “parallele”, il CIR ha il compito di conservare le informazioni provenienti da tutte le banche dati

⁶⁰ Cfr. «Un nuovo patto sulla migrazione e l'asilo», cit., § 2.6. V., inoltre, il § 4.2. Sul tema dell'interoperabilità nel contesto della cooperazione informativa dell'Unione europea, v. diffusamente B. GALGANI, *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale “virtuoso”*, Cedam, Milano, 2022, p. 16 ss.

⁶¹ Acronimo di *common identity repository*.

⁶² ... «che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816». A esso si affianca il reg. 2019/817/UE «che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'Unione europea nel settore delle frontiere e dei visti».

⁶³ Così, la «[s]ettima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza» (COM(2017) 261 final), p. 2.

⁶⁴ In particolare, oltre a Eurodac, l'infrastruttura connette lo *Schengen Information System* (SIS), in cui sono raccolti dati rilevanti nel settore delle frontiere e della sicurezza dell'area Schengen; il *Visa Information System* (VIS), che opera nel settore dei visti; l'*Entry/Exit System* (EES), entrato in vigore il 12 ottobre 2025 e contenente dati relativi a tutti i cittadini di Paesi terzi che attraversano le frontiere Schengen per soggiorni di breve durata; l'*European Travel Information and Authorisation System* (ETIAS), ancora in fase di sviluppo, dedicato alle informazioni di cittadini di Stati terzi esenti da visto che attraversano le frontiere Schengen; e l'*European Criminal Records Information System – Third Country Nationals* (ECRIS-TCN), la cui implementazione è ancora in corso, che riunisce i dati correlati ai cittadini di Paesi terzi che hanno riportato condanne in sede penale nel territorio dell'Unione. Per una panoramica relativa a tali sistemi, cfr. eu-LISA, *Identity Management Technologies in the Context of International Travel and Migration. Eu-LISA Research and Technology Monitoring Report September 2025*, § 2.2.

connesse – Eurodac compresa – e di creare fascicoli individuali che permettono l'identificazione⁶⁵. E tra le finalità per le quali è possibile avvalersi del CIR figurano, ai sensi dell'art. 22 reg. 2019/818/UE, proprio quelle «di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi».

Dal momento che non è possibile conoscere «in anticipo quale sistema di informazione dell'UE contenga dati sulle persone su cui devono compiere indagini», onde evitare «ritardi e inefficienze»⁶⁶, quest'ultima disposizione abilita le autorità designate ed Europol a consultare direttamente il CIR «per sapere se nell'Eurodac sono presenti dati su una determinata persona». E sebbene l'*output* di questa interrogazione non possa disvelare i dati del soggetto attenzionato, consistendo nella indicazione dell'esistenza di informazioni in quel *repository*, al quale dovrà poi essere domandato l'accesso secondo le modalità previste dall'apposito regolamento⁶⁷, appare evidente come questa iniziale risposta abbia di per sé una notevole rilevanza⁶⁸. Al punto che il reg. 2019/818/UE si affretta a puntualizzare come «la risposta dal CIR non dovrebbe essere interpretata o utilizzata come motivo o ragione per trarre conclusioni o adottare misure riguardo a una persona, ma dovrebbe essere utilizzata soltanto per presentare una richiesta di accesso ai sistemi di informazione sottostanti dell'UE soggetta alle condizioni e alle procedure stabilite dai rispettivi strumenti giuridici che regolamentano tale accesso»⁶⁹.

Pertanto, senza passare dal (pur insufficiente) vaglio dell'autorità di

⁶⁵ Cfr. art. 17 reg. 2019/818/UE. Il CIR è soltanto una delle componenti dell'architettura interoperabile. In particolare, accanto a essa figurano l'*European Search Portal* (ESP), cioè l'unica “finestra” di accesso ai vari sistemi; il *Multiple-Identity Detector* (MID), capace di creare e conservare fascicoli di conferma dell'identità, nonché di stabilire collegamenti tra identità; e lo *shared Biometric Matching Service* (sBMS), in cui sono conservati modelli biometrici creati a partire dai dati archiviati nel CIR, al fine di consentire la comparazione. Sul funzionamento di una tale complessa architettura, si veda G. DI PAOLO, *Verso una nuova architettura di gestione dei dati contenuti nei sistemi di informazione dell'Unione*, in *Cass. pen.*, 2019, p. 3382 ss.

⁶⁶ Cfr. il considerando n. 32 del reg. 2019/818/UE.

⁶⁷ Cfr. art. 22 § 3 reg. 2019/818/UE.

⁶⁸ Si vedano, al riguardo, le preoccupazioni di F. TASSINARI, *Data Protection and Interoperability in EU External Relations. Guaranteeing Global Data Transfers in the Area of Freedom, Security and Justice*, Brill, Leiden, 2025, p. 397, la quale sottolinea per l'appunto come «*the first query already allows users to understand if and where the data is stored, notwithstanding if full-access is granted or not*»; e di C.B. CASAGRAN, *Interconnecting Migration and Policing Databases in the EU*, in *Human Rights Law Review*, 2021, n. 21, p. 452, la quale rileva che «*the simple bit-flag already reveals some personal information about the individual ex ante, without having to access to their full data*».

⁶⁹ Così il considerando n. 33 del reg. 2019/818/UE.

verifica, quella designata può in autonomia rivolgersi al CIR con l'opportunità di ottenere un primo, importante riscontro.

Non solo. In base all'art. 33 § 2 reg. 2024/1358/UE, il responso positivo del CIR esonera l'autorità designata a osservare una delle condizioni cui è subordinato, in una logica di proporzionalità, l'accesso a Eurodac, ovvero sia – come visto – l'interrogazione preventiva delle banche dati nazionali e dei sistemi degli altri Stati membri, la quale rischia perciò di divenire superflua⁷⁰.

In definitiva, la potenziale elusione delle regole di accesso a Eurodac che può originare dall'interoperabilità dei sistemi di gestione di identità eurounitari suggerisce di delineare un'unica procedura di consultazione per finalità di contrasto. Una procedura che tenga conto della connessione tra i *databases* esistenti e, soprattutto, della particolare sensibilità dei dati contenuti al loro interno, la quale richiede controlli più adeguati in termini di indipendenza e terzietà del soggetto deputato a compierli⁷¹.

⁷⁰ In proposito, v. T. QUINTEL, *Data protection, Migration and Border Control. The GDPR, the Law Enforcement Directive and Beyond*, Hart, Oxford, 2022, p. 52, la quale rileva che «*searches in the CIR would allegedly render the current cascade regime of checking national systems prior to searching the AFSJ databases superfluous*».

⁷¹ Osserva criticamente come «*the interoperability components may allow police and border authorities to access certain personal data items without the supervision of a judicial body*», in aperto contrasto con la giurisprudenza della Corte di giustizia in materia di proporzionalità e stretta necessità del trattamento di dati così delicati, C.B. CASAGRAN, *Interconnecting Migration and Policing Databases*, cit., p. 452.

LA CONSULTAZIONE E LO SCAMBIO AUTOMATIZZATI DI DATI BIOMETRICI (... E NON SOLO) NEL “QUADRO PRÜM II”

NICOLÒ DI PACO

SOMMARIO: 1. Introduzione. – 2. Il procedimento per la consultazione e lo scambio dei dati biometrici: regole e criticità. – 3. *Segue*. La circolazione delle immagini facciali. – 4. L'accesso ai *police records* fra problemi di traduzione e questioni di ordine generale. – 5. Alcune riflessioni conclusive.

1. *Introduzione*

È indubbio che, per quanto meno battuta rispetto ad altri meccanismi di cooperazione in materia penale, quella c.d. “informativa”, ossia «lo scambio rapido ed efficace di dati rilevanti ai fini» di contrasto alla delittuosità, «abbia rappresentato e rappresenti tuttora»¹ il presupposto fondamentale per una completa realizzazione del mutuo riconoscimento².

Non deve allora sorprendere che, di recente, il legislatore unionale sia

¹ Così B. GALGANI, *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale “virtuoso”*, Wolters Kluwer-Cedam, Milano, 2022, p. 18 ss., a cui si rimanda per una ricostruzione più approfondita del percorso di progressiva affermazione della cooperazione informativa.

² Dopo tutto, la possibilità di accedere alle informazioni in possesso degli altri Stati membri rafforza quella «vicendevole fiducia interstatuale» che fonda «la *ratio essendi*» propria del principio della *confiance mutuelle*: le parole sono di B. GALGANI, *Assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea*, in A. MARANDOLA (a cura di), *Cooperazione giudiziaria penale*, Giuffrè, Milano, 2018, p. 446. In generale, in tema di mutuo riconoscimento e fiducia reciproca, si vedano, *ex multis*, E. GIORGI, *Il principio del mutuo riconoscimento nell'ordinamento dell'Unione europea*, Firenze University Press, Firenze, 2020, p. 22 ss.; S. MONTALDO, *I limiti della cooperazione in materia penale nell'Unione europea*, Editoriale scientifica, Napoli, 2015, p. 353 ss.; H. SATZGER, *Is mutual recognition a viable general path for cooperation?*, in NJECL, 2019, vol. 10, p. 44 ss.; J.R. SPENCER, *Il principio del mutuo riconoscimento*, in R.E. KOSTORIS (a cura di), *Manuale di procedura penale europea*, 4^a ed., Giappichelli, Torino, 2019, p. 345 ss.; W. VAN BALLEGOIJ, *The Nature of Mutual Recognition in European Law*, Larcier Interstetia, Antwerpen, 2015.

tornato – tramite il regolamento (UE) 2024/982 del 13 marzo 2024 «sulla consultazione e lo scambio automatizzato di dati per la cooperazione di polizia» (da qui in avanti, “regolamento Prüm” o “reg. Prüm”) – a interessarsi della tematica della circolazione di informazioni penalmente rilevanti per scopi di *law enforcement*.

L'intento è quello di «migliorare, semplificare e facilitare lo scambio»³, tra le autorità competenti degli Stati membri, di profili DNA, dati dattiloscopici, determinati dati di immatricolazione dei veicoli, immagini del volto ed estratti del casellario giudiziale – «nel pieno rispetto dei diritti fondamentali delle persone fisiche, tra cui il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali»⁴ – sì da «prevenire e combattere la criminalità e altre minacce alla sicurezza pubblica, compresi la criminalità organizzata e il terrorismo»⁵.

Prima di calarsi *in medias res*, appare opportuno ripercorrere, seppur per brevissimi tratti, le ragioni che hanno condotto all'adozione del regolamento.

Nel maggio del 2005, con l'obiettivo di implementare e rafforzare la lotta al terrorismo, alla criminalità transfrontaliera e all'immigrazione illegale, sette Paesi membri – segnatamente Belgio, Germania, Spagna, Francia, Lussemburgo, Paesi Bassi e Austria – firmavano il Trattato di Prüm, «inaugurando forme innovative»⁶ di circolazione di profili DNA, impronte digitali e dati di immatricolazione dei veicoli e con l'auspicio di «trasferire le disposizioni» ivi contenute «nel quadro giuridico dell'Unione europea allo scopo di giungere ad un miglioramento dello scambio di informazione»⁷ al suo interno.

Come noto, l'«europeizzazione»⁸ del trattato è dovuta alle decisioni quadro 2008/615/GAI e 2008/616/GAI (cc.dd. “decisioni Prüm”) ⁹: la

³ Cfr. considerando n. 2.

⁴ Il rispetto dei diritti fondamentali è imposto dall'art. 2 del regolamento Prüm. Il considerando n. 2 specifica, altresì, che lo scambio dei dati deve essere effettuato «nel pieno rispetto [...] delle norme sulla protezione dei dati».

⁵ Ciò è quanto si legge nel considerando n. 1.

⁶ Così, P. TROISI, *La circolazione di informazioni per le investigazioni penali nello spazio giuridico europeo*, Cedam, Padova, 2012, p. 17.

⁷ Cfr. le premesse al Trattato.

⁸ L'espressione è di 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*, 2021, f. 8, p. 202.

⁹ Altrettanto noto è che l'adesione dell'Italia al trattato di Prüm è avvenuta con la legge 30 giugno 2009, n. 85 che ha, altresì, istituito la banca dati nazionale del DNA. Per un'analisi puntuale della normativa di ratifica si rinvia ai contributi contenuti in L. MARAFIOTI-L. LUPÁRIA (a cura di), *Banca dati del DNA e accertamento penale. Commento alla legge di*

prima¹⁰, incorporando «la sostanza delle disposizioni del trattato [...] nel quadro giuridico»¹¹ unionale, ne aveva riprodotto il contenuto, rendendolo vincolante per tutti gli Stati membri; la seconda, invece, conteneva le previsioni di attuazione della decisione quadro 2008/615/GAI.

Il procedimento di trasmissione dei dati genetici e dattiloscopici – informato al principio di disponibilità¹² – era bifasico¹³: dapprima, il punto di contatto designato dal singolo Stato membro, su istanza della autorità di *law enforcement* domestiche, accedeva ai dati di indice contenuti negli schedari nazionali, al fine di verificare, tramite una procedura automatizzata di “*hit/no hit*”, la presenza di una corrispondenza. Solo in caso di risposta positiva, l'autorità interessata poteva richiedere la trasmissione delle informazioni personali del soggetto i cui dati di indice avessero restituito una corrispondenza, secondo quanto previsto dal diritto dello Stato richiesto e dalle normative sovranazionali in materia di assistenza giudiziaria¹⁴.

A dispetto di un sempre più crescente numero dei dati immagazzina-

ratifica del Trattato di Prüm, istitutiva del database generico nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85), Giuffrè, Milano, 2010 e in A. SCARCELLA (a cura di), Prelievo del DNA e banca dati nazionale, Cedam, Milano, 2009.

¹⁰ ... «sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera».

¹¹ Considerando n. 1 della decisione quadro 2008/615/GAI.

¹² Sul punto, occorre ricordare come, secondo quanto si legge al punto 2.1 (dedicato al «[m]iglioramento dello scambio di informazioni») della parte III del Programma dell'Aia sul «rafforzamento della libertà, della sicurezza e della giustizia nell'Unione europea» (adottato dal Consiglio europeo del 4 e 5 novembre 2004), in forza del principio di disponibilità, «in tutta l'Unione, un ufficiale di un servizio di contrasto di uno Stato membro che ha bisogno di informazioni nell'esercizio delle sue funzioni può ottenere tali informazioni da un altro Stato membro, e [...] il servizio di contrasto nell'altro Stato membro che dispone di tali informazioni è tenuto a trasmettergliene per i fini dichiarati, tenendo conto dei requisiti relativi alle indagini in corso nel suddetto Stato». Insomma, si deve garantire, nella visione del Consiglio, che «le autorità di contrasto di un» Paese dell'Unione, «ogniqualvolta [necessitino], nell'espletamento delle proprie funzioni, di assumere informazioni aliunde, [siano] messe nelle condizioni di ottenerle dal Paese “detentore” straniero, all'uopo obbligato a fornirle per le finalità richieste»: così, B. GALGANI, *Forme e garanzie nel prisma dell'innovazione tecnologica*, cit., p. 19. In tema, v. anche S. CIAMPI, *Principio di disponibilità e protezione dei dati personali nel “terzo pilastro” dell'Unione europea*, in F. PERONI-M. GIALUZ (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Eut, Trieste, 2009, p. 34 ss.

¹³ Il «doppio binario» si motivava in ragione dell'esigenza di assicurare adeguata tutela del diritto alla riservatezza: così, P. TROISI, *La circolazione di informazioni*, cit., p. 20.

¹⁴ In proposito, A. MARANDOLA, *Information sharing nella prospettiva del Trattato di Prüm e della decisione di recepimento nel quadro giuridico dell'Unione*, in F. PERONI-M. GIALUZ (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, cit., p. 172 metteva in luce come il trattato «lascia[sse] impregiudicata la centrale questione se in capo alla Parte richiesta [dovesse] configurarsi un obbligo, un onere o una mera facoltà di trasmettere l'informazione all'autorità richiedente».

ti nelle banche dati nazionali e disponibili alla consultazione¹⁵, la circolazione transnazionale per scopi securitari dei profili DNA, delle impronte digitali e delle informazioni inerenti all'immatricolazione dei veicoli ha stentato ad affermarsi in maniera stabile ed efficace¹⁶. Le cause di tali difficoltà sono da rinvenirsi, soprattutto, nelle «discrepanze fra gli Stati membri in termini di implementazione, quadri normativi nazionali e livello di automazione dei processi»¹⁷. A ciò si è andato ad assommare un certo immobilismo di alcuni Paesi¹⁸ che, a distanza di (molti) anni dalle decisioni quadro, non si erano ancora dotati di banche dati funzionali allo scambio automatizzato né di normative *ad hoc* volte a regolamentare il trasferimento delle informazioni¹⁹. Senza considerare che ogni Stato ha dovuto (o doveva) stabilire e mantenere – per ogni tipologia di dati – tante connessioni bilaterali quanti erano gli altri Stati membri, con evidenti complicazioni nella gestione della rete²⁰.

¹⁵ Secondo lo studio elaborato da Deloitte su richiesta della Commissione europea, al 2019 il *network Prüm* contava più di 9,2 milioni di profili DNA disponibili a una comparazione attraverso le banche dati nazionali, con più di 2,2 milioni di ricerche DNA fatte in quell'anno. Si registravano, inoltre, quattrocentomila ricerche di impronte digitali, con diecimila corrispondenze verificate, e più di sedici milioni di consultazioni di dati sulle immatricolazioni dei veicoli: cfr. DELOITTE, *Study on the Feasibility of Improving Information Exchange under the Prüm Decisions*, 2020, in *op.europa.eu*, p. 7.

¹⁶ Per una disamina più approfondita sui fattori che hanno reso difficoltosa la completa affermazione del quadro Prüm risultante dalle decisioni quadro del 2008 si rinvia, *ex multis*, a N. VAVOULA, *Police Information Exchange. The future developments regarding Prüm and the API Directive*, in *europarl.europa.eu*, 2020, p. 18-25.

¹⁷ *Ivi*, p. 18 (trad. it. nostra). Sul punto, v. altresì L. SCAFFARDI, *Next generation Prüm e le scelte strategiche della UE*, cit., p. 207 ss., la quale, con specifico riferimento al caso dei profili genetici, evidenzia come gli Stati membri avessero optato per «soluzioni normative differenti [anzitutto] in materia di raccolta e conservazione di DNA e dunque di disciplina delle banche dati». A differire era pertanto, in prima battuta, la stessa «determinazione dei criteri e delle condizioni di inserimento dei dati genetici (campioni o profili) negli schedari nazionali». Sul tema, si veda anche EAD, *Forensic genetics: the evolving challenge of DNA cross-border exchange*, in *BioLaw Journal*, 2021, f. 1 – *Special Issue*, p. 333 ss.

¹⁸ ... fra i quali figurava anche l'Italia. In proposito, vale la pena ricordare come nel luglio 2021 la Commissione abbia deferito l'Italia alla Corte di giustizia dell'Unione europea per il mancato rispetto degli obblighi derivanti dalle decisioni Prüm; la procedura risulta, però, conclusa in data 26 gennaio 2023.

¹⁹ Secondo N. VAVOULA, *Police Information Exchange*, cit., p. 19, tali discrasie erano dovute, probabilmente, anche a difficoltà finanziarie e tecniche. In senso analogo, v. F. AIME-N. ARGIRÒ-M. MERLI-L. LONETTI-F. SCARPONE, *Forensic Database (Part II). How Does EU Law Address Issue Concerning Acces for Forensic Purposes to Research Biobanks?*, in V. COLCELLI-R. CIPITANI-C. BROCHHAUSEN-DELIUS-R. ARNOLD (a cura di), *GDPR Requirements for Biobanking Activities Across Europe*, Springer, Cham, 2023, p. 207.

²⁰ Non solo. Come evidenziato da EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, in *edri.org*, 7 settembre 2022, p. 3, il quadro Prüm originario non pareva rispondente ai principi fissati dal Trattato di Lisbona e dalla

Da qui, anche nell'ottica di rimediare a quelle storture che hanno impedito la piena realizzazione del quadro Prüm originario, nel licenziare il regolamento, il legislatore eurounitario²¹ ha optato per un «approccio ibrido tra una soluzione decentrata e una centralizzata»²², tramite l'implementazione di due sistemi a livello centrale, il *router*²³ e l'Indice europeo dei casellari giudiziali (EPRIS)²⁴. Tali sistemi, ai quali dovranno essere collegate le singole banche dati nazionali²⁵, «fung[ono] da punto di con-

direttiva (UE) 2016/680 («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»), essendo entrato in vigore prima della loro adozione; pertanto «a modernisation of the 2008 Prüm decision [was] much needed». Sul tema della protezione dei dati personali nell'ambito dello scambio dei dati per come delineato dal Trattato di Prüm e dalle decisioni quadro del 2008, v. R. BELLANOVA, *The "Prüm Process": The way Forward for EU Police Cooperation and Data Exchange?*, in E. GUILD-F. GEYER, *Security versus Justice? Police and Judicial Cooperation in the European Union*, Routledge, Londra, 2008, p. 211-215.

²¹ ... seguendo i rilievi e i suggerimenti contenuti nello studio di fattibilità prima richiamato; v. DELOITTE, *Study on the Feasibility of Improving Information Exchange under the Prüm Decisions*, cit., p. 25: tale documento, infatti, raccomandava la creazione di un *router* centrale «as a brokering mechanism», di modo che gli Stati membri dovessero configurare e mantenere una singola connessione. Per una panoramica sulle tappe che hanno portato all'adozione del regolamento, v. N. AMELUNG-H. MACHADO, *Dancing in the Dark: Policy Transformations Through Obfuscating Contestations in the Case of Prüm II*, in *European Papers*, 2025, p. 783-791.

²² Questi i termini utilizzati nella relazione introduttiva alla proposta di regolamento presentata dalla Commissione europea l'8 dicembre 2021; cfr. *Proposta di regolamento del Parlamento europeo e del Consiglio sullo scambio automatizzato di dati per la cooperazione di polizia ("Prüm II")*, che modifica le decisioni 2008/615/GAI e 2008/616/GAI del Consiglio e i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818 del Parlamento europeo e del Consiglio, in *eur-lex.europa.eu*, p. 5. Sul punto, v. E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna*, Giappichelli, Torino, 2025, p. 198 e V. FAGGIANI, *Digitalisation of criminal justice in the EU through eu-LISA cooperation with Eurojust and Europol: between extraordinary potential and persistent opacity*, in *UNIO – EU Law Journal*, 2024, vol. 10, f. 2, p. 53.

²³ A tal riguardo, N. VAVOULA, *Police Information Exchange*, cit., p. 10 spiega come la scelta sia ricaduta su un *router* centrale piuttosto che su un «centralised information system, which has been rejected due to legal constraints on storing such data outside the national territory»; varie le ragioni alla base di simile scelta: «processing personal data at EU level will be avoided; accurate statistical data at central level will be produced and technical difficulties posed by bilateral connections will be eliminated».

²⁴ Stando all'art. 75 reg. Prüm, per l'entrata in funzione del sistema di consultazione e scambio automatizzati di dati per come consegnato dal regolamento si dovrà attendere l'indicazione da parte della Commissione, con appositi atti di esecuzione, delle date a decorrere delle quali gli Stati membri ed Europol dovranno iniziare a utilizzare il *router* ed EPRIS. In particolare, perché il meccanismo di circolazione abbia avvio sarà necessario che gli Stati membri adottino le misure necessarie a rendere disponibili i dati, nonché l'esito positivo del collaudo generale dei due sistemi centrali. Sulle componenti strutturali del *router* e di EPRIS e su loro funzionamento si tornerà più approfonditamente in seguito; cfr. § 2 e 4.

²⁵ ... non prima, però, che sia stata effettuata una valutazione di impatto sulla pro-

nessione tra tutti gli Stati membri», semplificando, così, «l'architettura del quadro Prüm»²⁶.

Il regolamento mantiene la fisionomia a doppio binario che già caratterizzava il primo quadro Prüm: la consultazione automatizzata restituisce dati biometrici indicizzati²⁷ o estratti del casellario giudiziale pseudonimizzati²⁸ – sì da non permettere, nella logica del legislatore, l'identificazione del soggetto a cui appartengono²⁹ – e, solo in caso di conferma della corrispondenza, lo Stato che ha avviato la procedura potrà ottenere informazioni più complete.

Rispetto al sistema precedente si amplia, però, il catalogo dei dati suscettibili di trasferimento da uno Stato membro all'altro³⁰ o a Europol, includendo – oltre ai profili DNA, alle impronte digitali e alle informazioni sull'immatricolazione dei veicoli³¹ – anche le immagini facciali e gli estratti del casellario giudiziale.

tezione dei dati personali, secondo la disciplina in materia fissata dalla direttiva (UE) 2016/680 (v. art. 50 § 4 reg. Prüm).

²⁶ V. considerando n. 24 del regolamento Prüm.

²⁷ In particolare, l'indicizzazione si concretizza nell'assegnazione al profilo di DNA, all'impronta digitale o all'immagine facciale di un «numero di riferimento» che permetta allo Stato membro che detiene quel dato o a Europol, in caso di corrispondenza, di «estrarre ulteriori dati e altre informazioni dalle loro banche dati» così da trasmetterle allo Stato richiesto o all'Agenzia dell'Unione europea per la cooperazione, là dove sia essa ad aver avviato l'interrogazione (cfr. artt. 4, 7, 12 e 21 reg. Prüm).

²⁸ Cfr. art. 25 § 2 reg. Prüm.

²⁹ V. *infra*, § 3 e 4.

³⁰ Per completezza, occorre segnalare come, ai sensi dell'art. 29 reg. Prüm, sia lasciata agli Stati la possibilità di decidere se usufruire del quadro Prüm II per effettuare consultazione automatizzate – oltre per le finalità di cui si dirà – anche per cercare persone scomparse nell'ambito di indagini penali o per motivi umanitari, oppure per identificare resti umani. La previsione si pone nel solco dei rilievi effettuati da Deloitte nello studio di fattibilità prima richiamato («[t]he scope of Prüm should be extended to allow the use of Prüm in non-criminal searches for missing persons and unidentified human bodies»). Qui si sottolineava, infatti, come alcuni ordinamenti prevedessero il ricorso al quadro Prüm per cercare persone scomparse o per identificare soggetti deceduti, mentre altri non contemplassero espressamente una simile eventualità: ecco allora che «[s]ince the possible cases that fall under the crime definition is not uniform across Member States, enlarging the material scope of the Prüm framework would benefit States whose legal framework does not cover using Prüm in certain situations». Così, DELOITTE, *Study on the Feasibility of Improving Information Exchange under the Prüm Decisions*, cit., p. 23. In proposito, come opportunamente evidenziato da EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., p. 17, mentre la creazione di un meccanismo di consultazione e lo scambio dei dati ai fini di indagine, prevenzione e accertamento trova la propria base legale negli art. 87 § 2 lett. a e 88 § 2 Tratt. f. UE, l'inclusione della ricerca delle persone scomparse e dell'identificazione di persone decedute fra le ragioni a giustificazione della comparazione non sembra trovare un analogo, solido, appiglio normativo. Sul tema, v. anche N. VAVOULA, *Police Information Exchange*, cit., p. 26 s.

³¹ La consultazione e lo scambio di dati di immatricolazione non sarà oggetto di spe-

2. Il procedimento per la consultazione e lo scambio dei dati biometrici: regole e criticità

Prendiamo, dunque, le mosse dalla circolazione dei profili DNA, delle impronte digitali e delle immagini del volto, informata, nel solco del modello originario, al principio di disponibilità: secondo quanto previsto dagli artt. 5, 10 e 19 reg. Prüm, infatti, gli Stati membri sono tenuti a garantire che siano accessibili agli altri Paesi dell'Unione europea e a Europol i dati biometrici ottenuti o provenienti dalle banche dati nazionali del DNA e da quelle specificatamente istituite per la prevenzione, l'indagine e l'accertamento dei reati.

Quanto all'avvio dell'*iter*, deve registrarsi una sostanziale differenza fra la procedura inerente i dati dattiloscopici o le *facial images*, da un lato, e quella avente a oggetto i profili DNA, dall'altro.

Se, nel primo caso, si lascia agli Stati membri (e a Europol) la scelta di presentare, tramite i propri punti di contatto³², la domanda di consultazione³³ per scopi di «prevenzione, indagine e accertamento dei reati»³⁴, con riferimento ai profili DNA, l'art. 6 stabilisce due ipotesi di interrogazione «diretta» od «obbligata» degli appositi archivi nazionali, entrambe «[a]i fini delle indagini penali».

Così, il primo paragrafo sancisce – con formulazione particolarmente verbosa – che, all'atto della prima connessione al *router*³⁵ tramite i pro-

cifica attenzione nel presente contributo. Al riguardo, merita comunque segnalare che in forza dell'art. 16 reg. Prüm, gli Stati membri devono consentire ai punti di contatto degli altri Paesi dell'Unione e a Europol di condurre – ai fini della prevenzione, dell'indagine e dell'accertamento di reati – consultazioni automatizzate «nel contesto di un singolo caso» (cfr. *infra*, § 2) dei «dati relativi ai proprietari o ai possessori dei veicoli di veicoli» oppure dei «dati relativi ai veicoli». In particolare, le ricerche aventi a oggetto le informazioni sui proprietari o i possessori possono essere effettuate – specifica il paragrafo 2 – «solo in caso di persone indagate o condannate».

³² Ai sensi dell'art. 30, ogni Stato membro deve designare uno o più punti di contatto per le procedure di consultazione e scambio dei dati.

³³ ... comprendente soltanto «il codice dello Stato membro richiedente», «la data, l'ora e il numero di riferimento della domanda» e «i numeri di riferimento dei dati dattiloscopici» oppure «le immagini del volto e i dati di riferimento», secondo quanto previsto, rispettivamente, dall'art. 15 § 1 e dall'art. 24 § 1.

³⁴ Gli artt. 10 e 20 reg. Prüm, invero, si limitano a stabilire il dovere degli Stati membri di autorizzare, per le finalità suddette, i punti di contatto nazionali degli altri Paesi dell'Unione ed Europol ad accedere ai dati dattiloscopici e a quelli sulle immagini del volto perché possano procedere «a consultazioni automatizzate tramite [...] raffronto». In proposito, merita sicuramente anticiparsi – anche se sul punto torneremo nel prosieguo (v. *infra*, § 3) – come il trasferimento delle immagini del volto sia ammesso solo allorquando i reati da prevenire o accertare siano puniti, secondo la legge dello Stato richiedente, con una pena massima superiore a un anno.

³⁵ In forza dell'art. 66 reg. Prüm, il «responsabile dello sviluppo del *router* e degli eventuali adeguamenti tecnici necessari per il funzionamento» è eu-LISA, ossia l'Agenzia

pri punti di contatto nazionali, i Paesi dell'Unione debbano effettuare «una consultazione automatizzata confrontando tutti i profili DNA conservati nelle loro banche dati del DNA con tutti i profili DNA conservati nelle banche dati del DNA di tutti gli altri Stati membri e con i dati Europol». L'obiettivo è quello «di evitare lacune nell'identificazione di corrispondenze tra i profili DNA conservati nella banca dati di uno Stato membro e i profili DNA conservati nelle banche dati di tutti gli altri Stati membri e i dati Europol»³⁶. Questa preliminare ricerca «dovrebbe essere effettuata bilateralmente e non necessariamente nello stesso momento con le banche dati di tutti gli Stati membri e i dati Europol»³⁷. Inoltre, come precisa sempre l'art. 6 § 1, «[l]e modalità per l'effettuazione di tali consultazioni, comprese la tempistica e la quantità per ciascun gruppo di profili, dovrebbero essere concordate» dai due Stati (o dallo Stato e da Europol) coinvolti «in conformità delle norme e delle procedure stabilite nel [...] regolamento».

Similmente, il paragrafo 2 impone agli Stati di verificare, ogni qual volta inseriscano nuovi profili DNA nei propri archivi, se vi siano *matches* «con tutti i profili DNA conservati nelle banche dati del DNA di tutti gli altri Stati membri e con i dati Europol»³⁸.

Ebbene, non poche perplessità possono essere sollevate in merito alla proporzionalità e, prima ancora, alla legalità delle operazioni di *scanner* diffuse e generalizzate previste dalla disposizione. Procediamo per gradi.

Posto che i profili DNA – come gli altri dati biometrici presi in con-

dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia, istituita dal regolamento (UE) 2018/1726. Quanto alle componenti, il *router* è costituito da «un'infrastruttura centrale», da «un canale di comunicazione sicuro tra» tale infrastruttura, «le autorità competenti autorizzate a usare il *router* [...] ed Europol» e, infine, da «un un'infrastruttura di comunicazione sicura tra l'infrastruttura centrale e il portale di ricerca europeo istituito dall'articolo 6 del regolamento (UE) 2019/817 e dall'articolo 6 del regolamento (UE) 2019/818 ai fini dell'articolo 39» (art. 35 reg. Prüm). In particolare, tale ultima componente è volta a permettere l'interoperabilità fra il *router* e l'archivio comune di dati di identità istituito dai regolamenti unionali da ultimo richiamati, i quali, come noto, hanno scolpito una «complessa modellistica di “interazione reciproca” tra sistemi informativi» «nel settore delle frontiere e dei visti, e in quello della cooperazione di polizia e giudiziaria, asilo e migrazione»: così, B. GALGANI, *Forme e garanzie nel prisma dell'innovazione tecnologica*, cit., p. 36. Per un approfondimento sul tema dell'interoperabilità nella cornice tracciata dal regolamento Prüm, si rinvia a N. AMELUNG-H. MACHADO, *Dancing in the Dark*, cit., p. 791-796; v. altresì, EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation (“Prüm II”)*, in *edps.europa.eu*, 2 marzo 2022, p. 15 s.

³⁶ Come specificato al considerando n. 13.

³⁷ *Ibidem*.

³⁸ In riguardo, il considerando 14 precisa che tali nuove consultazioni «dovrebbero essere effettuate regolarmente».

siderazione dal regolamento – costituiscono *ex se* dati personali che contengono informazioni uniche relative a un determinato individuo³⁹, va da sè che ogni attività tesa a “sottrarre” ai soggetti titolari il controllo esclusivo su tali dati determina un’ingerenza sul diritto alla *data protection*⁴⁰, ingerenza che, pertanto, dovrebbe trovare fondamento nella legge, essere necessaria e rispondere a obiettivi di interesse generale⁴¹.

Ora, se è fuori di dubbio che le finalità di indagine dei reati potrebbero giustificare limitazioni ai diritti fondamentali della persona, altrettanto incontrovertibile è che, in un’ottica di proporzionalità dell’intervento, il ricorso a strumenti significativamente impattanti – quale si candida a essere il raffronto *omnibus* dei profili DNA – dovrebbe essere ammesso solo in presenza di condotte delittuose di particolare gravità⁴².

³⁹ Il riferimento corre all’art. 3 dir. 2016/680 che definisce come dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile» e «considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo *online* o a uno o più elementi caratteristici dell’identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica». Inoltre, sempre a detta della disposizione richiamata, i dati biometrici sono «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».

⁴⁰ ... oltre che sul diritto al rispetto della vita privata *ex art. 8 § 1 Conv. e.d.u.*; v., *ex multis*, Corte e.d.u., Gr. Ch., 4 dicembre 2008, S. e Marper c. Regno Unito, spec. § 77.

⁴¹ Secondo le indicazioni generali di cui all’art. 52 della Carta dei diritti fondamentali dell’Unione europea.

⁴² Come sottolineato dall’EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation (“Prüm II”)*, cit., p. 9. In proposito, meritano sicuramente di essere richiamate le parole utilizzate dall’avvocato generale Giovanni Pitruzzella nelle conclusioni presentate nella causa C-205/2021, secondo il quale la raccolta e il trattamento dei dati biometrici e genetici, dal momento che «costituiscono una grave ingerenza nel diritto alla protezione dei dati personali», devono essere «autorizzati solo se strettamente necessari per il perseguimento di obiettivi legati alle forme gravi di criminalità»: cfr. *Conclusioni* dell’avvocato generale in Corte giust., sent. 26 gennaio 2023, C-205/21, V.S. Aderendo all’impostazione dell’avvocato generale, la Corte di Lussemburgo ha stabilito che l’art. 10 della direttiva 2016/680 «osta a una normativa nazionale che prevede la raccolta sistematica di dati biometrici e genetici di qualsiasi persona formalmente accusata di un reato doloso perseguibile d’ufficio, ai fini della loro registrazione», senza che l’autorità competente debba, all’uopo, «verificare e [...] dimostrare, da un lato, che tale raccolta è strettamente necessaria per il raggiungimento dei concreti obiettivi perseguiti e, dall’altro, che tali obiettivi non possono essere raggiunti mediante misure che costituiscono un’ingerenza meno grave nei diritti e nelle libertà della persona interessata». In proposito, v. anche Corte giust., sent. 28 novembre 2024, C-80/23 V.S.

Del resto, quella appena ricordata pare essere l’impostazione generale oramai adottata dalla Corte di giustizia dell’Unione europea: v., a titolo di esempio, Corte giust., sent. 6 ottobre 2020, C-511/18, C-512/18 e C-520/18, *La Quadrature du Net* e a. che, in tema di

Nondimeno, e a dispetto delle intenzioni generali fissate nel preambolo⁴³, l'art. 6, nel richiamare assai generiche finalità di "indagine penale", non circoscrive l'ambito applicativo delle procedure di consultazione doverosa a forme gravi di criminalità⁴⁴. In tal senso si possono, allora, legittimamente avanzare delle riserve sul fatto che l'art. 6 del regolamento Prüm soddisfi il canone di proporzionalità.

Non solo: l'"obbligatorietà" delle consultazioni non permette nemmeno di verificare la possibilità di ricorrere a strumenti meno afflittivi e, di riflesso, di valutare la stretta necessità del mezzo⁴⁵, che pare presunta *ex lege*.

Ancora (e in via preliminare), l'estrema latitudine del presupposto legittimante l'avvio della procedura fa ragionevolmente dubitare circa la conformità della disposizione al principio di legalità: segnatamente, «[a] rilevare» sul punto è il requisito «[del]la *qualità* della base giuridica che, al fine di assicurare la certezza del diritto, deve presentare i caratteri della accessibilità e della prevedibilità»⁴⁶.

conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione, ha stabilito che «per quanto riguarda l'obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati, conformemente al principio di proporzionalità, solo la lotta alle forme gravi di criminalità e la prevenzione di minacce gravi alla sicurezza pubblica sono idonee a giustificare ingerenze gravi nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta». Per un commento alla sentenza e, in generale, per una disamina sulle problematiche connesse alla conservazione dei dati relativi al traffico, si rinvia, *ex multis*, a M. LANDOLFI, *Data retention tra continui sviluppi e nodi irrisolti*, in *Leg. pen. (web)*, 7 novembre 2024.

⁴³ La mente corre al già richiamato considerando n. 1, secondo cui l'obiettivo – perseguito dall'Unione anche tramite il regolamento Prüm – di «offrire ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne [...] deve essere perseguito [...] attraverso misure appropriate per prevenire e combattere la criminalità e altre minacce alla sicurezza pubblica, compresi la criminalità organizzata e il terrorismo»: il riferimento alle forme più gravi di criminalità sembra, invero, richiedere una certa serietà delle condotte da accertare affinché si possa attivare il meccanismo di circolazione transfrontaliera dei dati.

⁴⁴ In proposito, v. F. SANVITALE, *Quello che il legislatore non dice in tema di prova genetica. Dalla banca dati nazionale del DNA al familial searching*, in *Leg. pen. (web)*, 18 aprile 2024, p. 5 e M. BOTTO, *Il DNA da "prova regina" a "testimone biologico"? I controversi effetti delle nuove frontiere dell'analisi genetico-forense sulla governance of crime*, *ivi*, 23 gennaio 2025, p. 9 s, nota 21.

⁴⁵ Come noto tale, valutazione rappresenta il secondo gradino dello scrutinio di proporzionalità. Più nello specifico, sul criterio di proporzionalità si vedano, su tutti, L. BELVINI, *Principio di proporzionalità e attività investigativa*, ESI, Napoli; M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont. – Riv. trim.*, 2014, f. 3-4, p. 144 ss.; D. Negri, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 2020, p. 3 ss.; F. NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *archiviodpc.dirittopenaleuoma.org*, 8 gennaio 2018; R. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, p. 1133 ss.

⁴⁶ Le parole – seppur usate in altro contesto – sono di G. BORGIA, *Profili sistematici*

In proposito, è da ricordare come la Corte europea dei diritti dell'uomo abbia ritenuto non integrato siffatto requisito a fronte di una previsione nazionale formulata in maniera talmente ampia (*«in connection with the administration of justice»*) da sembrar ammettere il trattamento dei dati biometrici (nel caso di specie, le immagini facciali) *«in connection with any judicial proceedings»*⁴⁷. Così, per quanto è di nostro interesse, la circostanza che il ricorso all'*iter* di confronto dei profili DNA sia ammesso nei soli procedimenti penali non sembra definire in maniera sufficientemente precisa l'ambito applicativo dello strumento⁴⁸: oltre a non fare riferimento a reati di particolare gravità, difatti, non si indicano nemmeno le specifiche finalità per cui la consultazione dovrebbe essere avviata, né le categorie di persone che possono essere soggette a siffatto trattamento di dati⁴⁹.

Perplessità non dissimili possono sollevarsi in merito alle ipotesi di consultazione delle impronte digitali o delle immagini del volto, le quali possono essere oggetto di raffronto «ai fini della prevenzione, dell'indagine e dell'accertamento di reati». Analogamente a quanto appena rilevato in relazione alla comparazione dei profili DNA, la grave ingerenza sui diritti fondamentali operata dal meccanismo in parola avrebbe dovuto suggerire, in un'ottica di proporzionalità, la fissazione di soglie di speciale gravità dei reati per i quali si sarebbe potuta avviare la ricerca transfrontaliera di corrispondenze.

Né vale a salvare la proporzionalità della misura il richiamo, nell'ipotesi delle *facial images*, ai reati punibili con una pena massima di un anno.

delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte euromunitario, in *Leg. pen. (web)*, 11 dicembre 2021, p. 19. Sul tema, si veda il documento della Corte e.d.u. *Guide on Article 8 of the European Convention on Human Rights*, aggiornato al 28 febbraio 2025, spec. p. 12 (il documento è reperibile al sito [ks.echr.coe.int](https://www.echr.coe.int/)).

⁴⁷ Corte e.d.u., 4 ottobre 2023, *Glukhin c. Russia*, § 83. Per un commento alla sentenza, si rinvia a G. GALLO, *Tecnologie di riconoscimento facciale e diritti fondamentali a rischio: il caso Glukhin c. Russia dinanzi alla Corte europea dei diritti dell'uomo*, in *MediaLaws*, 2023, f. 3, p. 189 ss.; F. PALMIOTTO-N. MENÉNDEZ GONZÁLEZ, *Facial recognition technology, democracy and human rights*, in *50 Computer Law & Security Review*, 2023, f. 3, p. 1 ss.; E. SACCHETTO, *Tecnologie di riconoscimento facciale*, cit., p. 127 ss.

⁴⁸ Del resto, di recente la Corte di giustizia dell'Unione europea – nel valutare la rispondenza al diritto unionale in tema di protezione dei dati personali di una normativa nazionale che consenta «indistintamente la raccolta di dati biometrici e genetici di tutte le persone sottoposte a un procedimento penale per un reato doloso o sospettate di aver commesso un tale reato – ha ribadito, richiamando un suo precedente approdo, come le «finalità del trattamento di [simili] dati [...] non possono essere designate in termini troppo generici, ma richiedono di essere definite in modo sufficientemente preciso e concreto da consentire di valutare il carattere “strettamente necessario” di detto trattamento»: così, Corte just., sent. 20 novembre 2025, C-57/23, *JH c. Policejní prezidium*, § 79.

⁴⁹ Come rilevato da EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation (“Prüm II”)*, cit., p. 9-10.

Da un lato, infatti, il limite “minimo” di pena appare talmente irrisorio da poter quasi essere considerato come non apposto, dal momento che fa rientrare sotto l’ombrello applicativo della disposizione anche delitti di (assai) modesto allarme sociale. Dall’altro, il *quantum* edittale non pare nemmeno in linea con le (già basse) soglie previste in altri provvedimenti unionali⁵⁰ in materia di prove penali⁵¹.

Sempre restando nel perimetro della proporzionalità, ulteriori dubbi emergono, in via generale, con riferimento alle previsioni secondo cui le consultazioni dei dati biometrici sono svolte «nel rispetto del diritto nazionale dello Stato richiedente» e «nel contesto di ciascun *singolo caso*»⁵², espressione, questa, con cui si indica «un singolo fascicolo relativo alla prevenzione, all’accertamento o all’indagine di un reato, alla ricerca di una persona scomparsa o all’identificazione di resti umani non identificati», giusta la definizione contenuta all’art. 4 n. 10 reg. Prüm.

Ne consegue che, in assenza di specifiche esigenze, si potrebbe svolgere la ricerca in maniera generalizzata e in relazione a qualsiasi individuo collegato a quel determinato “caso” e, quindi, non solo all’indagato o alla persona offesa, ma altresì a parenti o *partner* dell’uno o dell’altra, a persone informate sui fatti e, in generale, a persone nei confronti delle quali non sussiste un ragionevole sospetto né una condanna per un reato grave⁵³ e senza che questi ne siano al corrente, con evidenti ricadute oltretutto sulla presunzione di non colpevolezza, anche sull’autodeterminazione infor-

⁵⁰ Si intende far riferimento, in particolar modo, al regolamento (UE) 2023/1543 «relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l’esecuzione di pene detentive a seguito di procedimenti penali» (c.d. “regolamento *e-evidence*”). Segnatamente, l’art. 5 § 4 del regolamento *de quo* stabilisce che le competenti autorità possono emettere un ordine europeo di produzione per ottenere dati sul traffico o dati relativi al contenuto, oltretutto per una serie di reati specificatamente indicati, anche per i reati punibili con una pena detentiva della durata massima di almeno tre anni. Per un commento, v. G. BORGIA, *Un nuovo congegno per l’acquisizione della prova elettronica nell’Unione europea: il c.d. “regolamento e-evidence” è finalmente realtà*, in *Proc. pen. gius.*, 2023, p. 1272 ss.; V. FRANSSEN, *Cross-border gathering of electronic evidence in the EU: toward more direct cooperation under the e-Evidence regulation*, in V. MITSILEGAS-M. BERGSTRÖM-T. QUINTEL (a cura di), *Research Handbook on EU Criminal Law*, 2^a ed., Edward Elgar, Cheltenham, 2024, p. 184 ss.; F. SANVITALE, *Gli ordini europei di conservazione e produzione: un passo indietro per la tutela dei diritti fondamentali nelle indagini penali?*, in L. BERNARDINI-C. DE CARO (a cura di), *Sfide attuali e tendenza future del diritto processuale penale europeo*, Giapichelli, Torino, 2025, p. 161 ss.

⁵¹ Le ragioni del raffronto con atti normativi in materia di prove saranno chiare più avanti; cfr. *infra*, § 6.

⁵² Cfr. art. 6 § 4 con riferimento ai profili DNA, art. 11 § 1 in relazione alle impronte digitali e art. 20 § 1 per quanto attiene alle immagini del volto.

⁵³ EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., p. 22.

mativa, quale aspirazione del singolo – di ogni singolo – a «riaffermare la potestà [...] sui dati a lui riferibili»⁵⁴.

Con particolare riferimento a tale ultima prerogativa deve ricordarsi, come ben sottolineato in dottrina, che l'«analisi» e, nel nostro caso, la comparazione «automatizzata di dati presenta[no] una propria peculiare incisività sul diritto» *de quo* «che va [ben] oltre quella derivante dalle retrostanti operazioni di raccolta delle informazioni». Invero, l'impiego del *router* centrale e l'interrogazione simultanea di tutte le banche dati a esso collegate (v. *infra*) non determinano solo «una *ri-elaborazione* dei singoli dati acquisiti in precedenza» e «stoccati» negli archivi nazionali, «ma si sostanzia[no] anche e soprattutto nell'instaurazione di collegamenti tra di essi che [...] «*ri-generano*», così, nuove conoscenze inevitabilmente destinate a riverberare i propri effetti negativi sulla *Informationelles Selbstbestimmungsrecht*»⁵⁵. Una simile capacità intrusiva avrebbe dovuto suggerire al legislatore unionale di circoscrivere in maniera più dettagliata i presupposti per la circolazione fra Stati membri dei dati biometrici.

Tanto detto e venendo ai profili più propriamente operativi, lo Stato che intende avviare la consultazione presenta, tramite le proprie autorità competenti⁵⁶, una domanda di interrogazione al *router*, trasmettendo i dati biometrici.

Dall'art. 33 reg. Prüm si ricava come l'interrogazione debba essere giustificata. In particolare, le autorità competenti devono: specificare le finalità della consultazione («compreso un riferimento al caso specifico o all'indagine specifica e, ove applicabile, al reato»); precisare, in ipotesi, se questa riguarda un indagato, un condannato, una persona offesa oppure, ancora, un soggetto scomparso o resti umani non identificati; e, infine, indicare «l'eventualità che l'interrogazione intenda identificare una persona od ottenere maggiori dati su una persona nota» (§ 2). Le giustificazioni – che devono essere conservate dallo Stato membro o da Europol – servono a permettere uno scrutinio sulla proporzionalità e sulla necessità in concreto della consultazione⁵⁷, nonché «il monitoraggio ai fini della pro-

⁵⁴ Le parole sono di S. CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in D. NEGRI (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Aracne, Roma, 2007, p. 7.

⁵⁵ Così, anche per la citazione precedente, G. BORGIA, *Analisi automatizzate di dati per finalità di law enforcement e diritto all'autodeterminazione informativa: dalla Corte costituzionale federale tedesca utili indicazioni (anche) per il legislatore dell'Unione*, in G. GALGANI (a cura di), *Processi, rappresentazioni e piattaforme digitali*, Giappichelli, Torino, p. 236.

⁵⁶ Tali sono – giusta la previsione di cui all'art. 36 – «le autorità autorizzate ad avere accesso e a scambiare profili DNA, dati dattiloscopici e immagini del volto conformemente al presente regolamento».

⁵⁷ C. PALLANTE, *Le nuove sfide della cooperazione investigativa nello spazio europeo: l'ingresso dell'intelligenza artificiale nello scambio informativo*, in L. BERNARDINI-C. DE CARO (a cura di),

tezione dei dati, compresa la verifica dell'ammissibilità dell'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza e l'integrità degli stessi» (§ 3).

Una volta presentata, il sistema centrale invia la domanda di interrogazione, in maniera automatizzata, agli archivi nazionali di tutti gli Stati membri o di quelli espressamente indicati dallo Stato richiedente e al *database* di Europol. Eventuali corrispondenze sono segnalate automaticamente al *router*, che classifica le risposte confrontando i dati biometrici utilizzati per l'interrogazione e quelli forniti nelle risposte⁵⁸ da parte dello Stato membro o degli Stati membri richiesti o di Europol e inoltra allo Stato richiedente l'elenco dei dati biometrici per i quali è stata appurata una corrispondenza e le relative classifiche (art. 37 reg. Prüm).

Ricevuta la notifica del *match* e i dati con cui è stato riscontrato, il punto di contatto nazionale può decidere di confermarlo. Qualora si orienti in tal senso, deve informare lo Stato membro o gli Stati membri richiesti ossia quelli nelle cui banche dati si trovano i profili DNA, le impronte digitali o le immagini facciali che hanno restituito una corrispondenza. Il punto di contatto nazionale deve, inoltre, assicurare che almeno un membro del personale qualificato conduca un esame manuale dell'elenco per asseverare tale corrispondenza con i dati di riferimento ricevuti dallo Stato membro richiesto (artt. 6 § 6, 11 § 2 e 20 § 2 reg. Prüm).

Viene, così, previsto il «necessario intervento umano, evidenziato dalla normativa come correttivo agli eventuali errori della “*machina*”»⁵⁹. Sennonché – è stato fatto notare – nel disegnare in tali termini il procedimento di consultazione e riscontro, il regolamento introduce, in realtà, ipotesi di trattamento completamente automatizzato di dati⁶⁰. Ci spieghiamo meglio.

Sfide attuali e tendenze future del diritto processuale penale europeo, cit., p. 269 ritiene la giustificazione dell'interrogazione un «passaggio [...] essenziale per comprendere la proporzionalità e la necessità dell'utilizzo del sistema per fini investigativi e preventivi, assicurando una protezione dei dati da accessi non autorizzati e sproporzionati».

⁵⁸ Ai sensi degli artt. 9 § 2, 15 § 2 e 24 § 2, le risposte devono contenere: «l'indicazione della presenza di una o più corrispondenze, o della mancanza di corrispondenze»; «la data, l'ora e il numero di riferimento della domanda»; «la data, l'ora e il numero di riferimento della risposta»; «i codici dello Stato membro richiedente e dello Stato membro richiesto»; i numeri di riferimento dei profili DNA, dei dati dattiloscopici o delle immagini facciali «dello Stato membro richiedente e dello Stato membro richiesto»; i profili DNA, i dati dattiloscopici o le immagini facciali «per i quali è stata riscontrata una corrispondenza».

⁵⁹ C. PALLANTE, *Le nuove sfide della cooperazione investigativa nello spazio europeo*, cit., p. 270.

⁶⁰ V. EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., p. 20.

Come visto, là dove il *router* riceva una segnalazione da parte di una o più banche dati, si procede al rilascio allo Stato richiedente del profilo biometrico (secondo la procedura “*hit/no hit*”) e del corrispettivo numero di riferimento, onde permettere al relativo punto di contatto e al personale qualificato la verifica del riscontro. Tuttavia, ciò significa, a ben vedere, che il trasferimento oltre confine del profilo DNA, dell'impronta digitale o dell'immagine facciale – che, come abbiamo già avuto modo di ricordare, costituiscono dati personali⁶¹, per di più “sensibili”⁶² – si svolge in maniera automatica, in ragione della corrispondenza comunicata dal *router* e prima ancora di una conferma umana della stessa⁶³. Il tutto senza rispettare le condizioni fissate dall'art. 11 dir. 2016/680 a legittimazione di un processo deliberativo completamente automatizzato⁶⁴: a mancare sono, in particolare, quelle specifiche «misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi» del *data subject* che il paragrafo 2 della disposizione impone in caso di decisione basata unicamente sul trattamento automatizzato delle categorie particolari di dati di cui all'art. 10 della stessa direttiva.

Ma vi è di più. Il sistema centrale, come visto, invia allo Stato richiedente una classifica dei dati biometrici per i quali è stata riscontrata una correlazione; in altre parole, restituisce una lista di potenziali *matches*, elencati secondo una scala di maggiore “attinenza”: la corrispondenza, insomma, è tutto fuorché assicurata. Ne discende un alto rischio di errori e di

⁶¹ Dal momento che riguardano persone identificate o identificabili, giusta la definizione offerta dall'art. 3 direttiva 2016/680; in proposito, v. anche Corte e.d.u., Gr. Ch., 4 dicembre 2008, cit., § 68.

⁶² ... ossia appartenenti alle categorie particolari di dati ex art. 10 direttiva 2016/680 e che, come tali, meriterebbero, per contro, «una specifica protezione», poiché «il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali» (cfr. considerando n. 37 dir. 2016/680).

⁶³ V. EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., p. 20. Ciò vale tanto più se si pensa che, secondo una recente sentenza della Corte di giustizia, si è al cospetto di un processo deliberativo completamente automatizzato ai sensi dell'art. 22 GDPR, anche là dove il risultato del calcolo meccanizzato influenzi in maniera decisiva la decisione presa dall'operatore umano (il riferimento corre a Corte giust., sent. 7 dicembre 2023, C-634/21, OQ c. Land Hessen).

⁶⁴ Per un'analisi della disposizione si rinvia a B. GALGANI, *Giudizio penale, habeas data e garanzie fondamentali*, in *Arch. pen. (web)*, 2019, f. 1, pp. 20-31. Per un quadro più generale sulla direttiva, v. G. BORGIA, *Il trattamento di dati personali a fini di prevenzione, di indagine, di accertamento e di perseguimento di reati o di esecuzione di sanzioni penali: quali passi avanti alla luce dei recenti sviluppi?*, in A. MANTELERO-D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, Pisa, 2018, pp. 495-509.

scambi automatizzati illegittimi⁶⁵, tanto più se si considerano, da un lato, le ben note problematiche di qualità dei dati, e in particolare delle immagini facciali⁶⁶, che possono determinare l'insorgenza di falsi positivi e, dall'altro, la ricorrente inclusione negli archivi penali di persone non responsabili di reati, né (ancor peggio) sospettate di aver commesso un delitto⁶⁷. Ecco allora che, nella sostanza, si consente la circolazione transfrontaliera di informazioni "sensibili" di persone non condannate, né oggetto di indagine, ai fini della comparazione, sebbene non vi sia certezza di un *match* e, anzi, anche là dove poi non si confermi l'inerenza di tali dati a quelli immessi dallo Stato richiedente⁶⁸.

Non ridimensiona certo le criticità la circostanza per cui il regolamento impone che il profilo DNA, l'impronta digitale o l'immagine facciale, a cui si accede per la verifica della corrispondenza, non debbano contenere alcuna informazione aggiuntiva che permetta l'identificazione diretta di una persona fisica: anzitutto, perché quelle processate sono – lo si ripete – comunque categorie particolari di dati personali⁶⁹. In secondo luogo, occorre poi sottolineare come, secondo quanto previsto dalla direttiva 2016/680, i dati biometrici permettono *ex se* l'identificazione univoca della persona anche se non archiviati e trattati assieme alle informazioni – propriamente – biografiche⁷⁰. Inoltre, v'è da ricordare come l'interrogazione delle banche dati nazionali tramite il sistema centrale può essere volta, come specificato dal già richiamato art. 33 reg. Prüm, non solo a «identificare una persona» ma anche a «ottenere maggiori dati su una persona nota»: ciò significa che il soggetto può essere già conosciuto dalle autorità dello Stato richiedente. Insomma, non si può escludere (... anzi appare probabile) che già all'atto dell'invio dell'elenco, i titolari dei dati personali inclusi nella lista e trasferiti per il confronto potrebbero essere individuati, senza che sia all'uopo necessario lo scambio delle informazioni più dettagliate.

Ad ogni modo e concludendo sul punto, quando «le procedure» automatizzate «mostrano una corrispondenza tra i dati utilizzati per la

⁶⁵ Sempre, EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., p. 20.

⁶⁶ Sul punto si tornerà a stretto giro; cfr. *infra*, § 3.

⁶⁷ EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., p. 20.

⁶⁸ R. CAVALLI, *Prüm II and the EPRIS Index in Europe: an Attempt to Balance People's Security and Privacy?*, in *Computer Science & Information Technology (CT & IT)*, 2024, p. 68.

⁶⁹ EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., p. 20.

⁷⁰ *Ibidem*.

consultazione e i dati conservati nella banca dati dello Stato membro o degli Stati membri richiesti» (art. 47 reg. Prüm) e dopo che il membro qualificato del personale ha confermato manualmente il *match*, lo Stato membro richiedente può avanzare istanza di trasmissione dei «dati di base»⁷¹.

Per poter richiedere tali dati, lo Stato deve trasmettere «una descrizione dei fatti e un'indicazione del reato sottostante» – tramite una «tabella comune delle categorie di reati stabilita in un atto di esecuzione da adottare» – così da permettere una valutazione sulla «proporzionalità della richiesta, compresa la gravità del reato per il quale è stata effettuata una consultazione, conformemente al diritto nazionale dello Stato membro che fornisce la serie di dati di base» (art. 47 § 1 lett. c). Se tali condizioni (corrispondenza, verifica manuale e trasmissione della descrizione dei fatti e dell'indicazione del reato) sono soddisfatte, la serie di dati di base è rinviata tramite il *router* entro 48 ore. Pur tuttavia, se, in base alla legislazione nazionale, lo Stato membro richiesto può fornire una serie particolare di dati di base solo previa autorizzazione giudiziaria, si potrà derogare al termine previsto per l'invio, ma soltanto nella misura necessaria all'ottenimento di siffatta autorizzazione (art. 47 § 2).

3. Segue. *La circolazione delle immagini facciali*

Qualche attenzione in più deve riservarsi all'introduzione delle immagini del volto all'interno dei dati passibili di trasmissione.

Le ragioni alla base del nuovo inserimento sono facilmente intuibili: preso atto della crescente importanza che le tecnologie di riconoscimento facciale stanno assumendo nell'ambito dell'attività di contrasto e accertamento dei reati⁷² e, di conseguenza, l'altrettanto crescente disponibilità di

⁷¹ Ossia: «a) nome o nomi; b) cognome o cognomi; c) *alias* e nome o nomi usati in precedenza; d) data di nascita; e) cittadinanza o cittadinanze; f) luogo e paese di nascita; g) sesso; h) la data e il luogo in cui i dati biometrici sono stati acquisiti; i) il reato per il quale i dati biometrici sono stati acquisiti; j) il numero della causa penale; k) l'autorità competente per la causa penale» (art. 47 § 4 reg. Prüm).

⁷² In dottrina, v. G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *Leg. pen. (web)*, 11 dicembre 2021; ID., *L'errore nel riconoscimento facciale automatizzato – Sezione I. Profili giuridici*, in W. NOCERINO (a cura di), *L'errore tecnico e la prova penale*, Pacini Giuridica, Pisa, 2025, p. 175 ss.; J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.*, 2022, p. 1057 ss.; M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisprudenza penale, intelligenza artificiale ed etica del giudizio*, Giuffrè, Milano, 2021, p. 52 ss.; R. LOPEZ, *Riconoscimento facciale tramite software e individuazione del sospettato*, in A.

dati da impiegare nell'«identificazione» biometrica»⁷³, tramite l'accesso transfrontaliero alle *facial images* a fini comparativi, le autorità di *law enforcement* dovrebbero essere nelle condizioni di confrontare un ampio spettro di immagini così da poter dare (non solo un volto, ma anche) un nome agli autori di reati⁷⁴.

Sennonché, oltre alle criticità già illustrate e comuni alle ipotesi di consultazione e trasferimento di tutti dati biometrici, possono segnalarsi ulteriori problematiche direttamente legate alle specifiche caratteristiche delle tecnologie di *facial recognition*.

In prima battuta, possono sollevarsi perplessità sulla riuscita del meccanismo dal punto di vista strutturale: non è infatti un mistero che molti Paesi dell'Unione non siano ancora dotati dell'architettura tecnica⁷⁵ «né delle competenze operative necessarie per implementare in modo efficace e sistematico lo scambio» *ultra fines* delle immagini del volto. A difettare, in particolare, sono proprio le «piattaforme interoperabili adeguatamente sicure e conformi agli standard previsti dalla normativa eurounitaria»⁷⁶.

SCALFATI (a cura di), *Le Pre-investigazioni*, Giappichelli, Torino, 2020, p. 295 ss.; A. MARANDOLA, *Il riconoscimento facciale*, in C. CONTI-A. MARANDOLA (a cura di), *La prova scientifica*, Giuffrè, Milano, 2023, p. 495 ss.; G. MOBILIO, *Tecnologie di riconoscimento facciale*, Editoriale Scientifica, Napoli, 2021; E. SACCHETTO, Face to face: il complesso rapporto tra automated facial recognition technology e processo penale, in *Leg. pen. (web)*, 16 ottobre 2020; EAD., *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna*, cit.; EAD., *La capacità dimostrativa di un match di riconoscimento facciale nel procedimento penale alla luce del regolamento (UE) 2024/1689*, in L. BERNARDINI-C. DE CARO (a cura di), *Sfide attuali e tendenze future del diritto processuale penale europeo*, cit., p. 311 ss.; M. TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. proc.*, 2021, p. 1042 ss.

⁷³ Come ricorda G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato*, cit., p. 3, le tecnologie di riconoscimento facciale «possono essere impiegate tanto in chiave di “verifica”, quanto di “identificazione” biometrica». Nella prima evenienza, si valuta la corrispondenza fra «il modello biometrico rilevato e quello già in possesso dell'autorità associato ad un nominativo che si intende appunto verificare». Nel secondo caso, viene a essere operato un confronto «tra il *template* registrato e quelli disponibili», onde «scoprire l'identità di un individuo».

⁷⁴ N. VAVOULA, *Police Information Exchange*, cit., p. 31.

⁷⁵ Nella scheda finanziaria legislativa che accompagnava la proposta di regolamento si dava atto come al 2021 tredici Stati membri non avessero ancora banche dati nazionali di immagini facciali; cfr. *Proposta di regolamento del Parlamento europeo e del Consiglio sullo scambio automatizzato di dati per la cooperazione di polizia (“Prüm II”), che modifica le decisioni 2008/615/GAI e 2008/616/GAI del Consiglio e i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818 del Parlamento europeo e del Consiglio*, cit., p. 69. Sul punto, v. altresì EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., p. 27.

⁷⁶ Così, anche per la citazione precedente, E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna*, cit., p. 199. Sul tema della sicurezza e sul rischio di attacchi informatici ai *databases* delle

Ma anche a voler supporre che, nel breve-medio periodo⁷⁷, tutti gli Stati membri adottino le misure tecniche necessarie a permettere allo strumento di circolazione di funzionare⁷⁸, rimane il tema – sicuramente primario – dell’impatto che tale “smercio” di dati biometrici facciali potrebbe avere sui diritti fondamentali della persona.

Anzitutto, l'aver legittimato l'impiego dello strumento di scambio per la prevenzione anche di reati di minimo allarme sociale rischia concretamente di permettere e, anzi, incentivare una sorveglianza di massa, mettendo a repentaglio «la stessa libertà morale dell[e] person[e] [...], intesa come facoltà di autodeterminarsi rispetto agli stimoli»⁷⁹.

Ancora, è elemento ormai noto, oltretché ben studiato in dottrina⁸⁰, che i sistemi di riconoscimento facciale presentino un alto tasso di errore, restituendo sovente “falsi positivi”⁸¹. Ciò è dovuto, in particolar modo, alla qualità delle immagini, sia quelle da verificare⁸², che quelle contenute nel *database* interrogato⁸³: più i “termini” del confronto sono di bassa qualità, maggiore è il rischio che il riconoscimento venga negativamente condizionato. Senza considerare che i *software* di comparazione di immagini «non sono in grado di stabilire se due profili biometrici (quello sconosciuto e quello noto) appartengono alla stessa persona, esprimendo piuttosto la probabilità che essi coincidano»⁸⁴.

Se a simili notazioni si aggiunge la circostanza, già segnalata, per cui il

immagini facciali, si vedano le riflessioni di T. KARATHANASIS, *Biometric Data and Facial Recognition Technology in the EU*, in N. MENÉNDEZ GONZÁLEZ-G. MOBILIO (a cura di), *Next democratic Frontiers for Facial Recognition Technology (FRT). The Legal, Ethical and Democratic Implications of FRT*, Springer, Cham, 2025, p. 101 s.

⁷⁷ Ai sensi dell'art. 75 § 2 reg. Prüm, gli Stati devono provvedere, entro due anni dall'entrata in funzione del *router* (v. *supra*, nota 24), che le immagini del volto siano disponibili ai fini della consultazione automatizzata.

⁷⁸ Sebbene L. SCAFFARDI, *Next generation Prüm e le scelte strategiche della UE*, cit., p. 220 pare dubitarne.

⁷⁹ Le parole, seppur usate con riferimento agli strumenti di riconoscimento facciale in *real time*, sono di M. TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, cit., p. 1054.

⁸⁰ Su tutti, G. BORGIA, *L'errore nel riconoscimento facciale automatizzato*, cit., p. 180-186.

⁸¹ V. EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., p. 27, secondo cui «facial recognition is notoriously error-prone and unreliable».

⁸² Invero, «fattori quali l'illuminazione, l'ombra, l'angolo, la densità dei *pixel*, l'espressione del viso e l'occlusione parziale del volto possono dare vita a risultati fuorvianti»: così, G. BORGIA, *L'errore nel riconoscimento facciale automatizzato*, cit., p. 184.

⁸³ V'è, del resto, una differenza notevole «tra la foto segnaletica realizzata in un “ambiente controllato” come una stazione di polizia o un penitenziario, in cui l’illuminazione e l’orientamento del soggetto possono essere regolati, e il *frame* estratto da un video registrato da un sistema di telecamere a circuito chiuso installato in un luogo di transito quale una stazione ferroviaria o una piazza»; cfr. *ibidem*.

⁸⁴ Ancora G. BORGIA, *L'errore nel riconoscimento facciale automatizzato*, cit., p. 184.

router centrale invia allo Stato richiedente un «elenco dei dati biometrici [facciali] per i quali è stata riscontrata una corrispondenza e le relative classifiche» (art. 37 § 4 reg. Prüm), si può agevolmente comprendere la misura del pericolo che all'interno della lista vi siano «profili» di persone totalmente estranee agli eventi che devono essere prevenuti o accertati.

La presenza – che, a questo punto, potremmo dar quasi per certa – di falsi positivi potrebbe, allora, determinare l'iscrizione negli appositi registri degli indagati nazionali di tali soggetti esterni alla vicenda, nonché, nelle ipotesi peggiori, l'applicazione di misure limitative della loro libertà personale, in patente contrasto con la presunzione di non colpevolezza.

Ma vi è di più. Come è stato opportunamente rilevato, lo «stuolo» di *matches* – molti o, perfino, tutti non accurati – che viene riversato sullo Stato richiedente potrebbe influire negativamente anche sull'attività di contrasto alla delittuosità e di accertamento dei reati, aprendo «numeroso ipotesi investigative che potrebbero infine rivelarsi forvianti»⁸⁵.

Occorre, poi, rilevare l'assenza di armonizzazione fra le legislazioni nazionali in merito agli stessi presupposti e criteri per l'acquisizione, lo stoccaggio, la lavorazione e la trasmissione delle *facial images*⁸⁶. Ciò potrebbe determinare differenti livelli di garanzie fra gli Stati membri, oltre a disparità di trattamento⁸⁷, dal momento che l'inserimento di una persona nel *database* nazionale e, dunque, la possibilità che il suo volto circoli da Paese a Paese a fini «identificativi» o di riscontro verrebbero a dipendere esclusivamente dal luogo ove è stata catturata l'immagine⁸⁸.

Sussiste un ulteriore aspetto problematico: la scelta di non tracciare regole comuni atte a disciplinare l'acquisizione delle immagini facciali implica che oggetto di comparazione siano anche immagini «carpite» secondo *standard* qualitativi (e di garanzie individuali) inferiori a quelli fissati dallo Stato richiedente. Da qui, si fa tutt'altro che remota la possibilità che «le carenze interne ai singoli ordinamenti finiscano per riverberare i propri effetti negativi anche in altri sistemi»⁸⁹. Ebbene, tale potenziale diffusione

⁸⁵ L. SCAFFARDI, *Next generation Prüm e le scelte strategiche della UE*, cit., p. 219.

⁸⁶ In proposito, v. E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 199.

⁸⁷ Come rilevato da EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., p. 26.

⁸⁸ In proposito, basti ricordare che l'art. 19 § 1 reg. Prüm rimette alla legge degli Stati membri la scelta se includere, nelle rispettive banche dati – istituite per la prevenzione, l'indagine e l'accertamento dei reati – da collegare al *router*, le immagini del volto delle vittime.

⁸⁹ G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuri sviluppi normativi sul fronte europolitano*, cit., p. 23.

endemica degli errori è ancor più preoccupante se si considerano le discriminazioni che gli strumenti di riconoscimento facciale «hanno dimostrato di perpetrare nei riguardi di determinate categorie di individui», i quali sono, in questo modo, «maggiormente esposti al pericolo di essere erroneamente ricompresi nella lista delle possibili corrispondenze»⁹⁰.

Insomma, la prospettiva è allarmante: il legislatore unionale sembra non solo aver aperto i cancelli a «nuove forme di sorveglianza pervasiva»⁹¹ suscettibili di limitare eccessivamente la libertà morale delle persone, ma aver altresì dato avvio a un processo di circolazione di elementi cognitivi – se non, come si vedrà, probatori⁹² – errati e discriminatori⁹³.

4. *L'accesso ai police records fra problemi di traduzione e questioni di ordine generale*

Ancorché estraneo a quelli che dovrebbero essere i confini propri della presente indagine, merita qualche accenno anche il procedimento di scambio degli estratti del casellario giudiziale.

Sebbene già nel programma di Stoccolma del 2009 il Consiglio europeo esortasse la Commissione a «effettuare uno studio di fattibilità sulla necessità di istituire un indice europeo dei casellari giudiziari (*European Police Records Index System — EPRIS*) e sul valore aggiunto che esso»⁹⁴ avrebbe

⁹⁰ Così, ancora una volta, G. BORGIA, *L'errore nel riconoscimento facciale automatizzato*, cit., p. 185, il quale ricorda come i *bias* riguardano, soprattutto, il colore della pelle, il genere e l'età.

⁹¹ L. SCAFFARDI, *Next generation Prüm e le scelte strategiche della UE*, cit., p. 221.

⁹² Cfr. *infra*, § 6.

⁹³ Certamente condivisibili sono le osservazioni di E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 200, secondo la quale l'«errore derivante da *bias* algoritmico», dilatando i suoi effetti «su più ordinamenti giuridici», rischia di compromettere «la fiducia reciproca tra autorità e, soprattutto, l'effettività delle garanzie dei diritti fondamentali». In proposito, v. anche N. AMELUNG-H. MACHADO, *Dancing in the Dark*, cit., p. 798.

⁹⁴ V. il punto 4.2.3, intitolato «[m]obilitare gli strumenti tecnologici necessari», del *Programma di Stoccolma – Un'Europa aperta e sicura al servizio e a tutela dei cittadini*, adottato dal Consiglio europeo il 10 e 11 dicembre 2009. In tema, si veda anche la ricerca svolta – su richiesta della Commissione – sulle possibili modalità di sviluppo dello scambio di *police records* fra Stati membri in cui si evidenziava come ci fosse «*a strong interest of investigators in an efficient international information exchange, especially with regard to cases that may have international implications*» e come «*[b]y developing and maintaining active relationships between different local, national and international law enforcement agencies, investigators throughout the EU successfully bring criminal cases to prosecution and conclusion*»; cfr., *Study on possible ways to enhance efficiency in the exchange of police records between the Member States by setting up a European Police Records Index System EPRIS*, in *op.europa.eu*, p. 5.

be rappresentato, si è dovuto attendere – e, si anticipa, l’attesa non è stata certo ripagata – il regolamento in commento affinché venisse istituito, al fianco del sistema europeo di informazione sui casellari giudiziari (ECRIS)⁹⁵, un meccanismo teso a permettere la circolazione transfrontaliera dei *police records*.

Muovendo dalla disciplina normativa, occorre subito notare come, contrariamente a quanto previsto con riferimento ai dati biometrici, l’art. 25 § 1 reg. Prüm rimette agli Stati membri la scelta⁹⁶ di partecipare allo

⁹⁵ Istituito con decisione quadro 2009/316/GAI come modificata dalla direttiva (UE) 2019/884, ECRIS si sostanzia in un «meccanismo che, pur ovviamente prefiggendosi l’obiettivo di rendere più veloce e completa la trasmissione dei dati, [continua] a ruotare intorno allo Stato di cittadinanza del condannato, senza peraltro procedere all’armonizzazione dei sistemi nazionali di base»; così, B. GALGANI, *Forme e garanzie nel prisma dell’innovazione tecnologica*, cit., p. 27, la quale evidenzia altresì come «il flusso comunicativo continu[i] a rinvenire il proprio “innesco naturale” nella richiesta avanzata da parte dello Stato che intende conoscere la biografia criminale di un determinato soggetto». L’istanza trova disciplina nell’art. 6 della decisione, a mente del quale, «quando si richiedono informazioni al casellario giudiziario di uno Stato membro ai fini di un procedimento penale contro una persona o a fini diversi da un procedimento penale, l’autorità centrale di tale Stato membro può, conformemente al diritto nazionale, rivolgere all’autorità centrale di un altro Stato membro una richiesta di estrazione di informazioni e dati a esse attinenti dal casellario giudiziario».

In dottrina, v. anche D. CIMADOMO, *I casellari e l’anagrafe*, in G. SPANGHER (diretto da), *Trattato di procedura penale*, vol. VI, L. KALB (a cura di), *Esecuzione e rapporti con autorità giurisdizionali straniere*, Utet, Torino, 2009, p. 360-368; ID., *Il casellario giudiziario*, in L. KALB (a cura di), *«Spazio europeo di giustizia» e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali*, Giappichelli, Torino, 2012, p. 845-847; G. DI PAOLO, *Il riconoscimento degli effetti della condanna e lo scambio di dati estratti dal casellario giudiziale (dd.lgs. 12 maggio 2016, nn. 73, 74, 75)*, in F. RUGGIERI (a cura di), *Processo penale e regole europee: atti, diritti, soggetti e decisioni*, Giappichelli, Torino, 2017, p. 235 ss.; M. GIALUZ, *Il casellario giudiziario europeo: una frontiera dell’integrazione in materia penale*, in F. PERONI-M. GIALUZ (a cura di), *Cooperazione informativa e giustizia penale nell’Unione europea*, cit., p. 191 ss.; L. KALB, *Il sistema informativo giudiziario: il casellario e l’anagrafe*, in G. SPANGHER-A. MARANDOLA-G. GARUTI-L. KALB (diretto da), *Procedura penale. Teoria e pratica del processo*, vol. IV, L. KALB (a cura di), *Impugnazioni. Esecuzione penale. Rapporti giurisdizionali con autorità straniere*, Utet, 2015, p. 778 ss.; R. TROISI, *La considerazione dei precedenti penali “europei” nell’ordinamento interno*, in *Dir. pen. proc.*, 2016, p. 1159 ss.

⁹⁶ Nondimeno, la circostanza per cui l’accesso alle banche dati degli Stati membri contenenti informazioni estratte dai casellari giudiziari sia consentito «in uno spirito di reciprocità» (cfr. considerando n. 18 del reg. Prüm) solo a quei Paesi dell’Unione che, a loro volta, mettono a disposizione i loro archivi porta a ritenere che «*the exchange of police records may not be considered genuinely voluntary, but rather heavily incentivised*»; in questi termini, EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., p. 29. In proposito, EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation (“Prüm II”)*, cit., p. 12 legge la non obbligatorietà dell’adesione quale possibile elemento sintomatico della scarsa fiducia che il legislatore unionale ripone sullo scambio dei *police records*.

scambio automatizzato degli «estratti del casellario giudiziale», ossia – giusta la definizione contenuta all'art. 4 n. 21 reg. Prüm – dei «dati anagrafici di persone indagate e condannate disponibili nelle banche dati nazionali istituite a fini di prevenzione, indagine e accertamento di reati».

Sempre ai sensi dell'art. 25 § 1, là dove intendano prendere parte allo scambio, i Paesi devono garantire «la disponibilità di indici dei casellari giudiziali nazionali contenenti serie» dei suddetti «dati anagrafici di persone sospettate e condannate»⁹⁷. Il secondo paragrafo della disposizione precisa che i nomi, i cognomi e gli *alias* devono essere – già lo si è anticipato – pseudonimizzati, ossia trattati in modo tale da non essere attribuibili «a un interessato specifico senza l'utilizzo di informazioni aggiuntive»⁹⁸.

In forza dell'art. 26, la consultazione⁹⁹ dei *police records* può essere avviata da uno Stato membro o da Europol solo «[a]i fini della prevenzione, dell'indagine e dell'accertamento di reati punibili con una pena detentiva massima di almeno un anno ai sensi della legge dello Stato membro richiedente» e, alla stessa stregua di quella riguardante i dati biometrici, è svolta «nel contesto di ciascun singolo caso».

La consultazione avviene tramite EPRIS¹⁰⁰, indicando almeno due fra il nome (o i nomi) della persona, il suo cognome (o cognomi) e la sua data di nascita; se disponibili, lo Stato richiedente (o Europol) può

⁹⁷ Segnatamente, tali serie di dati devono contenere: «a) nome o nomi; b) cognome o cognomi; c) alias e nome o nomi usati in precedenza; d) data di nascita; e) cittadinanza o cittadinanze; f) paese di nascita; g) genere».

⁹⁸ ... e purché queste «informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile»; cfr. art. 3 n. 5 dir. 2016/680, specificamente richiamato dall'art. 4 n. 22 reg. Prüm.

⁹⁹ A mente dell'art. 28 reg. Prüm la domanda di consultazione deve indicare «il codice dello Stato membro richiedente», «la data, l'ora e il numero di riferimento della domanda» e, «se disponibili», i dati di cui all'art. 25.

¹⁰⁰ Secondo quanto previsto dall'art. 65 reg. Prüm, è di Europol la responsabilità dello «sviluppo» e della gestione tecnica di EPRIS. Quanto ai componenti dell'Indice europeo dei casellari giudiziari, l'art. 42 § 3 reg. Prüm stabilisce che esso è costituito da «un'infrastruttura decentrata negli Stati membri, comprendente uno strumento di consultazione che consenta l'interrogazione simultanea degli indici dei casellari giudiziali nazionali, sulla base delle banche dati nazionali», da «un'infrastruttura centrale a sostegno» del sopracennato strumento di consultazione e volta a permettere «l'interrogazione simultanea degli indici dei casellari giudiziali nazionali» e, infine, da «un canale di comunicazione sicuro tra [detta] infrastruttura centrale, gli Stati membri ed Europol». Per un'analisi del ruolo di Europol nel «quadro Prüm II», v. R. CAVALLI, *Prüm II and the EPRIS Index in Europe*, cit., p. 62-64.

altresì immettere l'*alias*, la cittadinanza, il paese di nascita e il genere. Ancora una volta, si prescrive la pseudonimizzazione di questi dati (art. 43).

Successivamente, EPRIS inoltra la domanda agli indici dei casellari giudiziali nazionali degli Stati membri, che vengono così interrogati «in modo automatizzato e senza ritardo» (art. 44 § 1 e 2). Le eventuali corrispondenze sono rinviate, altrettanto automaticamente, all'Indice europeo (§ 3).

Proprio come il *router* centrale, anche EPRIS provvede a rendere noto al Paese richiedente e a Europol, sempre in maniera automatizzata, l'elenco dei *matches*, elenco che deve riportare la «qualità» delle corrispondenze, nonché «lo Stato membro o gli Stati membri i cui indici dei casellari giudiziali contengono i dati» per i quali vi è stato un riscontro (§ 4).

Lo Stato richiedente decide, poi, «quali sono le corrispondenze alle quali è necessario dare seguito e invia una domanda motivata di follow-up contenente i dati di cui agli articoli 25 e 27, e qualsiasi ulteriore informazione pertinente allo Stato membro o agli Stati membri richiesti tramite SIENA¹⁰¹». Quest'ultimi sono chiamati a trattare le istanze «senza ritardo per decidere se condividere i dati conservati nella loro banca dati».

Così delineata la procedura volta al trasferimento *ultra fines* dei *police records*, occorre volgere l'attenzione agli (per vero, innumerevoli) aspetti problematici che caratterizzano il meccanismo in parola.

Prima di tutto, però, appare opportuno evidenziare una criticità «tutta italiana». Se, infatti, nella versione in lingua inglese il regolamento parla di «*police records*»¹⁰² per indicare quelle informazioni sulle persone indagate e condannate suscettibili di scambio automatizzato, per distinguerle dai «*criminal records*», ossia i casellari giudiziari oggetto di circolazione tramite ECRIS, la traduzione italiana – lo si è visto – riporta la dicitura «estratti del casellario giudiziale».

Si tratta di una scelta lessicale errata: è circostanza risaputa che, nel nostro ordinamento, all'interno del casellario giudiziale¹⁰³ si iscrivono,

¹⁰¹ Ossia, come ricorda l'art. 4 n. 28 reg. Prüm, «l'applicazione di rete per lo scambio sicuro di informazioni, gestita e sviluppata da Europol in conformità del regolamento (UE) 2016/794».

¹⁰² «*Fichiers de police*» nella versione francese e «*antecedentes policiales*», in quella spagnola.

¹⁰³ Termine con cui si delinea sia «il «contenitore» delle informazioni ricavabili a seguito della relativa iscrizione», sia «lo strumento sussidiario e complementare della funzione giudiziaria, esercitata anche attraverso la consultazione del complesso di notizie rilevanti ai fini dell'applicazione della legge»: così, D. CIMADOMO, *I casellari e l'anagrafe*, cit., p. 346. In termini analoghi si esprime L. KALB, *Il sistema informativo giudiziario: il casellario e l'anagrafe*, cit., p. 749. In dottrina, si veda anche DEL POZZO, voce *Casellario giudiziale*, in *Enc. dir.*, vol. VI, Giuffrè, Milano 1960, p. 366 ss.; P. MOCALI, voce *Casellario giudiziale*, in *Dig. disc. pen.*,

per quanto è qui di interesse, solamente «i provvedimenti giudiziari penali di condanna definitiva»¹⁰⁴ (art. 3 comma 1 n. 1 d.P.R. 14 novembre 2002, n. 313¹⁰⁵); mentre, non vi trovano cittadinanza le informazioni inerenti ai c.d. “precedenti di polizia” o, comunque, ai procedimenti in corso nei confronti di una determinata persona.

Questi, tutt'al più, vengono riportati nel sistema informativo interforze (S.D.I.); tale «pseudo-casellario»¹⁰⁶, invero, accoglie, secondo quanto previsto dall'art. 7 legge 1 aprile 1981, n. 121¹⁰⁷, tutte le «notizie risultanti da documenti che comunque siano conservati dalla pubblica amministrazione o da enti pubblici, o risultanti da sentenze o provvedimenti dell'autorità giudiziaria o da atti concernenti l'istruzione penale acquisibili ai sensi dell'articolo 165-ter del codice» di rito del 1930, ora dell'art. 118 c.p.p.¹⁰⁸.

Ancora differente è il contenuto del casellario dei carichi pendenti, in cui sono iscritti «per estratto» tutti i provvedimenti giudiziari di esercizio dell'azione penale, la revoca della sentenza di non luogo a procedere, il decreto di citazione emesso nel giudizio di revisione, i provvedimenti giudiziari che comportano l'assunzione della qualità di imputato nell'ambito dei procedimenti di competenza del giudice di pace, come «ogni altro provvedimento giudiziario che decide sull'imputazione, emesso nelle fasi e nei gradi successivi»¹⁰⁹.

Ecco allora che il riferimento agli “estratti del casellario giudiziale” per indicare anche i dati anagrafici di persone “indagate” risulta tecnicamente inesatto. L'espressione terminologica utilizzata rischia, inoltre, di creare (non solo una sovrapposizione¹¹⁰ ma anche) confusione fra la procedura di consultazione dei *police records* prevista dal regolamento Prüm e la richiesta di estrazione di informazioni e dati dal casellario giudiziale tramite ECRIS.

In realtà, non appare nemmeno chiaro quale banca dati interna potrebbe essere collegata all'infrastruttura centrale (insomma, a EPRIS) sì da

vol. II, Utet, Torino, 1988, p. 102 ss. V. altresì B. BOCCHINI-M. BRUNI-C. LEONI, voce *Casellario giudiziale*, in *Dig. disc. pen.*, Agg., I, Utet, Torino, 2005, p. 149.

¹⁰⁴ Come noto, all'interno del casellario confluiscono anche alcuni provvedimenti di carattere liberatorio: in tema, v. L. AGOSTINO, *Trattamento dei dati giudiziari, esiti proscioglitivi e aporie in materia di casellario*, in *Arch. pen. (web)*, 2024, f. 2, p. 1 ss.

¹⁰⁵ Si tratta del *Testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di casellario giudiziale europeo, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti*.

¹⁰⁶ Lo definisce così D. CIMADOMO, *I casellari e l'anagrafe*, cit., p. 352.

¹⁰⁷ Recante «[n]uovo ordinamento dell'Amministrazione della pubblica sicurezza».

¹⁰⁸ Come rileva D. CIMADOMO, *I casellari e l'anagrafe*, cit., p. 352.

¹⁰⁹ Cfr. art. 6 d.P.R. 313/2002.

¹¹⁰ V. *infra*.

poter essere interrogata in maniera automatizzata dai punti di contatto degli altri Stati membri o da Europol¹¹¹: difatti, se, da un lato, il casellario giudiziale “italiano” ha al suo interno un *plafond* informativo più ristretto di quello contemplato dalla normativa unionale, sull’altro versante, per ragioni sostanzialmente contrarie, desta particolare timore l’idea di permettere l’accesso *ab externo* allo S.D.I. considerata l’estrema latitudine delle informazioni nello stesso presenti.

Per certo, è da escludersi che EPRIS possa attingere al casellario dei carichi pendenti, posto che, come ricordato, qui vi si possono trovare soltanto i provvedimenti riguardanti gli imputati: categoria, questa, che non viene menzionata dal regolamento.

Spostando il faro sulle problematiche di carattere generale, salta all’occhio come la disciplina della consultazione e dello scambio degli estratti del casellario giudiziale sollevi le medesime questioni sulla legalità e sulla proporzionalità della misura, già analizzate con riferimento ai dati biometrici. I dubbi sorgono, in particolare, in ragione dell’estrema ampiezza del presupposto fissato per l’avvio della procedura («[a]i fini della prevenzione, dell’indagine e dell’accertamento di reati punibili con una pena detentiva massima di almeno un anno»). A tal proposito, merita sicuramente evidenziarsi come nei progetti iniziali EPRIS fosse pensato quale strumento di circolazione di informazioni e di *intelligence* funzionale a «*detect cross-border connections and identify structures of international organized crime or terrorist networks*»¹¹².

Inoltre, la possibilità di svolgere la consultazione nell’ambito di ciascun singolo caso, piuttosto che in relazione a un singolo individuo, fa ritenere fondato il timore di ricerche “a tappeto”.

Sempre sulla scia di quanto già analizzato in merito ai dati biometrici, anche con riferimento agli estratti del casellario giudiziale è stato sottolineato il tema della diretta attribuibilità soggettiva dei dati personali fatti circolare in maniera automatizzata da EPRIS¹¹³. Certo, in forza degli art. 25 § 2 e 43 § 3 i dati contenuti negli archivi nazionali e quelli impiegati

¹¹¹ In forza dell’art. 75 § 7 reg. Prüm, infatti, i Paesi che intendono partecipare allo scambio automatizzato dei casellari giudiziali devono comunicare «agli altri Stati membri, alla Commissione e a Europol il contenuto dei loro indici dei casellari giudiziali nazionali e delle banche dati nazionali utilizzate per stabilire tali indici e le condizioni per le consultazioni automatizzate».

¹¹² Cfr. la comunicazione della Presidenza del Consiglio dell’Unione del 21 dicembre 2009, n. 15526/2/09, recante a oggetto «*European Police Records Index System – elements for a pre-study*»; il documento è consultabile al sito data.consilium.europa.eu.

¹¹³ EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., p. 21

ai fini dell'interrogazione devono essere pseudonimizzati; ma, in primo luogo, «*pseudonymisation does not stop these data from being personal data*»¹¹⁴, il che vuol dire che, onde permettere allo Stato richiedente di «decide[re] quali sono le corrispondenze alle quali è necessario dare seguito e invia[re] una domanda motivata di follow-up», si inoltra in maniera automatica – ossia, senza intervento umano – un elenco di dati personali. In secondo luogo, è da rimarcare come lo Stato richiedente, giusta la previsione di cui allo stesso art. 43 reg. Prüm, debba immettere, ai fini della consultazione, il nome, il cognome e/o la data di nascita del soggetto. Ciò significa che, sebbene i dati di risulta siano pseudonimizzati, il *match* è restituito sulla base delle informazioni biografiche immesse dallo stesso Stato richiedente: insomma, almeno per quanto attiene a quest'ultimo, l'identificazione univoca del soggetto è *in re ipsa*¹¹⁵.

Ulteriori profili critici investono più il versante propriamente contestuale.

Come evidenziato dall'associazione *Statewatch* in uno studio del 2011, i *police records* possono fondarsi sia su informazioni verificate che su notizie di «*soft "intelligence"*»¹¹⁶, basate su sospetti, segnalazioni oppure voci; quindi, elementi che non sono passati sotto il vaglio di un'autorità giudiziaria. È, poi, da tenere di conto la possibilità – non così remota – che le informazioni raccolte in merito a persone indagate di aver commesso un fatto non siano successivamente aggiornate; non tengano, cioè, conto dell'eventuale sviluppo in senso liberatorio del procedimento penale: basti porre mente al caso di un soggetto che è stato più volte segnalato, ma che è incensurato dal momento che i relativi processi non si sono mai svolti – poiché, per esempio, i sospetti si sono rivelati non fondati – oppure si sono tutti conclusi con sentenze di proscioglimento.

Ne discende, allora, che il meccanismo implementato dal quadro Prüm II potrebbe disseminare fra le forze di polizia e le autorità giudiziarie europee informazioni non verificate, non aggiornate o del tutto errate¹¹⁷. Ciò potrebbe comportare effetti oltremodo pregiudizievole per i titolari dei dati scambiati, nei confronti dei quali potrebbero essere disposte attività investigative particolarmente ingerenti, nonché misure limitative

¹¹⁴ *Ibidem*.

¹¹⁵ *Ibidem*.

¹¹⁶ Cfr. STATEWATCH, *Implementing the "principle of availability": The European Criminal Records Information System – The European Police Records Index System – The Information Exchange Platform for Law Enforcement Authorities*, 1° settembre 2011, in *statewatch.org*, p. 27.

¹¹⁷ *Ibidem*. V. anche EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation ("Prüm II")*, cit., p. 12.

della libertà personale, con ulteriori violazioni della presunzione di non colpevolezza.

Rimane, infine, sullo sfondo la questione – tutt’altro che di semplice risoluzione – della sovrapposizione con la procedura di scambio tramite ECRIS: se, da un lato, viene da domandarsi sulla concreta necessità di prevedere il trasferimento dei *police records* inerenti a persone condannate alla luce della possibilità, già contemplata, di richiedere l’estrazione di informazioni dal casellario giudiziale¹¹⁸; dall’altro, appare ragionevolmente probabile che, attese la snellezza del procedimento di trasmissione dei dati sancito dal regolamento Prüm e l’assenza di un vaglio giudiziale sull’istanza di interrogazione, se e quando il meccanismo di nuova introduzione sarà a pieno regime, quello istituito con la decisione quadro 2009/316/GAI sarà definitivamente accantonato.

5. *Alcune riflessioni conclusive*

Cercando di tirare le fila, la sensazione è anzitutto quella di essere di fronte a una normativa che – oltre a presentare le innumerevoli criticità di cui si è già detto – non pare nemmeno aver posto rimedio a tutte quelle inefficienze che hanno contrassegnato il quadro Prüm originario. In particolare, se la (prossima) creazione del *router* e di EPRIS sembra risolvere la problematica inerente alla gestione della rete di connessioni bilaterali fra Stati membri, nondimeno è da registrare la persistente carenza di armonizzazione fra le discipline statali in materia di raccolta, gestione e archiviazione delle informazioni e di funzionamento dei relativi archivi digitali¹¹⁹.

In assenza di un’architettura comune in materia di criteri e condizioni di inserimento dei dati biometrici (come pure dei *police records*) nelle rispettive banche dati, ma anche con riguardo alle procedure di utilizzo e circolazione dei dati, si fa concreto il rischio di uno scambio “a più velocità” che, come si è modo avuto di sottolineare anche in precedenza, potrebbe comportare profonde disparità di trattamento.

Inoltre, la dottrina non ha tardato a sottolineare i «continui rinvii ad atti» di esecuzione¹²⁰ onde «definire alcuni aspetti peculiari, come l’entra-

¹¹⁸ Sul punto, si veda EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., 29 ove si sollevano dubbi sulla stessa necessità e proporzionalità dell’inclusione dei *police records* nel quadro Prüm II, anche alla luce della possibilità di condividere i casellari giudiziali tramite ECRIS.

¹¹⁹ Come rileva C. PALLANTE, *Le nuove sfide della cooperazione investigativa nello spazio europeo*, cit., p. 272.

¹²⁰ Cfr. art. 31 reg. Prüm.

ta in vigore della normativa e la definizione dei criteri *standard* di qualità¹²¹ del materiale da scambiare»¹²², ma pure «le modalità e le specifiche tecniche per le procedure di consultazione automatizzata, le norme per lo scambio di dati [...] e i dati da scambiare»¹²³.

Si tratta di una delega della «funzione disciplinare»¹²⁴ ad atti non legislativi che, non solo rende «di fatto meno organica la materia *de qua*»¹²⁵, ma pare altresì spingere verso una rarefazione – se non una vera e propria erosione – dello stesso principio di legalità¹²⁶. È di tutta evidenza, infatti, come agli atti esecutivi sia rimessa la “normazione” di profili fondamentali, in assenza – questa è, quantomeno, l'impressione – di una puntuale perimetrazione dei confini entro cui tale attività di regolazione accessoria deve essere svolta. Si pensi, ad esempio, a come si demandi alla Commissione l'indicazione delle norme minime di qualità per il raffronto dei dati biometrici, senza tuttavia specificare il significato da attribuire all'espressione “qualità dei dati”. Oppure, si ponga ancora mente alla circostanza che la Commissione è chiamata a individuare le «norme europee o internazionali»¹²⁷ che devono essere utilizzate dagli Stati membri e da Europol per lo scambio degli stessi dati biometrici; anche in quest'ultimo caso, mancano totalmente “indicazioni di massima” a cui la Commissione dovrà attenersi nella sua opera di puntualizzazione.

Due ulteriori aspetti meritano di essere accennati in chiusura.

Il primo attiene alla possibilità¹²⁸, espressamente contemplata dal-

¹²¹ Si vedano gli artt. 8 § 2, 13 § 2 e 22 § 2 reg Prüm, in forza dei quali la Commissione è chiamata a stabilire, «tramite un atto di esecuzione, una norma minima di qualità per consentire il confronto» dei profili DNA, dei dati dattiloscopici e delle immagini del volto.

¹²² Così, C. PALLANTE, *Le nuove sfide della cooperazione investigativa nello spazio europeo*, cit., p. 272.

¹²³ Cfr. considerando n. 35 del regolamento Prüm.

¹²⁴ Le parole sono di B. GALGANI, *Forme e garanzie nel prisma dell'innovazione tecnologica*, cit., p. 166 s., la quale ha modo di evidenziare le «ambiguità ontologiche» del c.d. *soft law*, tanto «in punto di (dubbio) ossequio alla legalità processuale» quanto «in punto di (dimidiate) coerenza e vincolatività».

¹²⁵ Ancora, C. PALLANTE, *Le nuove sfide della cooperazione investigativa nello spazio europeo*, cit., p. 272.

¹²⁶ Più in generale, D. NEGRI, *Splendori e miserie della legalità processuale*, in *Legge e potere nel processo penale*, Wolters Kluwer-Cedam, Milano-Padova, 2017, p. 74 osserva come la «proliferazione di atti – di varia e spesso dubbia natura giuridica – che ambiscono a porsi quali fonti regolatrici, oltre e persino contro la legge» stia «dando vita ad un'autentica delegificazione della stessa disciplina processuale».

¹²⁷ V. artt. 8 § 3, 13 § 3 e 22 § 3.

¹²⁸ ... a cui si affianca, sul versante reciproco, la facoltà degli Stati membri di consultare i «dati biometrici forniti da paesi terzi e conservati da Europol» (art. 48) e quella di

l'art. 60 reg. Prüm, per gli Stati membri ed Europol di «trasferi[re] i dati personali ricevuti a norma del [...] regolamento a un paese terzo o a un'organizzazione internazionale»¹²⁹. La previsione desta particolari perplessità: il probabile scenario è quello di favorire misure di repressione politica da parte di Paesi terzi¹³⁰, che, proprio grazie al procedimento *de quo*, avrebbero un fin troppo facile strumento di accesso alle informazioni sensibili di persone “invisi”.

Inoltre, spostandoci sul versante della *data protection*, occorre osservare come la diffusione extra-UE dei dati rischi di farne perdere le “tracce”. Certo, l'art. 60 dispone che il trasferimento deve avvenire «in conformità del capo V della direttiva (UE) 2016/680»¹³¹ – o se sono soddisfatte le condizioni di cui all'art. 25 del regolamento (UE) 2016/794¹³², quando è Europol a inviare i dati al di là dei confini dell'Unione europea – e previa autorizzazione dello Stato membro richiesto; tuttavia, risulta, comunque, assai difficoltoso riuscire a seguire il percorso compiuto dalle informazioni personali, che una volta ricevute dal Paese terzo potrebbero essere “inoltrate” alle autorità di un altro Stato, e così via, finendo per uscire in maniera definitiva dalla sfera di controllo del soggetto titolare.

Da ultimo, vi è una questione, per così dire, di sistema.

Come rilevato da alcuni autori, si assiste sempre più a tendenza di

Europol di accedere «ai dati conservati nelle banche dati degli Stati membri tramite l'uso di dati forniti da paesi terzi» (art. 49).

¹²⁹ Circostanza, questa, che dovrebbe essere presa in considerazione nell'ambito della verifica in merito alla proporzionalità e necessità in concreto della procedura di consultazione e scambio avviata dallo Stato membro o da Europol (cfr. *supra*, § 3). Da tale angolo prospettico, degna di menzione è una sentenza della Corte costituzionale tedesca (*Bundesverfassungsgericht*) del 2023, in cui – per l'appunto – si riconduce fra i fattori, da tenere di conto nella valutazione della proporzionalità di strumenti particolarmente intrusivi sull'autodeterminazione informativa, la possibilità che i dati raccolti e processati possano essere comunicati ad altri Stati; cfr. BVerfG, 26 febbraio 2023, 1 BvR 1547/19, 1 BvR 2634/20 § 99. Per un commento alla sentenza *de qua* – reperibile al sito *bundesverfassungsgericht.de* – si rinvia a G. BORGIA, *Analisi automatizzate di dati per finalità di law enforcement e diritto all'autodeterminazione informativa: dalla Corte costituzionale federale tedesca utili indicazioni (anche) per il legislatore dell'Unione*, cit., p. 229 ss.

¹³⁰ EUROPEAN DIGITAL RIGHTS, *Respecting fundamental rights in the cross-border investigation of serious crimes*, cit., p. 11.

¹³¹ A rilevare sono, in particolare, gli artt. 36, 37 e 38 della direttiva in parola, che subordinano il trasferimento dei dati a una decisione di adeguatezza del paese terzo emessa dalla Commissione, all'assicurazione, da parte dello stesso Paese terzo, di garanzie in merito alla protezione dei dati o, infine, alla ricorrenza di specifiche situazioni.

¹³² In forza della disposizione *de qua*, Europol può inviare dati personali a un Paese terzo o a un'organizzazione internazionale solamente a fronte di una decisione di adeguatezza adottata dalla Commissione o di un accordo internazionale o di cooperazione concluso con il Paese terzo o l'organizzazione da, rispettivamente, l'Unione europea o da Europol.

«datificazione» della prova, ossia a uno «scivolamento dal “dato” all’elemento di prova (alla prova, eventualmente)». Più nello specifico, si rileva come il dato, «preesiste[ndo] al procedimento penale [...], finisca per essere incasellato, nella nostra tradizionale tassonomia processualpenalistica, all’interno della categoria della prova documentale»¹³³.

Preso atto di ciò, viene allora da chiedersi se il meccanismo di consultazione e scambio di dati biometrici implementato dal regolamento Prüm non si traduca in una vera e propria modalità di acquisizione transnazionale di prove; del resto, oggetto di trasferimento sono «informazioni in formato elettronico già autonomamente elaborate e conservate, anche a prescindere da un procedimento penale, in altro Paese dell’Unione europea»¹³⁴.

Se così fosse, potrebbe allora presentarsi il rischio di una sovrapposizione con gli strumenti “ordinari” di cooperazione giudiziaria in materia istruttoria, primo fra tutti l’ordine europeo di indagine (OEI), e con le garanzie da questi posti. In proposito, vale la pena ricordare come la direttiva 2014/41/UE fissi un requisito minimo per introdurre strumenti altri, rispetto all’OEI, di “movimentazione” di elementi istruttori fra Paesi appartenenti all’Unione. Il riferimento corre all’art. 34, in forza del quale gli Stati membri possono, sì, concludere, anche successivamente all’entrata in funzione dell’OEI, «accordi o intese bilaterali o multilaterali con altri Stati membri» tesi a favorire la circolazione delle prove, ma purché «sia rispettato il livello delle salvaguardie di cui alla [stessa] direttiva».

Ebbene, da tale angolo visuale, può avanzarsi più di una riserva sul fatto che l’architettura predisposta dal legislatore unionale nel 2024 accordi lo stesso livello di garanzie fissato dalla direttiva 2014/41. Viene, infatti, agevole constatare come nel procedimento di consultazione e, soprattutto, di scambio dei dati biometrici manchi – giusto per rilevare il *vunlus* più immediato – un vero e proprio controllo sull’interrogazione avanzata dalla Stato richiedente. Certo, l’art. 33 impone la registrazione delle giustificazioni delle consultazioni e l’art. 47 § 6 dispone che il rinvio dei dati di base è «soggetto alla decisione di un essere umano». Tuttavia, non si contempla un necessario e generale “passaggio giurisdizionale” in cui oggetto di valutazione siano la legittimità e la proporzionalità della misura¹³⁵, né si

¹³³ Così, anche per la citazione precedente, A. PROCACCINO, *Securitizzazione dell’Unione europea e poteri concorrenti. Dall’investigazione, alla prevenzione, all’osservazione*, in *Dir. pen. cont. – Riv. trim.*, 2023, f. 1, p. 152 s.

¹³⁴ In questi termini, G. DI PAOLO, *La circolazione transfrontaliera delle prove elettroniche*, in *Penale Dir. e proc. (web)*, 13 maggio 2024, nota n. 15.

¹³⁵ Come anticipato, l’art. 33 § 3 reg. Prüm prevede che le giustificazioni alle interrogazioni inerenti ai dati biometrici «sono utilizzate unicamente per valutare se le consul-

prevede espressamente la possibilità dello Stato richiesto di rifiutarsi di inviare i dati di base¹³⁶ nel caso in cui il punto di contatto e il membro qualificato del Paese richiedente abbiano verificato la corrispondenza segnalata dal *router*.

Tanto detto, posto che nel quadro Prüm originario, lo scambio dei dati – lo si è visto¹³⁷ – doveva, per espressa previsione, seguire le forme fissate dalle normative sovranazionali in materia di assistenza giudiziaria, si potrebbe allora ritenere che l'assenza di un'analogia, chiara, indicazione nel regolamento Prüm sia sintomatica del fatto che, in materia di circolazione (a fini istruttori) di dati biometrici, il nuovo meccanismo è destinato a sostituire l'ordine europeo di indagine. Tuttavia, occorre ricordare che il regolamento del 2024 rinviene la propria base giuridica negli art. 87 § 2 lett. a e 88 § 2 Tratt. f. UE – in materia di cooperazione di polizia – e non nell'art. 82, dedicato, per contro, alla cooperazione in materia giudiziaria. Mancherebbe, quindi, il fondamento normativo per una “successione” legislativa.

Il che porta a concludere nel senso che – quantomeno nel nostro ordinamento – i dati scambiati tramite il sistema Prüm dovrebbero andare incontro a una regola di esclusione probatoria: come evidenziato in dottrina, infatti, le prove – e, secondo ciò che si è osservato in precedenza, tali sono (o sono destinati a diventare) i dati – raccolte all'estero in maniera autonoma per un procedimento interno, tanto se precostituite¹³⁸,

tazioni sono proporzionali e necessarie ai fini della prevenzione, dell'indagine e dell'accertamento di un reato». Tuttavia, secondo quanto si ricava dal § 4 della medesima disposizione, tale valutazione è demandata – a fini di verifica interna – ai titolari del trattamento, ossia, giusta la definizione di cui all'art. 3 § 8 direttiva 2016/680, «l'autorità competente che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali». L'unico intervento giurisdizionale contemplato è quello previsto dall'art. 47 § 2, intervento che, tuttavia, è eventuale e rimesso alla legislazione dello Stato membro.

¹³⁶ Evidenzia la carenza di un'espressa statuizione di motivi di rifiuto R. CAVALLI, *Prüm II and the EPRIS Index in Europe*, cit., p. 69. Certo, come visto, l'art. 47 § 1 prevede che, in caso di richiesta di dati di base, si debba trasmettere la descrizione dei fatti e un'indicazione del reato «al fine di valutare la proporzionalità della richiesta, compresa la gravità del reato per il quale è stata effettuata una consultazione, conformemente al diritto nazionale dello Stato membro che fornisce la serie di dati di base»; tuttavia, non si stabilisce espressamente che lo Stato richiesto possa rifiutare la trasmissione delle informazioni biografiche se ritiene la consultazione non proporzionata.

¹³⁷ Cfr. *supra*, § 1.

¹³⁸ In proposito, vale la pena ricordare come ai sensi dell'art. 1 comma 1 lett. a d.lgs. 21 giugno 2017, n. 108 (attuativo della direttiva 2014/41) l'OEI è quel «il provvedimento emesso dalla autorità giudiziaria o dalla autorità amministrativa e convalidato dall'autorità giudiziaria di uno Stato membro dell'Unione europea» anche per «*per acquisire informazioni o prove che sono già disponibili*» (enfasi nostra). Allo stesso modo, l'art. 1 dir. 2014/41 dispone espressamente che «[l']OEI può anche essere emesso per ottenere prove già in possesso delle autorità competenti dello Stato di esecuzione». Il tema dell'acquisizione di prove pre-

quanto se formate nel corso del procedimento stesso, non potrebbero essere oggetto di acquisizione in Italia se non per il tramite di un ordine europeo di indagine¹³⁹.

costituite tramite l'OEI è stato, come noto, al centro della decisione della Corte di giustizia sul caso Encrochat (Corte giust., sent. 30 aprile 2024, C-670/22, M.N) e delle sentenze delle Sezioni unite della Corte di cassazione sulla vicenda dei criptofonini Sky ECC (Cass., Sez. Un., 29 febbraio 2024, n. 23755 e Cass., Sez. Un., febbraio 2024, n. 23756, in *sistema-penale.it*, 17 luglio 2024, con nota di M. DANIELE, *Le sentenze "gemelle" delle Sezioni Unite sui criptofonini*). Per un commento alla sentenza del Corte di Lussemburgo, si rinvia, *ex multis*, R. BELFIORE, *L'ordine europeo di indagine nella sentenza "Encrochat" della Corte di giustizia UE*, in *Riv. it. dir. proc. pen.*, 2024, p. 1264 ss.; E. LORENZETTO, *Il caso Encrochat e l'ordine europeo di indagine penale nella staffetta fra Corte di giustizia e diritto dello Stato di emissione*, in *Cass. pen.*, 2024, p. 2887 ss.; M. PERRUCCIO, *Ordine europeo di indagine e criptofonini: l'interpretazione della Corte di giustizia nel caso Encrochat*, in L. BERNARDINI-C. DE CARO (a cura di), *Sfide attuali e tendenza future del diritto processuale penale europeo*, cit., p. 143 ss.

Sulle sentenze della Suprema corte domestica tema si vedano, anche, M. DANIELE, *OEI e messaggi digitali già acquisiti all'estero. Riflessioni a partire dal caso Sky ECC*, *sistema-penale.it*, 27 marzo 2025; F. GIUNCHEDI, *Sezioni unite e acquisizione di dati dalla piattaforma Sky-ECC: soluzioni formalmente ineccepibili, ma lesive dei diritti di difesa e del contraddittorio tecnico*, in *Proc. pen. gius.*, 2025, p. 91 ss.; L. FILIPPI, *Le S.U. ammettono le prove francesi sui criptofonini acquisite con l'ordine europeo di indagine*, in *Pen. Dir. e proc. (web)*, 1° marzo 2024; O. MURRO-W. NOCERINO, *Più ombre che luci nelle sentenze delle Sezioni Unite in tema di criptofonini*, *ivi*, 21 ottobre 2024.

¹³⁹ V. M. DANIELE, *La sfera d'uso delle prove raccolte*, in M. DANIELE-R.E. KOSTORIS (a cura di), *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transazionale delle prove nel d.lgs. n. 108 del 2017*, Giappichelli, Torino, 2018, p. 185 e 195.

AUTORI

LORENZO AGOSTINO, *Assegnista di ricerca in Diritto processuale penale – Università di Pisa*

LAURA BARTOLI, *Ricercatrice di Diritto processuale penale – Università di Bologna*

STEFANO BILLI, *Dottore di ricerca in Diritto processuale penale - Università di Macerata*

VALERIA BOSCO, *Ricercatrice di Diritto processuale penale – Università di Macerata*

ALBERTO CAMON, *Professore ordinario di Diritto processuale penale – Università di Bologna*

CLAUDIA CESARI, *Professoressa ordinaria di Diritto processuale penale – Università di Macerata*

GIACOMO COTTI, *Dottore di ricerca in Scienze Giuridiche – Università di Bologna*

ELEONORA ANNA ALEXANDRA DEI-CAS, *Ricercatrice di Diritto processuale penale – Università di Modena e Reggio Emilia*

NICOLÒ DI PACO, *Dottore di ricerca in Diritto processuale penale – Università di Pisa*

ELENA VALENTINI, *Professoressa associata di Diritto processuale penale – Università di Bologna*

In questa collana

1. AA.VV., *Legge e potere nel processo penale. Pensando a Massimo Nobili* (atti del convegno, Bologna, 4 e 5 novembre 2016), 2017, p. VIII-255.
2. MARCELLO L. Busetto, *Controlli giudiziali sulla qualità della difesa tecnica. Un itinerario fra fonti europee e diritto interno*, 2017, p. VII-239.
3. VALENTINA BONINI, *Il sistema di protezione della vittima e i suoi riflessi sulla libertà personale*, 2018, p. IX-434.
4. DANIELE NEGRI e LORENZO ZILLETTI (a cura di), *Nei limiti della costituzione. Il codice repubblicano e il processo penale contemporaneo*, 2019, p. XV-321.
5. FABIO NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, 2020, p. XIII-246.
6. LAURA BARTOLI, *La sospensione del procedimento con messa alla prova*, 2020, p. IX-474.
7. MICHELE CAIANIELLO and ALBERTO CAMON (edited by), *Digital forensic evidence. Towards common european standards in antifraud administrative and criminal investigations*, 2021, p. XII-258.
8. MASSIMO NOBILI, *Scritti inediti*, a cura di Alberto Camon, 2021, p. IX-140.
9. BENEDETTA GALGANI, *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, 2022, p. XI-428.
10. FABIO NICOLICCHIA, *Ente e imputato nella procedura penale d'impresa. Conflitti, interferenze, anomalie di sistema*, 2022, p. XI-218.
11. ALBERTO CAMON, *Il processo penale sul grande schermo. Lezioni di diritto tenute al cinema*, 2022, p. XVI-186.
12. FRANCESCO BARTOLO MORELLI, *L'annullamento senza rinvio nel giudizio penale di cassazione. Le coordinate di un potere ancipite*, 2023, p. X-262.
13. MARIANNA BIRAL, *La testimonianza anonima degli agenti sotto copertura*, 2023, p. X-266.

14. ELVIRA NADIA LA ROCCA, *L'accertamento della volontà dell'imputato nelle rinunce al contraddittorio*, 2024, p. XIV-302.
15. ANTONIO CAPPuccio e STEFANO RUGGERI (a cura di), *Antichi e nuovi modelli di giustizia partecipata e cultura della giurisdizione. Verso una tutela penale più umana ed egualitaria*, 2024, p. XII-648.
16. ANGELO ZAPPULLA, *Il testimone senza identità*, p. X-370.
17. CLAUDIA CESARI (a cura di), *Nuove tecnologie, dati biometrici e procedimento penale*, 2026, p. XII-298.

Questo volume presenta le riflessioni frutto della ricerca svolta dagli Autori nell'ambito del progetto dal titolo “*Nuove tecnologie, dati biometrici e procedimento penale*”, Finanziato dall'Unione Europea – *NextGenerationEU* – Missione 4 Istruzione e ricerca – Componente 2 *Dalla ricerca all'impresa* – Investimento 1.1, Avviso PRIN 2022 DD N. 104 del 2/2/2022, codice progetto MUR 2022CWNCH8 e coordinato dall'Università di Macerata, con le Università di Bologna, di Ferrara e di Pisa, con lo scopo di contribuire a fornire elementi di approfondimento in ordine alle criticità e prospettive di riforma concernenti la raccolta, la conservazione e l'impiego investigativo e processuale dei dati biometrici.

CLAUDIA CESARI è Professoressa ordinaria di Diritto processuale penale presso l'Università di Macerata.



€ 42,00 I.V.A. INCLUSA