DISPOSITIVI ELETTRONICI INDOSSABILI E PROVA PENALE

di Laura Bartoli e Alberto Camon[1]

(*Ricercatrice* senior *di Procedura penale, Università degli Studi di Bologna, e Professore ordinario di Procedura penale, Università degli Studi di Bologna)*

Se mai le cose potessero parlare –
ma se parlassero, potrebbero anche mentire

(Wisława Szymborska, *Se mai*, in *Racconto Antico*, Milano 2025)

[1] Nonostante il lavoro sia frutto di una riflessione condivisa, la redazione della Parte I e del § 4 della Parte III è opera di Alberto Camon; la Parte II e il resto della Parte III sono di Laura Bartoli.
Lo studio è frutto della ricerca svolta dagli autori nell'ambito del progetto dal titolo "Dispositivi indossabili e accertamento penale". Finanziato dall'Unione Europea – NextGenerationEU a valere sul Piano Nazionale di Ripresa e Resilienza (PNRR) – Missione 4 Istruzione e ricerca – Componente 2 Dalla ricerca all'impresa – Investimento 1.1, Avviso PRIN 2022 DD N. 104 del 02/02/2022, dal titolo "Nuove tecnologie, dati biometrici e procedimenti penali", codice progetto MUR 2022CWNCH8 – CUP J53D23005360006.
Una sua versione, pur diversa da quella qui pubblicata, è destinata al volume a cura di C. Cesari, *Nuove tecnologie, dati biometrici e procedimento penale*, Milano 2026.

Parte I – *Brave new world*

1. 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 esserlo anche da siti "affiliati". Li possiamo rifiutare ma – sempre ammesso che l'operazione riesca[2] – 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 installati[3]. 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 You tube, tutto viene tracciato»[4].

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

[2] 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*[2], trad. it., Roma 2025, 177 s.).

[3] J. Geary, *Tracking the trackers: What are cookies? An introduction to web tracking*, in *theguardian.com*, 23.4.2012.

[4] B. Turner, *When Big Data Meets Big Brother: Why Courts Should Apply United States v. Jones to Protect People's Data*, 16 *North Carolina Journal of Law and Technology* 377, 2015, 382.

mondo «inondato di sensori» [5] che registrano movimenti, suoni, luci, potenziali elettrici, temperatura, umidità, posizione; un mondo popolato da "oggetti incantati"[6], 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 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 prenderla[7]; forchette intelligenti che monitorano quando e quanto velocemente si mangia[8]; tappeti destinati alle case degli anziani che misurano i loro passi allo scopo di prevenire cadute e fratture[9]…: il novero degli oggetti che possono essere collegati a internet è limitato soltanto dalla fantasia degli inventori[10]. 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 casa[11]. 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

[5] E. Haber, *The Wiretapping of things*, 53 *U.C. Davis Law Review* 733 (2019), 748.

[6] «*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*) e successivamente ripresa da molti (a esempio, A. McEwen, H. Cassimally, *Designing the Internet of* Things, Hoboken, 2014, 16; nella letteratura italiana, G. Sartor, *L'intelligenza artificiale e il diritto*, Torino 2022, 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».

[7] V. *perma.cc/Y3D3-YT4U*.

[8] V. *perma.cc/W3S3-7KBK*.

[9] S. R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 *Northwestern University Law Review* 1153, 2011, scaricabile da https://scholar.law.colorado.edu/articles/177, 1168.

[10] M. Ashton, *Debugging the real world: robust criminal prosecution in the internet of things*, 59 *Arizona Law Review* 805, 2017, 808.

[11] A. Bianchini, *Always On, Always Listening: Navigating Fourth Amendment Rights in a Smart Home*, 86 *Geo. Wash. L. Rev. Arguendo* 1, 2018, 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*, 4 s.

può svelare qualcosa»[12].

2. 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 degli strumenti che ne fanno parte è passato attraverso tre stadi: il "corpo esterno", il "corpo interno", il "corpo fuso"[13]. 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 elettronici[14], 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)[15].

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 medico[16]; dispositivi adoperati dai diabetici per monitorare il livello di glucosio[17]; reggiseni che registrano piccole variazioni della temperatura, che

[12] S.R. Peppet, *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, 119.
[13] A.M. Matwyshyn, *The internet of bodies*, 61 *William and Mary Law Review 77,* 2019, 94.
La tripartizione è ripresa da C. Amato, *Internet of Bodies: Digital Content Directive, and beyond*, 12 *Journal of Intellectual Property, Information, Technology, and Electronic Commerce Law* 181, 2021, 183 s.
[14] Q. Hardy, *Big Data in Your Blood*, in *The New York Times,* 7.9.2012.
[15] 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*, https://electronics.howstuffworks.com/gadgets/fitness/fitbit.htm; Q. Hardy, *Big Data in Your Blood*, cit.; S. R. Peppet, *Regulating the Internet of Things*, cit., 93 s.
[16] V. *perma.cc/874Z-8H65*.
[17] 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*, 222.

a loro volta possono indicare un tumore agli stadi iniziali[18]; e così via. Alcune aziende specializzate offrono un "ecosistema" chiuso di dispositivi e servizi[19]: lo stesso brand può offrire lo smartwatch, lo sfigmomanometro connesso, la bilancia intelligente, il termometro 2.0, il materassino che misura la qualità del sonno e una sorta di conchiglia da applicare 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 trasgressore[20].

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 gestititi da un'app per cellulare; suture dotate di sensori che raccolgono dati sulle ferite in via di guarigione…[21].

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

[18] V. *perma.cc/EG6E-MUYA*.
[19] È il *core business* di Withings, compagnia che costruisce esclusivamente apparecchi per la telemedicina personalizzata.
[20] Il dispositivo si chiama Pavlok: *shop.pavlok.com*.
[21] A.M. Matwyshyn, *The internet of bodies*, cit., 103 s.

tenuta del diritto alla *privacy*[22]. In qualche misura essi mescolano il mondo fisico e biologico con quello digitale[23]: corpi e bit si fondono, la carne umana s'intreccia con *hardware*, *software* e algoritmi[24], il confine fra uomo e macchina si fa sfumato[25]. Tutto questo permette di raccogliere dettagli intimi della vita degli utenti[26]; 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 biometrica[27].

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 medico[28].

---

[22] M.M. Christovich, *Why Should We Care What Fitbit Shares - A Proposed Statutory Solution to Protect Sensative Personal Fitness Information*, 38 *Hastings Communication and Entertainment Law Journal* 91, 2016, 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 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 *Boston University Law Review*, scaricabile da *papers.ssrn.com/sol3/papers.cfm?abstract_id=4693396*, 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, https://jolt.richmond.edu/jolt-archive/v21i2/article6.pdf, 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, 75 s.
[23] C. Amato, *Internet of Bodies*, cit., 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, 221; K.E. Tapp, *Smart devices won't be "smart" until society demands an expectation of privacy*, 56 *U. Louisville L. Rev.* 83, 2017, 86.
M. Ashton (*Debugging the real world*, cit., 809) parla d'un «portale fra il cyberspazio e il mondo reale».
[24] A.M. Matwyshyn, *The internet of bodies*, cit., 80.
[25] M. Swan, *Sensor Mania*, cit., 248.
[26] K. Saphner, *You Should Be Free to Talk the Talk and Walk the Walk: Applying Riley V. California to Smart Activity Trackers*, in *Minnesota Law Review*, 2016, 1715 s.
[27] S. R. Peppet, *Regulating the Internet of Things*, cit., 93 s.
[28] D. Gray, *A right to go dark*, 72 *Southern Methodis University Law Review* 621, 2019, 655 s.

Gli apparecchi sono onnipresenti: «*always on, always sensing, always collecting, and always communicating*» [29], diventano parte di noi; hanno accesso 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 psiche [30]. 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 case[31]; ma l'*internet of bodies* si spinge più in là: apre una finestra che s'affaccia all'interno del corpo umano.

3. 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

[29] Così A.D. Thierer, *The internet of things*, cit., 60. In seguito l'immagine è stata ripresa da A. Bianchini, *Always On, Always Listening*, cit.
[30] D. Gray, *A right to go dark*, cit., 653 s., secondo il quale acquisire i dati registrati dai *wearables* sarebbe in contrasto con il V emendamento della costituzione statunitense.
[31] FTC Staff, *Internet of things* (report dal workshop su: *The Internet of Things: Privacy and Security in a Connected World,* 19.11.2013), in *ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf*, 17

ma di condividere se stessi come modo per costruire un'identità. Qualcuno parla al riguardo di "autosorveglianza"[32]; qualcun altro, di "sorveglianza partecipativa"[33].

Sono riflessioni suggestive, che stanno riscuotendo molto successo[34] 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 esiste[35]. 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 informazioni[36]. Proprio per questo, qualche anno fa negli Stati Uniti scoppiò uno

[32] J. Kang, K. Shilton, D. Estrin, J. Burke, M. Hansen, *Self-surveillance Privacy*, 97 *Iowa Law Review* 809, 2012, 812 s.

[33] A. Albrechtslund, *Online Social Networking as Participatory Surveillance*, in *First Monday*, 2008, scaricabile da *researchgate.net/publication/220166794_Online_Social_Networking_as_Participatory_Surveillance*, 5 s.

[34] 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*, 13.1.2015; M.M. Christovich, *Why Should We Care*, cit., 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 *Catholic University Journal of Law and Technology* 89, 2020, 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 *West Virginia Law Review* 891, 2017, 893; Id., *I Spy: The New Self-Cybersurveillance and the "Internet of Things"*, 72 *Washington & Lee Law Review* 1459, 2015, 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, 103. V. pure – ma in prospettiva non perfettamente coincidente – N.M. Richards, *The dangers of surveillance*, 2017, 126 *Harvard Law Review* 1934, 2013.

[35] J. Kang-K. Shilton-D. Estrin-J. Burke-M. Hansen, *Self-surveillance Privacy*, cit., 825 s.

[36] 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*, 24.12.2014; A. Sui, W. Sui, S. Liu, R. Rhodes, *Ethical considerations for the use of consumer wearables in health research*, 9 *Digital Health* 1, 2023, 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. United States,* 29 *William & Mary Bill of Rights Journal* 533, 2020, 550; B. Turner, *When Big Data Meets Big Brother*, cit., 392.

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 Google[37].

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 dispositivo[38]; quando si riesce a trovarla, spesso è incompleta o sibillina[39], soprattutto per quanto riguarda gli usi che, dei dati ceduti, possono essere fatti[40]; 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 raccolti[41].

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 raccolti[42]. 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 concorrenza[43].

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"[44]. Può

---

[37] N. Chauriye, *Wearable Devices as Admissible Evidence: Technology is Killing Our Opportunity to Lie*, 24 *Catholic University Journal of Law & Technology* 495, 2016, 503 e 526.

[38] G. Johnson, *Privacy and the Internet of Things: Why Changing Expectations Demand Heightened Standards*, 1 *Washington University Jurisrudence Review* 345, 2019, 354; S.R. Peppet, *Regulating the Internet of Things*, cit., 139 s.; Z. Takhshid, *Wearable AI,* cit., 13.

[39] 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*, 28 s.)

[40] J. Kang, K. Shilton, D. Estrin, J. Burke, M. Hansen, *Self-surveillance Privacy*, cit., 824 s.

[41] M.M. Christovich, *Why Should We* Care, cit., 107 s.

[42] Z. Hussain, *Weary of Wearables: IP, Privacy, and Data Security Concerns*, in *lawpracticetoday.org*, 14.1.2016; G. Johnson, *Privacy and the Internet of Things*, cit., 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 product*»); A. Rodis, *Fitbit data and the fourth* amendment, cit., 545 s.; A.D. Thierer, *The internet of things*, cit., 29; M. Swan, *Sensor Mania*, cit., 231.

[43] J. Kang-K. Shilton-D. Estrin-J. Burke-M. Hansen, *Self-surveillance Privacy*, cit., 824 s.

[44] F. Nicolai, M.-H. Maras, J. Trautmann, J. Schneider, *When objects betray you: the Internet of Things and the*

capitare che il datore di lavoro richieda d'indossare un badge di tracciamento della posizione[45]; che un'impresa di trasporti si attenda che i suoi autisti indossino indumenti o dispositivi che monitorano il loro stato d'allerta[46]; 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 doloso[47], 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'interessato[48]; ci stiamo dirigendo verso una società della sorveglianza ma non lo facciamo con piena consapevolezza: «camminiamo come sonnambuli»[49].

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'è[50].

Per molti decenni s'è pensato, sull'una e sull'altra sponda dell'oceano, che le informazioni spontaneamente rivelate ad un terzo non potessero godere di particolare protezione da parte dell'ordinamento, perché l'interessato avrebbe spontaneamente abdicato alle sue aspettative di riservatezza[51]; quest'idea è entrata in crisi e da più parti

---

privilege against self-incrimination, 33 *Information & Communications Technology Law* 255, 2024, scaricabile da https://publications.cispa.de/, 14 s.

[45] A.M. Matwyshyn, *The internet of bodies*, cit., 101

[46] A.M. Matwyshyn, *The internet of bodies*, cit., 83 s.

[47] *Infra*, Parte I, § 5.

[48] Nell'impostazione di O.S. Kerr, *Implementing Carpenter. The digital fourth amendment*, 14.12.2018, scaricabile da https://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., 891 s., il quale, con un curioso ossimoro, parla d'un «*consensual and inadvertent tool that undermines privacy protection*».

[49] M.M. Christovich, *Why Should We Care*, cit., 105.

[50] B. Turner, *When Big Data Meets Big Brother*, cit., 422 s.; C. Slobogin, *Subpoenas and Privacy*, 54 *DePaul Law Review* 805, 2005, 829.

[51] 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

s'averte 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 parte[52]: «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»[53].

4. Abbiamo visto che l'*internet of bodies* comprende una gamma di congegni ampia e variegata. Qui non è possibile passarli in rassegna tutti, ma 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 digitali[54]. I dati vengono temporaneamente stivati all'interno degli apparecchi ma sono destinati ad essere sovrascritti in tempi abbastanza rapidi (qualche giorno)[55], perché di solito i *wearables* hanno una memoria

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 rinvengono 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, 21.4.2022, 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., 16.5.2008, 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, 20.5.1997, n. 5894, Bottaro ed altri, in *C.e.d.*, rv. 207931 – 01); sono, tutte, prese di posizione riconducibili ad un'idea analoga alla *third party doctrine*.

[52] B. Turner, *When Big Data Meets Big Brother*, cit., 38, 425 e 433 s.

Riflessioni analoghe in A. Bianchini, *Always On, Always Listening*, cit., 4 s.; M.M. Christovich, *Why Should We Care*, cit., 95 s.; C. Del Rosso, C.M. Bast, *Protecting Online* Privacy, cit., 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, 531 s.; I. Friedland, *Drinking from the Fire Hose*, cit., 909 s.; E. Haber, *The Wiretapping of things*, cit., 757; M. Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 *Harvard Law Review* 1790, 2022, 1791 s.

Per un'appassionata difesa della *third party docrine* v. tuttavia O. Kerr, *The Case for the Third-Party Doctrine*, 107 *Michigan Law Rew* 561, 2009.

[53] Così N. Gorsuch, nella *dissenting opinion* a Carpenter v. United States, 585 U.S. 296, 2018.

[54] S.R. Peppet, *Regulating the Internet of Things*, cit., 98; v. anche A.H. Raymond, S.J. Shackelford, *Jury glasses: wearable technology and its role in crowdsourcing justice*, 17 *Cardozo Journal of Conflict Resolution* 115, 2015, 121.

[55] 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.

ridotta[56].

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 cavo[57], scaricano i dati sull'app che a sua volta li riversa nel *cloud*[58]; 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 nutrizione[59]. 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 luoghi[60]; e la disciplina che ne regola l'acquisizione cambia ogni volta, a seconda della fonte da cui la prova viene ricavata.

5. 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 eccezione[61].

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 professione[62].

Kendall, *"Outrunning" the fourth amendment: a functional approach to searches of wearable fitness tracking devices*, 43 *S. Illinois University Law Journal* 333, 2019, 336 s.

[56] K. Saphner, *You Should Be Free to Talk the Talk*, cit., 1717.

[57] M. Ashton, *Debugging the real world*, cit., 808; M. Swan, *Sensor Mania*, cit., 220.

[58] J. Evans, K. Ringrose, *From Fitbits to Pacemakers: Protecting Consumer Privacy and Security in the Healthtech Age Security in the Healthtech Age*, 68 *Cleveland State Law Review "Et Cetera"* 1, 2019, 2.

[59] J. Kang, K. Shilton, D. Estrin, J. Burke, M. Hansen, *Self-surveillance Privacy*, cit., 813 s.

[60] F. Nicolai-M.H. Maras-J. Trautmann-J. Schneider, *When objects betray you*, cit., 17 s.

[61] Cfr. A.G. Ferguson, *The "Smart" Fourth Amendment*, 102 *Cornell Law Rev*. 547, 2017, 560 s.; N. Shakoory, *Wearables: your next trial witness?*, in *San Francisco Daily Journal*, 10.12.2014.

[62] Cfr. E.S. Brotten, *"Every Move You Make*, cit.; N. Chauriye, *Wearable Devices as Admissible Evidence*, cit., 597; S. Gibbs, *Court sets legal precedent with evidence from Fitbit health tracker*, in *theguardian.com*, 18.11.2014; S.

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 trascinata in bagno e violentata; 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*[63].

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 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 assicurativa[64].

Richard Dabate racconta alla polizia che, dopo essere tornato a casa, ha dovuto affrontare un intruso; la moglie Connie, a sua volta, era rincasata 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.

Griffiths, *Fitbit data is now being used in COURT: Wearable technology is set to revolutionise personal injury and accident claims*, in *dailymail.co.uk*, 17.11.2014; P. Olson, *Fitbit Data Now Being Used In The Courtroom*, in *forbes.com*, 17.11.2014.

[63] Commonwealth v. Risley, Criminal Docket: CP-36-CR-0002937-2015.
Sul caso Risley si vedano N. Chauriye, *Wearable Devices as Admissible Evidence*, cit., 495 s.; C. Coble, *Can Your Fitbit Data Be Used Against You in Court?*, in *findlaw.com*, 21.3.2019; 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*, 28.6.2015; M. Snyder, *Police: Woman's fitness watch disproved rape report*, *abc27.com*, 19.6.2015.

[64] *Man's pacemaker data used against him in arson case*, in *cbsnews.com/news/mans-cardiac-pacemaker-data-led-to-arson-charges*, 11.2.2017; A.E. Draft, *Pacemakers, Fitbits, and the fourth amendment*, cit., 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 *International Journal of evidence and 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/*, 5.4.2018.

Richard Dabate verrà condannato per l'omicidio della moglie[65].

Come spesso capita quando si tratta d'usare nel processo penale nuovi ritrovati tecnologici[66], gli Stati Uniti aprono la strada, ma ben presto la tendenza contagia altri ordinamenti; dati estratti da *wearables* sono usati come prova in Germania[67], nel Regno unito, in Australia[68]; vengono usati per incriminare e condannare, ma anche per scagionare[69]. E fanno la loro comparsa anche nei palazzi di giustizia italiani. In una vicenda che ha attirato molto l'attenzione della stampa locale[70], 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

[65] N. Black, *Fitbit data, other digital evidence used by prosection in murder case*, in *legalnews.com*, 29.5.2017; C. Brondoni, *Smascherare un killer con il Fitbit*, *wired.it/article/fitbit-omicidio-prova-dabate/*, 4.8.2024; D. Cassens Weiss, *Murdered woman's Fitbit data inconsistent with husband's story, police say*, in *abajournal.com*, 25.4.2017; A. Rodis, *Fitbit data and the fourth amendment*, cit., 534 s.; D.A. Stein, *The Fitbit Murder and Our New Digital Witnesses*, in *goldmandefense.com/fitbit-murder-new-digital-witnesses/*; N. Wetsman, *Behind the expert testimony in the "Fitbit murder" trial*, in *theverge.com*, 12.5.2022.
Il mandato d'arresto di Dabate è reperibile in *documentcloud.org/documents/3678236-Dabate-Arrest-Warrant.html.*

[66] A. Camon, *Il cacciatore di Imsi*, in *AP* 2020, 177.

[67] 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,* 20.4.2018.

[68] 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 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 https://gizmodo.com, 2.4.2018.
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. Journal* 506, 2019.

[69] 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., 546 s.

[70] Cfr., per esempio, A. Baccaro-L. Muleo, *Giampaolo Amato, l'ex medico della Virtus incastrato dallo smartwatch: «dormivo», l'orologio dice che era sveglio*, in https://corrieredibologna.corriere.it, 28.9.2023; G. Canè, *Quando lo smartwatch diventa la "prova" di un delitto: l'omicidio di Bologna e i casi precedenti*, in *corriere.it*, 28.9.2023; M. Madonia, *Il medico Giampaolo Amato e la condanna all'ergastolo: «Per me vuol dire morire in carcere, non sono un mostro»*, https://corrieredibologna.corriere.it, 17.10.2024.

significativi a sostegno dell'ipotesi accusatoria»[71].

Pubblici ministeri e difensori di tutto il mondo si stanno accorgendo della minera d'oro che si trova al polso delle parti processuali[72]; i *wearable* sono una «scatola nera del corpo umano»[73], un esercito di piccole spie[74] pronte a testimoniare contro, o a favore, dei propri utenti[75].

Parte II – Intanto, in Europa

1. Gli Stati Uniti, dunque, stanno affrontando il cosiddetto *translation problem*[76]. La grammatica del pubblico potere cristallizzata nella Costituzione – 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 messaggi[77].

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 subdolo[78].

---

[71] Trib. Bologna, 14.1.2025, Amato, inedita, 90.
[72] J.G. Browning, L. Angelo, *The changing practice of law*, cit., 507.
[73] E.S. Brotten, *Every Move You Make*, cit.
[74] A.G. Ferguson,*The Internet of Things and the Fourth Amendment of Effects*, 104 *Cal. Law Rev.* 807, 2016, 818.
[75] P. Augustine, *Wearable Evidence: Why the Pennsylvania Judiciary Should Require a Warrant to Search Wearable Technology*, 17 *Journal of Technology, Law and Policy*, *tlp.law.pitt.edu/ojs/tlp/article/view/197*, 2; A.N. Kitchen, *Smart devices and criminal investigations*, cit., 12 e 45; K. Saphner, *You Should Be Free to Talk the Talk*, cit., 1691.
[76] L'efficace espressione è di M. Washington-N. Richards, *Digital Civil Liberties and the Translation Problem*, in D.K. Brown-J. Turner-B. Weisser (a cura di), *The Oxford Handbook of Criminal Process*, Oxford 2019, 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*, vol. 27, 2019, 267-291.
[77] Da una premessa simile muove l'analisi di O.S. Kerr, *The Digital Fourth Amendment*, Oxford 2025.
[78] È la premessa narrativa di un romanzo che, non a caso, è oggi acclamato come un classico moderno: P.K. Dick, *Ubik,* 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

Non siamo in una situazione identica[79], 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.

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 soluzioni[80]. 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 Cedu); 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 famigliare, 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

riservatezza dei pensieri dei propri clienti grazie alle capacità dei propri impiegati, gli inerziali, anti-talenti in grado di azzerare il campo generato dai telepati.

[79] 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*, 4.3.2021. 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*, 16.9.2014, 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.

[80] 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*, Milano 2025, 4.

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 personali [81] (d'ora innanzi: GDPR), cui si sommano la direttiva "e-Privacy" [82], il Regolamento sul trattamento dei dati da parte delle istituzioni europee[83], il Data act[84] 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»[85].

L'insieme di norme che riguarda più da vicino l'accertamento è senza dubbio l'ultimo che, insieme all'art. 8 Cedu, 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 fini. Per farlo, partiremo dai capisaldi stabiliti dal GDPR per il trattamento dei dati personali; passeremo infine alle cautele che l'art. 8 Cedu e la LED dettano alle forze dell'ordine.

[81] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27.4.2016, entrato in vigore nel 2018.
[82] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12.7.2002 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 28.1.2020, disponibile alla pagina *edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_en*.
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), 10.1.2017 (COM/2017/010).
[83] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio del 23.10.2018, cit.
[84] Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13.12.2023, 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 12.9.2025.
[85] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27.4.2016 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 DQ 2008/977/GAI del Consiglio.

2. Lo strumento normativo da cui conviene partire è il Regolamento generale sulla protezione dei dati, che costituisce l'architrave normativa di ogni forma di raccolta e lavorazione di informazioni personali. Esso 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 successive[86]: 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 appare [87]. 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 benestare di facciata che di fatto sposta l'autonomia decisionale e il controllo dei dati dall'utente all'azienda digitale[89]. 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 autodeterminarsi[90], di prendere scelte meditate su di sé e sulla condivisione delle

[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 2020, e in particolare il contributo di C. De Terwagne, *Article 5. Principles relating to processing of personal data*, *ibidem*, 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*, 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*, 16.9.2024, disponibile alla pagina https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_it.pdf, 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, 19.6.2025, 2.

[90] Il lessico eurounitario deve molto alla pionieristica elaborazione tedesca della *Informationelle Selbstbestimmung*: il diritto all'autodeterminazione informativa postulato prima dalla dottrina tedesca e poi

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 stretto[93] – quelli, cioè, che consentono di identificare univocamente una persona

affermato dalla Corte costituzionale tedesca come un corollario della dignità umana: BVerG, I senato, 15.12 1983, 1 BvR 209/83, § 146 ss. Per un approfondimento dogmatico v. K.M. Linzbach, *Additiver Grundrechtseingriff und informationelle Selbstbestimmung. Grundrechtsdogmatik als Legitimationsproblem*, Tübingen 2025.

[91] CEPD, *Linee-guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, versione 1.1, adottate il 4.5.2020, 5, disponibili alla pagina *edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_it*.

[92] *Ivi*, 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*, 17.4.2024, 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. Campazas-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. Ahlert-C. Brown-M. Birge-A. Gibbs, *Electrocardiogram-based biometrics for user identification – Using your heartbeat as a digital key*, in *Journal of Electrocardiology*, vol. 80, 2023, 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

– ma di certo produce informazioni relative alla salute del soggetto che indossa l'apparecchio[94]. Anche a loro, quindi, si applica il divieto stabilito dall'art. 9 GDPR[95].

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 autorizzati. 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 esplicite[96]. Il dispositivo, insomma, deve essere pensato per funzionare

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*, 12.2.2021, disponibile alla pagina *health.ec.europa.eu/publications/assessment-eu-member-states-rules-health-data-light-gdpr_en*, 14 e 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., 218 s.

[96] Approfondiremo tutte le espressioni al § successivo.

al meglio, con il minimo impatto possibile sulla riservatezza[97]. 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* acquistato[99].

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

[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, 20.10.2020, 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 16.2.2022. 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 v. *Your Fitbit is useless – unless you consent to unlawful data sharing*, 31.8.2023, disponibile alla pagina https://noyb.eu/en/your-fitbit-useless-unless-you-consent-unlawful-data-sharing.

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 specificazioni 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. 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 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 apparecchi[100]. 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 carpiti 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 smettere di rilevare l'informazione[101]. 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

[100] Gruppo di lavoro articolo 29 per la protezione dei dati, *Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti*, cit., 22 s.
[101] La *privacy policy* qui descritta è consultabile alla pagina: *apple.com/legal/privacy/data/en/health-app.*

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 soggetto[102]. 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 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

[102] S. Quadir-N.S. Kahn-G. Anjum-N. Uddin, *A wearable sensors dataset for stress & boredom associated activity recognition*, in *Data in Brief*, vol. 54, 2024, n. 110550.

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 malintenzionati[103]. 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 perfetta[104], ma getta i semi da cui nascono le questioni più spinose per l'uso di quelle informazioni nel processo penale: le affronteremo a tempo debito[105].

4. 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

[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), 19.9.2025). 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., 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 co. 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, 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 13.9.2025. 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., 78.

[105] V. oltre, Parte III, § 3.

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 traumatica[106]. 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 Cedu, 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 eccessivamente compresso. Non è questa la sede per ripercorrere la giurisprudenza della Corte europea dei diritti dell'uomo sull'art. 8 in tutte le sue pieghe[107]; 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 recenti[108].

Il palinsesto ricalca le previsioni dell'art. 8 comma 2 Cedu 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».

[106] V. A. Lana, *Smartwatch gli salva la vita: chiama i soccorsi mentre lui è incosciente*, in *corriere.it*, 22.9.2019.
[107] Per un panorama completo v. Corte eur., *Guide on Article 8 of the European Convention on Human Rights*, 28.2.2025, disponibile al sito *ks.echr.coe.int*; Corte eur., *Guide to the Case-Law of the of the European Court of Human Rights. Data protection*, 31.8.2025, *ivi*.
[108] Le indicazioni della Corte eur. ci torneranno utili soprattutto nel chiederci come il giudice debba valutare la prova prodotta dal dispositivo indossabile: v. Parte III, § 11.

Il primo segmento consiste in un'analisi approfondita del quadro normativo nazionale[109]. 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 tirannia[110]. Il sistema dei contrappesi 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 strette[111]. 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 offuscarlo[112].

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,

[109] Val la pena ricordare che la Corte eur. 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 eur., 16.11.2021, *Särgava c. Estonia*, § 86.

[110] Corte eur., 25.6.1997, *Halford c. Regno Unito*, § 49. La Corte europea dei diritti dell'uomo 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 in quanto tale: Corte eur. GC, 4.12.2015, *Zakharov c. Russia*, § 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 eur., 13.2.2024, *Podchasov c. Russia*, cit., § 55.

[111] Corte eur., 4.7.2023, *Glukhin c. Russia*, § 83.

[112] Per un esempio recente c. Corte eur., 13.2. 2025, *Macharik c. Repubblica Ceca*, § 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 Cedu era stato pienamente rispettato, ma l'art. 8 Cedu no: la base legale era evidentemente troppo confusa per i requisiti di prevedibilità.

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 informazioni[113]: 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 richiesto[114]. 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 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. Il secondo gradino del test adottato dalla Corte europea dei diritti dell'uomo 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 Cedu; 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

[113] V. *infra*, Parte III.
[114] Per orientarsi nella valutazione, la Corte europea dei diritti dell'uomo 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).
[115] Corte eur., 28.11.2024, *Le Marrec c. Francia (dec.)*, § 78.
[116] Corte eur., *Glukhin c. Russia*, cit., § 89 («pressing social need» nella dicitura inglese); Corte eur, 30.5.2017, *Trabajo Rueda c. Spagna*, § 42 («besoin social emperieux» nelle sentenze in francese).

(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 sanitario[117]: 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 europea 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 considerato tutti gli interessi in conflitto, svolgendo una valutazione di proporzionalità adeguata[118].

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 commerciali[119]. 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 restringe[120]. 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

[117] Corte eur., 25.2. 1997, *Z. c. Finlandia*, § 95.

[118] In questo senso v. Corte eur., *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*, 3.9.2025.

[120] Corte eur., 4.6.2013, *Peruzzo e Martens c. Germania*, § 41; Corte eur. GC, 10.4.2007, *Evans c. Regno Unito*, § 77.

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.

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

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 congiunta[121]; sono però assai più numerosi i casi in cui le valutazioni si mantengono parallele. In materia di prove, la Corte europea 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 diritto[122]. 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 Cedu 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

[121] Corte eur., *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 Cedu: la ricca argomentazione relativa all'art. 6 Cedu 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 eur., *Yalçinkaya c. Turchia*, cit., § 303, 304 e 316.

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 Cedu sarebbe violato. Un secondo fattore che la giurisprudenza valorizza è la correttezza del procedimento probatorio. Il modo – conforme 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 condividerli o ritenerli infondati, non può invece ignorarli. Anche tale indicazione, lo vedremo, ci tornerà utile.

7. 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 trasposta in Italia con il d.lgs. 18.5.2018 n. 51. Prima della sua approvazione, il diritto eurounitario tutelava le informazioni raccolte dall'autorità giudiziaria soltanto nel momento in cui venivano trasferite all'estero[123]; il testo del 2016, invece, detta garanzie di *privacy* minime dirette alle autorità nazionali.

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

[123] Secondo alcuni commentatori, le norme previgenti (DQ 2008/977/GAI, del 27.11.2008, 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. Papakostantinou, *The New Police and Criminal Justice Data Protection Directive. A First Analysis*, in *New Jour. Eur. Crim. Law*, vol. 7, 2016, 8.

nell'ambito di un'indagine[124]. Una importante conferenza 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 attività[125]; 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 europea 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 riservatezza[126]. Lo stesso vale per il vincolo dell'apparecchio: se servisse per compiere accertamenti impossibili da svolgere sulla copia, lo si potrà trattenere[127].

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, assume grande rilievo nel campo degli

[124] Sull'estensione esatta della norma v. C. Jasserand, *Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?*, in *Computer Law & Security Rev.*, vol. 34, 2018, 154 ss.

[125] Europol's Data Protection Experts Network (EDEN), *Paradise Lost? Policing in the age of data protection*, 19-20.9.2019; 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*.

[126] 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: C.G.UE, 4.10.2024, C-548/21, *Bezirkshauptmannschaft Landeck*, § 69 ss.

[127] Come vedremo, l'ipotesi è forse più concreta per i *wearables* che per altri dispositivi: v. oltre, Parte III, § 5.

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 decisioni[128].

8. 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 salute [129] 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»[130].

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 godono 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

[128] Sul punto torneremo a breve: Parte III, § 10. 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 2024, 181 ss.

[129] 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».

[130] C.G.UE, 1.8.2022, 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.

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 severi[131]. Ogni tentativo d'accesso si deve quindi conformare alle garanzie dell'art. 10 LED[132]. 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»[133].

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'avverbio «solo», cui la Corte ha attribuito un senso forte: significa che le informazioni possono essere trattate in un numero necessariamente limitato di occasioni[134]. Ciò significa che la legge nazionale deve

[131] C.G.UE, 4.10.2024, C-548/21, cit.
[132] Sui riflessi della pronuncia nell'ordinamento italiano v. oltre, Parte III, § 6.
[133] La disposizione riproduce quasi testualmente la sua omologa, l'art. 10 direttiva 2016/680.
[134] C.G.UE, 4.10.2024, C-548/21, cit., § 108; [134] C.G.UE, 26.1.2023, C-205/21, cit., § 118.

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 italiano[135].

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 importante[136] 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'obiettivo[137].

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 concreto[138].

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 nette[139].

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

Parte III – Le regole per il processo italiano

1. L'informazione prodotta dai dispositivi indossabili, come abbiamo visto, non è una semplice rilevazione registrata e archiviata. Il dato è semmai frutto di una lunga

[135] Sul punto torneremo tra poco: v. Parte III, § 5.
[136] C.G.UE, 4.10.2024, cit., § 99
[137] [137] C.G.UE, 26.1.2023, 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.
[138] C.G.UE, 4.10.2024, cit., § 102.
[139] V. oltre, Parte III, § 6.

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 afferrare [140]. 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 in questa sezione: 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*? 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

[140] 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.

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 prodotto[141].

2. 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» [142]; 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.

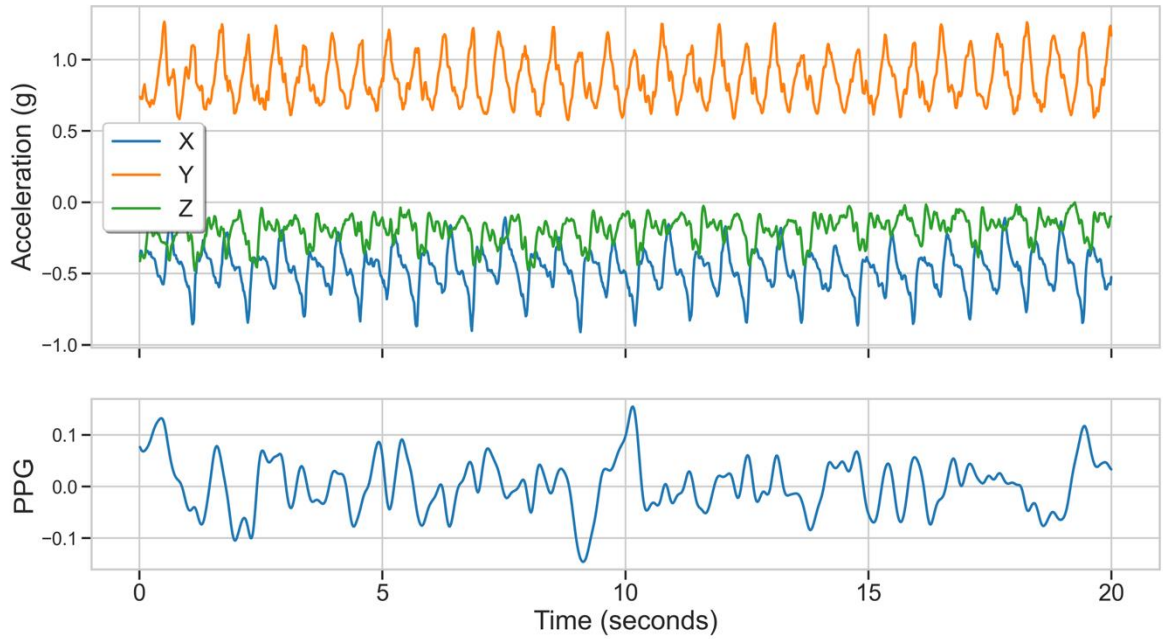
L'immagine che riportiamo, per esempio, contiene i segnali registrati da due sensori (l'accelerometro e il sensore ottico) di un dispositivo indossabile durante 20 secondi di camminata di un adulto sano. Osservando la rilevazione, una persona impreparata non riuscirebbe nemmeno a comprendere qual è l'attività osservata; ottenere informazioni vere e proprie – distanza percorsa, numero di passi, frequenza cardiaca – sarebbe impossibile senza l'aiuto di un tecnico.

Fig. 1 – Rilevazione di 20 secondi di camminata di un adulto sano effettuato con l'indossabile 'Empatica'

[141] V. *retro*, Sez. II, § 3.

[142] Questa la definizione del dizionario Sabini-Coletti.

[143] 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 '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*, vol. 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*, Vol. 50, 2024, n. 301804.



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 Cpp, delle perquisizioni (art. 147 comma 1-*bis* Cpp), dei sequestri (artt. 254, 254-*bis*, 259 Cpp; insomma: si tratta quasi 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 accennato[144], 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

[144] V. *retro*, Parte II, § 3.

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'accaduto[145]. 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 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 immodificabile e sottratte al ciclo incessante di scritture e cancellature.

[145] V. *retro*, Parte I, § 5.

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 piano[146].

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.

3. 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 contenitori diversi[147], 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 eccezioni[148], gli unici test di affidabilità che hanno dovuto superare sono quelli interni,

[146] Per alcuni esempi v. J.P. van Zandwijk-K. Lensen-A. Boztas, *Have you been upstairs?*, cit., 2 s.; J.P. van Zandwijk- A. Boztas, *The phone reveals your motion: Digital traces of walking, driving and other movements on iPhones*, *ivi*, vol. 37, 2021, 301170, 4 ss.

[147] La comunicazione tra dispositivi può causare duplicazioni di dati o marche temporali diverse, ma le informazioni rilevate restano le stesse.

[148] 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 *fda.gov*, 8.8.2018; e FDA, *Hypertension Notification Feature (HTNF)*, *ivi*, 11 e 12.9.2025

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 ospedaliero[149]. 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 basato sul *machine learning*[150]: 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

(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 *fda.gov*, 28.9.2022, 19.

[149] FDA, De Novo *Classification Request*, cit., 2.

[150] Lo si desume da FDA, *Hypertension Notification Feature*, cit.

saremmo d'accapo[151].

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 forense[152], 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 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 dovizia[153].

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 laboratorio[154]. La misurazione potrebbe essere falsata o addirittura impedita, per esempio, dal sangue che sporca il sensore, o da uno spostamento repentino del dispositivo[155].

---

[151] 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*.

[152] 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*, vol. 61, 2021, 205-211.

[153] 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*, 22.2.2025. 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*, vol. 37, 2021, n. 301170.

[154] Lo segnalano, per esempio, J.P. van Zandwijk-A. Boztas, *The phone reveals your motion*, cit., 10.

[155] M. Schlusche-K. Yen-S. Knödler-K. Feld, *Digitale Spuren in einem Mordprozess*, in *Rechtsmedizin*, vol. 35, 2025,

4. 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 semplice[156]. Questo spiega perché molti studiosi statunitensi si stiano interrogando sulla disciplina applicabile all'intercettazione delle trasmissioni fatte da questi strumenti[157].

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 Cpp si prestino ad abbracciare anche lo scambio d'informazioni fra apparecchi elettronici; pur con molte incertezze, la giurisprudenza è al riguardo abbastanza possibilista[158].

Il mezzo sarebbe senz'altro efficace e rispetterebbe le garanzie che esige la Corte di giustizia per il trattamento dei dati sensibili[159]. 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 possibile[160].

5. Il modo più facile per acquisire le informazioni che servono è porre l'apparecchio

448.

[156] 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., 563 s.; P. Roberts, *BitDefender Finds Phone to Smart Watch Communications easy to Snoop*, in securityledger.com, 10.12.2014.

[157] E. Haber, *The Wiretapping of things*, cit., 748 s.; G. Johnson, *Privacy and the Internet of Things*, cit., 370; A.N. Kitchen, *Smart devices and criminal investigations*, cit., 49 s.; A.G. Ferguson, *The Internet of Things*, cit., 807 s.; Id., *The "Smart" Fourth Amendment*, cit., 549 s.

[158] Analisi della questione e citazione di precedenti in A. Camon, *I confini mobili delle intercettazioni*, cit., 9 ss.

[159] V. *retro*, Parte II, § 8.

[160] Avvertono del pericolo anche M. Schlusche-K. Yen-S. Knödler-K. Feld, *Digitale Spuren in einem Mordprozess*, cit., 449 riferendosi al problema dell'interpretazione dei dati in un contesto forense.

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 persona[161]. La memoria del *wearable*, però, è limitata: non contiene l'archivio particolarmente 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 vittima[162].

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 processo[163], 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 Cpp). È disposto con decreto motivato dell'autorità giudiziaria (art. 253 Cpp) – 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 Cpp).

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

[161] M. Bicciato, *Femminicidio Giada Zanola, il giallo del telefonino: dopo 86 giorni resta introvabile*, in *corriere.it*, 25.8.2024. Il dibattimento è tuttora in corso presso la Corte d'Assise di Padova.
[162] 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: Parte III, § 9.
[163] J.P. van Zandwijk-A. Boztas, *Digital traces and physical activities: opportunities, challenges and pitfalls*, in *Science&Justice*, vol. 63, 2023, 370 s.

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 europea dei diritti dell'uomo[164], 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 della «totalità dei messaggi, filmati e fotografie ivi contenuti», il decreto è nullo perché il sacrificio per i diritti del singolo sarebbe ingiustificato[165]. 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"[166]. 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 indipendente[167].

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

[164] V. sopra, Parte II, § 5.
[165] Questa la conclusione di Cass., Sez. VI, 26.11.2025, n. 38331, in *italgiure.giustizia.it/sncass/*, cui si rinvia anche per la ricostruzione del complesso iter giurisprudenziale che ha portato all'approdo.
[166] V. *retro*, Parte II, § 8.
[167] Questo, in breve, il precipitato di C.G.UE, 4.11.2024, *Bezirkshauptmannschaft Landeck*, cit.

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 pubblica «secondo le specifiche regole dettate dal legislatore idonee a garantire anche i diritti dell'indagato»[168]. 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'altro[169]. Per quanto autonomo, non si può chiedere al pubblico ministero di essere terzo rispetto a sé stesso[170].

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 giudice[171]; 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 Cpp, 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'indagato[172]. Nemmeno questo equilibrio sembra soddisfacente, non

[168] Cass., Sez. V, 28.1.2025, n. 8376, in *C.e.d.*, n. 287976-01.
[169] C.G.UE, 4.11.2024, *Bezirkshauptmannschaft Landeck*, cit., § 103.
[170] 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»: C.G.UE, 2.3.2021, C-746/18, *Prokuratuur*, § 54.
[171] Cass., Sez. VI, 1.4.2025, n. 13585, in *C.e.d.*, n. 287867-01, anche in *www.sistemapenale.it*, 19.5.2025, 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)*.
[172] Cass., Sez. VI, 1.4.2025, n. 13585, in *C.e.d.*, n. 287867-02.

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.

6. 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* Cpp intitolato «sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviata e ricevuta»[173]. 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 giudicante 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 irripetibile[174]; 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

[173] Camera dei deputati, Proposta di legge approvata dal Senato della Repubblica il 10.4.2024 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*.

[174] 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 Cpp 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, 27.11.2020, 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 *CP* 2012, 441 e ss.).

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 2025[175], l'odierno articolo 6 è dedicato esattamente 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. 51/2018 e del codice di procedura penale così da adeguarli alla sentenza *Bezirkshauptmannschaft Landeck*, espressamente citata nell'articolato[176]. 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 Cpp, 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 Cpp. 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.

7. 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

[175] 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 3.12.2025, «Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2025», Atto Senato 1737, XIX legislatura, disponibile al sito *senato.it*.
[176] Camera dei deputati, *Dossier sulla legge di delegazione europea 2025*, 1.12.2025, disponibile al sito *camera.it*, 57 s.

accede tramite una procedura di poco diversa dall'ordinario. Gli investigatori potrebbero inoltrare alle aziende una richiesta di consegna dei dati necessari (art. 248 Cpp). Se venissero prodotti, non ci sarebbe bisogno di utilizzare poteri coercitivi; altrimenti si potrebbe ricorrere all'art. 254-*bis* Cpp 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»[177]: godono di possibilità e risorse che alcuni stati sovrani possono solo invidiare[178], 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,

[177] Le espressioni sono di S. Cassese, *I giganti del digitale e gli Stati*, in *corriere.it*, 16.4.2024.
[178] 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*, 14.12.2025.

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 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* Cpp 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 meno[179].

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)[180], 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'11.12.2025[181]. 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 ordini[182]. La direttiva 2023/1544 e il d.lgs. 216/2025 obbligano i prestatori di servizi a indicare uno «stabilimento designato» o un «rappresentante legale» in uno o più paesi dell'Unione europea (art. 4 d.lgs.

[179] 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, 96 ss.

[180] Regolamento 2022/2065 del Parlamento europeo e del Consiglio del 19.10.2022 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, 2024; Hofmann-B. Raue (a cura di), *Digital Services Act. Article-by-Article Commentary*, Baden-Baden 2025.

[181] Comunicato stampa del Consiglio dei ministri n. 151, in *governo.it*, 11.12.2025.

[182] L'art. 3 comma 2 d.lgs. 30.12.2025 n. 216 esime i *provider* italiani che prestano servizi esclusivamente in Italia: per loro bastano gli artt. 248 e 254-*bis* Cpp.

216/2025) [183] . Essi si dovranno occupare della «ricezione, dell'ottemperanza e dell'esecuzione» degli ordini (art. 3 comma 2 d.lgs. 216/2025). 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. 30.12.2025 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. 215/2025 ne disciplina due versioni: una destinata all'ordinamento nazionale, cristallizzata nell'art. 263-*bis* Cpp (art. 9 comma 3 d.lgs. 215/2025); l'altra rivolta alle imprese che si trovano all'estero (art. 3 d.lgs. 215/2025). 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 categorie[184]: 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.

[183] 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. 216/2025); resta quindi esclusa la Danimarca, che non ha partecipato all'adozione degli atti normativi (v. considerando n. 101 del regolamento 2023/1543).
[184] Sul punto, il d.lgs. 215/2025 opera un rinvio diretto alle definizioni del dell'art. 3 regolamento 2023/1543.

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 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 sbloccato[185]. 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. 215/2025stabilisce 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.

8. 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 internet[186]. Sul piano giuridico, come abbiamo visto, anche

[185] La quantità degli elementi dipende dalle impostazioni di condivisione dell'utente e dallo spazio di memoria che ha disposizione nel *cloud*.

[186] 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 use of fake accounts*, in *thegurdian.com*, 18.11.2021. Per una ricostruzione v. Congressional Research Service, *Law Enforcement and Technology: Using Social Media*, in *crsreports.congress.gov*, R47008, 11.1.2022; R. Levinson-Waldman, *Principles for Social Media Use by Law Enforcement*, in *brennancenter.org*, 7.2.2024. Il punto

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* Cpp.

9. 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 persona[187]. 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 sua[188]. Quel dato, probabilmente, 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

meriterebbe un approfondimento, ma ci porterebbe probabilmente troppo lontano.

[187] 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.

[188] M. Totaro, *Lo smart watch lascia l'Sos: decine di soccorritori lo cercano per ore nei boschi, ma dormiva a casa*, in *repubblica.it*, 17.8.2025.

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 rotolo di carta igienica o addirittura una banana[189].

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'edificio[190]. 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 sottostimato[191]. 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 sicurezza[192].

Poniamo di aver superato anche questo ostacolo: resta il dilemma dell'affidabilità delle informazioni. La verifica soffre di tutti i limiti che 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.

---

[189] V. la deliziosa fotografia in M. Schlusche-K. Yen-S. Knödler-K. Feld, *Digitale Spuren in einem Mordprozess*, cit., 448, che mostra un indossabile mentre comunica i valori del battito di una banana lievemente tachicardica.
[190] Per un esempio in questo senso, v. J.P. van Zandwijk-A. Boztas, *Digital traces and physical activities*, cit., 372 s.
[191] M. Schlusche-K. Yen-S. Knödler-K. Feld, *Digitale Spuren in einem Mordprozess*, cit., 447.
[192] *Se si vuole pogare è meglio spegnere lo smartwatch*, in *ilpost.it*, 15.6.2025.

Un caso tedesco può aiutarci a chiarire il punto[193]: 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 suppore 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 cardiaca[194], 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 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.

[193] L'indagine è riportata nel dettaglio in M. Schlusche-K. Yen-S. Knödler-K. Feld, *Digitale Spuren in einem Mordprozess*, cit., 446 ss.
[194] M. Schlusche-K. Yen-S. Knödler-K. Feld, *Digitale Spuren in einem Mordprozess*, cit., 447 ss.

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 irresponsabile[195]. 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 (proprietari), 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 due strumenti diversi, così da studiare le convergenze e le divergenze nell'esibizione del prodotto finito[196].

10. Davanti a uno scenario così complesso, come può orientarsi il giudice? È armato

[195] 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., 2.
[196] 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*, vol. 52, 2025, n. 301881, 8.

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 plausibili[197].

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 rimostranze 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 esistite[198].

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 europea suggeriscono la strada da percorrere[199]. 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.

[197] 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*, vol. 65, 2025, n. 101352.
[198] V. sopra, Parte II, § 6.
[199] Per l'esame dei precetti e i necessari riferimenti giurisprudenziali v. sopra, Parte II, § 6.

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 realtà[200]. 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.

11. 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 atto: il bisogno di limitare per legge l'accesso ai dati è stato avvertito in maniera trasversale: lo rintracciamo nella giurisprudenza della Corte europea dei diritti dell'uomo, 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

[200] Secondo J.P. van Zandwijk-A. Boztas, *Digital traces and physical activities*, cit., 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).

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 europea dei diritti dell'uomo. 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 *wearables*, 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.