EMILIANO GERMANI-LAURA FEROLA

IL *WEARABLE COMPUTING* E GLI ORIZZONTI FUTURI DELLA PRIVACY

SOMMARIO: 1. Lo sviluppo delle tecnologie informatiche e la diffusione dei *wearable devices* (dispositivi indossabili). — 2. Un primo fronte da esplorare: la privacy del fruitore. — 3. Gli aspetti di maggiore criticità. Alla ricerca di termini e modalità per preservare la sfera di riservatezza dei terzi. — 4. Costi e benefici del *wearable computing*: un equilibrio perfetto o uno sbilanciamento da livellare? — 5. Primi accorgimenti tecnici proposti dai produttori dei dispositivi indossabili a tutela della privacy. — 6. Le conseguenze delle innovazioni tecnologiche e il "percorso a ritroso" che dalla protezione dei dati personali (ri)porta alla valorizzazione della riservatezza. — 7. Non solo tecnologia, ma anche diritto per contemperare i diversi interessi in gioco.

1. Lo sviluppo delle tecnologie informatiche e la diffusione dei *wearable devices* (dispositivi indossabili).

Il mondo dell'informatica si sta proiettando verso la creazione di una nuova generazione di strumenti in grado di raccogliere ed elaborare in tempo reale dati e informazioni, rendendoli di uso comune e diffuso, i *wearable devices* [1]. Questi ultimi sono dispositivi miniaturizzati "indossabili" che si integrano con il corpo del fruitore, concepiti per interagire costantemente con chi li indossa, agevolare l'utente nelle sue azioni e consentirgli di accedere alle informazioni raccolte in qualsiasi momento [2].

* Il presente saggio è stato preventivamente sottoposto a referaggio anonimo affidato a un componente il Comitato Scientifico dei Referenti della Rivista secondo le correnti prassi nella comunità dei giuristi.

[1] Per un approfondimento in materia si rinvia ai lavori dell'ISWC-*International Symposium on Wearable Computers*, uno dei più importanti simposi internazionali che riunisce ogni anno esperti e ricercatori del mondo accademico, la cui prima edizione ha avuto luogo a Cambridge (USA) nel 1997. I contributi prodotti sono rinvenibili in *http://www.iswc.net/*.

[2] Appare sintomatica la carenza di una specifica dottrina sui dispositivi indossabili, e sulle criticità da essi generate, sotto un profilo squisitamente giuridico. Tra i pochi che si sono cimentati, sia pure sporadicamente, su tali aspetti, cfr. N. Bilton, *Disruptions: At Odds Over Privacy Challenges of Wearable Computing*, in *BITS - The New York Times*, 26 May 2013; L. Taylor-S. Annereau, *The Advent of Weara-*

Le peculiari caratteristiche che contraddistinguono tali dispositivi, non più relegati al pianeta dei *geek*, dei tecno-fanatici, evidenziano tutta la loro portata innovativa nelle relazioni interpersonali: in primo luogo, questi strumenti sono una diretta espressione dell'*ubiquitous computing* (o *ubicomp*), poiché non si limitano ad introdurre la tecnologia informatica in oggetti di uso quotidiano e diffuso, ma sono in grado di interagire tra loro e con l'ambiente circostante in modo automatico e, spesso, anche senza che l'utente ne sia pienamente consapevole.

Essi, inoltre, garantiscono la continua accessibilità alle informazioni, essendo sempre a contatto ed operando in simbiosi con il fruitore e, quindi, costantemente disponibili all'uso [3]. In questo si differenziano sia da altri *devices* mobili come *smartphone* e *tablet* — che, pur essendo sempre accesi, vengono trasportati in tasca oppure in una borsa, e devono essere quindi estratti ed attivati per essere utilizzabili —, sia dal tradizionale *personal computer*, che è solitamente acceso solo quando viene utilizzato e non sempre è trasportabile (un *pc desktop* è in postazione fissa), per cui è materialmente accessibile solo a determinate condizioni.

Ulteriore elemento distintivo dei dispositivi *wearable* deriva dalla possibilità di agire secondo una logica *multitasking* [4] in quanto il fruitore — diversamente dal *personal computer* o dallo *smartphone* — può facilmente utilizzarli ed impartire determinati comandi anche mentre svolge altre attività (come camminare, parlare, guidare, ecc.), senza doverle interromperle, ad esempio, per digitare un testo o un numero di telefono.

Un'altra rilevante caratteristica è quella della connettività: pur non costituendo un tratto di differenziazione specifico dei *wearable devices* rispetto ad altri dispositivi, risulta tuttavia essere un elemento funzionale imprescindibile, se non in alcuni casi il principale elemento caratterizzante le tecnologie indossabili, specificatamente concepite per aumentare le possibilità di interazione del fruitore con l'ambiente sia reale, sia virtuale.

Sotto un diverso profilo, strettamente legato al loro utilizzo, attualmente si individuano due macro-categorie fondamentali di

---

ble Technology and Accompanying Privacy and Data Protection Challenges, in *Global Law Watch - Bloomberg BNA*, 27 September 2013; H. Tsukayama, *Wearable tech such as Google Glass, Galaxy Gear raises alarms for privacy advocates*, in *The Washington Post*, 1 October 2013.

[3] In termini tecnici, tale singolare funzionalità comporta che il flusso del segnale da essere umano a computer e viceversa è attivo in modo continuo, al fine di fornire un'interfaccia utente costante.

[4] Ci si riferisce al c.d. *human multitasking*, cioè alla capacità dell'essere umano di eseguire diverse attività o compiti contemporaneamente, e, in ambito informatico, al c.d. *multitasking* o *multiprocessualità* informatica, vale a dire alla capacità di un sistema operativo di consentire ad un computer o altro strumento elettronico di eseguire più programmi contemporaneamente.

supporti *wearable*: quelli destinati ad impiego biomedicale e quelli "ad uso personale" (ludico, sportivo, ecc.).

I dispositivi *wearable* bio-medicali sono oggi sempre più diffusi e rappresentano una vasta tipologia di strumentazioni utilizzate per il monitoraggio a distanza e continuativo delle condizioni fisiche di pazienti a rischio o affetti da particolari patologie; essi si sono rivelati utili soprattutto nel campo della medicina sportiva, nel cui ambito vengono utilizzati per monitorare la *performance* degli atleti professionisti impegnati nei programmi di allenamento (es. fascette indossabili per la rilevazione della frequenza cardiaca, misuratori di distanza *GPS* nelle scarpe, ecc.).

Accanto a questi dispositivi, complici l'abbassamento dei costi e il crescente interesse del mercato nei confronti di supporti *mobile* sempre più versatili, sono stati perfezionati dispositivi con una vocazione più spiccatamente commerciale, utilizzabili dagli utenti nella normale vita quotidiana, nel tempo libero oppure come supporto ad attività pratiche di vario genere (lavoro, *fitness*, ecc.). Questo secondo ambito, meno tecnico ma molto più vasto, è quello che probabilmente sarà interessato nei prossimi anni dalla più forte diffusione dei dispositivi, non solo per il crescente numero di fruitori, ma anche per l'ampiezza di gamma dell'offerta [5].

Già oggi la tipologia dei supporti *wearable* è particolarmente nutrita [6] ed essi possono essere classificati in relazione all'oggetto in cui sono integrati o che, in alcuni casi, essi stessi integrano. Tra quelli di maggiore utilità si annoverano i c.d. accessori intelligenti (es. bracciali, occhiali, spille, ciondoli, ecc.), che racchiudono micro-telecamere in grado di raccogliere immagini, scattare fotografie, realizzare video e consentirne la pubblicazione sul *web* in tempo reale (es. nei profili personali dei *social network*). Se in tal caso vengono proposti per lo più come strumenti di *lifelogging* o *life caching* [7], in altri ambiti gli stessi dispositivi sono invece

[5] Secondo alcune stime di esperti del settore, il mercato dei dispositivi intelligenti indossabili supererà il miliardo e mezzo di dollari entro il 2014, con un rilevante incremento del fatturato rispetto ai circa 800 milioni dollari dell'anno precedente; si prevede, altresì, che la vendita di prodotti *wearable* crescerà di dieci volte, raggiungendo i 150 milioni di dispositivi entro il 2018. V. *Smart Wearable Device. Fitness, Healthcare, Entertainment & Enterprise 2013-2018*, Juniper Research, 2013, pp. 126.

[6] Sulla varietà dei dispositivi esistenti v. *Tecnologie indossabili: vademecum futuristico per stili di vita futuribili!*, in *http://www.solotablet.it/blog/approfondimenti/tecnologie-indossabili-wearable-technology*; S. Vettore, *Wearable computing, privacy e futuro dell'archivistica*, 2013, in *http://memoriadigitale.me/2013/08/20/wearable-computing-privacy-e-futuro-dellarchivistica/*; R. Saracco, *Wearable Computers: moda del futuro o tecnologia di oggi?*, in *http://www.apogeonline.com/webzine/2003/09/15/01/200309150101*.

[7] Il termine *lifelogging* significa, letteralmente, l'abitudine di "narrare" se stessi attraverso un'attrezzatura elettronica che pubblica sul *web* dati, testi e immagini attraverso la loro pubblicazione sui *social network*. Il *life caching* si riferisce alla ten-

specificatamente concepiti come *activity trackers* per la raccolta continua e in tempo reale di informazioni sullo stato psico-fisico o di salute del fruitore (es., come già illustrato, bracciali usati nel settore medico o sportivo) o per offrire funzioni di "realtà aumentata" (es. gli occhiali intelligenti) [8]; altri ancora sono capaci di interagire in modo complesso e dinamico con l'ambiente, adattando automaticamente le proprie funzionalità in base agli stimoli ricevuti (si pensi alle microcamere integrate in ciondoli e spille dotati di sensori di rilevazione di movimento, temperatura, luminosità, ecc.); taluni *devices*, poi, memorizzano dati biometrici (es. impronte digitali, timbro vocale, ecc.) [9] che vengono utilizzati per consentire di aprire la porta di casa, accedere a conti bancari o ad altri dispositivi elettronici, mentre alcuni si integrano fisicamente con il corpo umano, supplendo a sue carenze o addirittura sostituendolo in determinate funzionalità (come nel caso degli impianti per non vedenti già sperimentati negli Stati Uniti).

Va poi menzionato l'abbigliamento *smart*, recante *microchip* o confezionato con tessuti "intelligenti" che consentono, ad esempio, il monitoraggio di parametri vitali (frequenza cardiaca, temperatura, qualità e durata del sonno, ecc.) di chi li indossa. Tali capi, inoltre, possono integrare anche mini-antenne e dispositivi per il *GPS* in modo da inviare dati, tramite una rete *wireless* o un cellulare, verso un *server cloud* cui accede il proprio medico o l'allenatore di *fitness* (si pensi alle scarpe da ginnastica con *microchip* e antenna *wireless* che raccolgono e trasmettono ad altri *devices* informazioni su condizioni e prestazioni fisiche dello

denza a raccogliere e memorizzare in *database*, locali o in *cloud*, tracce di tutti gli eventi considerati significativi della propria vita, per poi eventualmente condividerli con gli altri.

[8] Per *augmented reality* (ovvero "realtà aumentata", il cui acronimo è *AR*), si intende la sperimentazione di percezioni sensoriali arricchite mediante l'uso di dispositivi elettronici in grado di manipolare le informazioni ambientali, comprese quelle che non sarebbero percepibili attraverso i cinque sensi. Sviluppata per un impiego strettamente limitato al mondo scientifico e militare, questa tecnologia si sta diffondendo attraverso le applicazioni sviluppate per *smartphone* e *tablet*. Esempi di realtà aumentata sono rinvenibili nel campo della geolocalizzazione; della *facial recognition* e della *object recognition* tramite foto e video; del *tagging* di luoghi allo scopo di darsi appuntamenti o rintracciarsi; della visualizzazione di immagini elettroniche sovrapposte a immagini tratte direttamente dalla realtà, ecc.

[9] Nel prossimo futuro, i *devices* potranno essere controllati con la voce; tuttavia, se ad oggi bisogna porre delle domande per avere delle risposte, prossimamente verranno sperimentati sistemi capaci di predire le nostre richieste analizzando i dati in loro possesso sui luoghi frequentati, le persone contattate, le preferenze culinarie o musicali. Grazie alla diffusione dei *devices*, è prevedibile che i lettori di impronte digitali verranno sempre più utilizzati a fini di sicurezza. Allo stato, infatti, servono solo a sbloccare il telefono o effettuare acquisti *online*, ma presto potranno essere usati anche per autorizzare pagamenti, accedere a numerosi servizi, aprire la porta di casa, casseforti o automobili. Le impronte digitali potrebbero essere presto soppiantate dall'iride. La scansione del nostro occhio offre una nuova strada alla sicurezza e funziona senza dover toccare nulla: basta avere il *device* di fronte a sé per sbloccarlo o controllarlo.

sportivo, quali la distanza percorsa, la velocità, ecc.) [10]. Si stima che, nel prossimo futuro, le funzionalità di questi dispositivi possano essere ancora più evolute ed estremamente diffuse, inclusi il monitoraggio complessivo e costante del quadro clinico di pazienti e anziani, nonché il controllo dello stato psico-fisico di individui adibiti a mansioni particolarmente delicate come i piloti di aereo.

Infine, gli orologi intelligenti (c.d. *smartwatches*) sono dispositivi da polso che, oltre a misurare il tempo come gli orologi tradizionali, sono anche in grado di interagire con *smartphone*, *tablet* ed altri *devices*, consentendo la condivisione di informazioni (per lo più parametri vitali o prestazioni fisiche) raccolte grazie al contatto diretto con il fruitore o dall'ambiente esterno, nonchè la semplificazione di alcune operazioni in mobilità (rispondere a chiamate telefoniche o leggere messaggi senza estrarre dalla tasca lo *smartphone*) [11].

La diffusione di massa dei *wearable devices* comporterà indubbiamente una serie di mutamenti sostanziali nei rapporti interindividuali: le potenzialità insite in tali strumenti potrebbero rivoluzionare il rapporto di milioni di utenti con la tecnologia informatica, incidendo in modo significativo sulla percezione della realtà da parte di chi li utilizza e preconizzando una società dove la privacy rischia di essere erosa in forma progressiva e inesorabile. Proprio per tali motivi, occorre individuare mezzi di tutela calibrati sui nuovi strumenti dell'informatica, che stanno irrimediabilmente mettendo in tensione consolidate categorie giuridiche. La protezione dei dati personali si pone allora come garanzia per scongiurare il pericolo che le nuove tecnologie, anche quando semplificano le attività quotidiane, diventino congegni perversi, fondati su un uso spregiudicato dei dati personali che potrebbe alimentare, per di più, una vera e propria "mercato" digitale, basato sullo sfruttamento commerciale delle informazioni individuali [12].

[10] Si presume che troverà un largo sviluppo il "*software as a service*", in cui la nuvola non viene utilizzata solo per stoccare dati, ma diventa un vero cervello centrale da cui attingere programmi e informazioni da elaborare poi sul proprio *device*. Secondo la società di ricerca *Gartner Inc.*, nel 2014 il "*personal cloud*" (*i.e.* l'archiviazione di dati *online* tramite servizi come *DropBox* o *iCloud*) soppianterà l'*hard disk* del PC, portando una migrazione dei dati dai supporti fissi verso la rete (in *www.gartner.com*).

[11] Nel tentativo di fornire una panoramica esaustiva, vanno ricordate le tecnologie, in larghissima parte ancora sperimentali, non propriamente classificabili come *wearable devices*, ma piuttosto *embedded*, cioè integrate direttamente nel corpo del fruitore, come i tatuaggi elettronici o i *microchip* sottocutanei in grado di rilevare informazioni fisiologiche, di trasmettere dati e interagire con altri dispostivi.

[12] In tal senso v. Garante per la protezione dei dati personali, *Relazione annuale 2012 - Discorso del Presidente A. Soro*, Roma, 2013 (in *www.garanteprivacy.it*; doc. *web* n. 2470652), p. 13. Il documento, nel lanciare l'allarme dei possibili effetti degenerativi derivanti da un uso ir-

2. Un primo fronte da esplorare: la privacy del fruitore.

L'utilizzo dei *wearable devices* disvela, dunque, una serie di interrogativi riguardanti, in primo luogo, la riservatezza del fruitore: il dispositivo indossabile potrebbe essere *hackerato*, oppure smarrito o rubato al suo possessore. Occorre quindi individuare un livello standard di sicurezza dei dati raccolti e conservati dal *device*, molti dei quali idonei a rivelare, anche indirettamente, persino informazioni di natura sensibile (come quelli sulla salute dell'interessato), biometrica o, comunque, in genere delicate.

È necessario, perciò, ingenerare nei fruitori la consapevolezza che tali dispositivi possono raccogliere, trattare e conservare una grande quantità di dati (c.d. *big data*) rendendoli facilmente condivisibili nell'ambito dei *social networks* o mediante altri canali (come nell'ipotesi di interazione con *devices* in possesso di altre persone) ed evidenziare chiaramente che, una volta diffusi sul *web*, tali dati, di fatto, non appartengono più agli utenti (almeno non in via esclusiva), con il rischio di imprevedibili conseguenze pregiudizievoli sulla sua identità e reputazione. I dispositivi indossabili, inoltre, sono potenzialmente in grado di elaborare i *big data* per identificare le caratteristiche comportamentali dell'individuo, correlando le informazioni sulla base di diagnosi predittive ovvero di forme di profilazione estremamente sofisticate [13], al fine di ricavarne modelli comportamentali standardizzati sulle cui basi prevedere ed omologare le scelte (di

responsabile delle nuove tecnologie, evidenzia che, se da un lato vengono così costruiti modelli identitari omologati e omologanti, pregiudicando la stessa possibilità dell'autodeterminazione individuale, dall'altro, i dati raccolti fuoriescono dalla sfera di controllo dei singoli per finire negli "archivi" di soggetti ispirati essenzialmente dalla logica del profitto. Con specifico riferimento ai dispositivi indossabili, si noti che la possibilità di inserire un sensore in qualunque oggetto o nel corpo umano, e di poter sempre attivare un collegamento con il *web*, consente di mercificare e di attribuire un prezzo alle informazioni che se ne ricavano. I sensori e la connettività permanente generano così nuovi mercati nel campo dell'informazione, incentivando gli individui a monetizzare i dati che li riguardano. Ne consegue che i dati personali acquistano una diversa connotazione: sono l'oro del nuovo millennio, l'oro digitale o immateriale, e Internet il nuovo Klondike, il Far West dei moderni pionieri, fenomeno illustrato, in termini suggestivi ma efficaci, da G. Busia, *Le frontiere della privacy in Internet. La nuova corsa all'oro per i dati personali*, in O. Pollicino-E. Bertolini-V. Lubello (a cura di), *Internet: regole e tutela dei diritti fondamentali*, Roma, 2013, p. 27. Su tali aspetti cfr., altresì, C. Rees, *Tomorrow's Privacy: Personal Information as Property*, in *International data privacy law*, 2013, p. 220; E. Morozov, *Il mercato della privacy*, in *Internazionale (F.A. Zeitung)*, 2013, p. 34; J. Rose-O. Rehse-B. Röber, *The Value of Our Digital Identity*, 2012, in *www.libertyglobal.com*.

[13] Sugli aspetti più inquietanti emergenti dall'evoluzione tecnologica e dalla sua interrelazione con il *web*, cfr. V. Mayer-Schonberger-K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, 2013, pp. 242, e *Big data demands big responsibility*, in *Financial Times*, 22 dicembre 2013, reperibile in *http://www.ft.com/cms/s/0/eae12124-697c-11e3-aba3-00144feabdc0.html#axzz2ppY7Jou9*. In effetti, l'Internet delle cose ("*Internet of Things*") diventerà sempre più l'Internet di ogni cosa ("*Internet of Everything*") proprio in virtù delle potenzialità offerte dal-

consumo, del tempo libero, ecc.) degli interessati, ai quali vengono somministrate forme di pubblicità mirata e selettiva [14].

Il fruitore deve essere quindi adeguatamente informato in modo da essere posto in grado di valutare consapevolmente l'impatto che un flusso massiccio e pressoché ininterrotto di informazioni può esercitare sulla sua "immagine diffusa" e sulla propria reputazione (o su quella dei suoi cari, sulla sua attività professionale, ovvero per le aziende o istituzioni presso le quali è incardinato, ecc.) [15].

In aggiunta, non è ancora chiaro se e come sia possibile intercettare lo scambio di dati tra un *wearable device* e altri dispositivi [16], come ad esempio un *personal computer*, uno *smartphone* o un *tablet* [17]: non sembra inverosimile ipotizzare l'esistenza di rischi legati alla possibile dispersione di informazioni nell'am-

---

l'analisi dei *big data*: la sveglia si regolerà automaticamente in base ai nostri impegni, il cassonetto comunicherà autonomamente alla centrale operativa quando è il momento di essere scaricato e il semaforo funzionerà solo in presenza di automobili. Le sperimentazioni sono già in atto e nel 2014 potrebbero essere immessi sul mercato i primi dispositivi in grado di connettersi alla rete e comunicare tra loro senza l'intervento umano.

[14] Sorge quindi il dubbio — inquietante, eppure non così lontano dal vero — che si possa plasmare ed orientare l'autodeterminazione degli individui: con queste forme di profilazione, infatti, si opera un forte condizionamento della libertà di scelta dei singoli, attraverso meccanismi che appaiono, per certi versi, subdoli e insidiosi proprio perché filtrano e selezionano, all'insaputa degli interessati e sulla base di catalogazioni comportamentali predefinite da chi gestisce gli strumenti di comunicazione telematica, le offerte emergenti dal mondo non solo dei consumi, ma anche, più in generale, delle relazioni sociali (si consideri che Internet è utilizzato in maniera crescente per l'invio ai cittadini di messaggi di propaganda elettorale specificatamente calibrati sul potenziale elettore). Così G. Busia, *Le frontiere della privacy in Internet. La nuova corsa all'oro per i dati personali*, cit. *supra*.

[15] Tali questioni assumono rilevanza soprattutto in relazione ad un possibile utilizzo di questi strumenti da parte di minori, più esposti ad un uso non pienamente consapevole dei rischi. Per un approfondimento in merito, v. la *Opinion 02/2013 "On apps on smart devices"* redatta dal *Gruppo di lavoro Articolo 29 sulla tutela dei dati personali* (27 febbraio 2013), disponibile in *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf*, nonché il *Rapporto informativo della Federal Trade Commission "Mobile Apps for Kids: Current Privacy Disclosures are Disappointing"* (febbraio 2012), reperibile in *http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf*.

[16] Una simile eventualità, oltre a costituire una violazione delle disposizioni in materia di protezione dei dati personali, assume rilevanza penale ai sensi degli artt. 617-*quater*, comma 1, e 617-*quinquies*, comma 1, c.p. i quali puniscono — rispettivamente — chiunque intercetta fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, nonché coloro che, fuori dai casi consentiti dalla legge, installano apparecchiature atte ad intercettare, impedire od interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi. Non si dimentichi, inoltre, che anche l'art. 15 della Costituzione sancisce l'inviolabilità della libertà e della segretezza della corrispondenza "*e di ogni altra forma di comunicazione*", stabilendo che "*la loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge*".

[17] Tale ipotesi non appare del tutto inverosimile se si considera che il Garante per la protezione dei dati personali è stato investito, con un ricorso, della richiesta di cancellazione e di blocco dei dati trattati in violazione di legge derivanti dalla illecita registrazione e diffusione su un *blog* di comunicazioni radioamatoriali che riguardavano il ricorrente indebitamente intercettate, nonché dall'associazione del suo codice identificativo (e dunque indirettamente del suo nominativo) ad immagini e

biente tecnologico circostante, laddove non si utilizzino canali di collegamento sicuri, ovvero alla captazione, anche involontaria, di dati da parte di terzi durante l'interazione tra dispositivi [18].

Alla luce di quanto sopra illustrato, sorgono numerosi quesiti ancora sostanzialmente insoluti: le soluzioni tecnologiche e la disciplina vigente garantiscono la correttezza del trattamento dei dati del fruitore? Quali *privacy policies* sono state predisposte dai produttori dei *devices*, quali regole osservano tali soggetti ed eventuali terze parti coinvolte, direttamente o indirettamente, nell'accesso alle informazioni riguardanti i fruitori dei dispositivi? Quale è la quantità e natura dei dati raccolti automaticamente dal *device* [19], la finalità della raccolta e le modalità del loro successivo trattamento?

Già per quanto riguarda *devices* mobili "tradizionali", come *smartphone* e *tablet*, sono stati manifestati dubbi riguardo la gestione della *privacy* in relazione alle informazioni sugli utenti [20], quando si scaricano e utilizzano *app* [21], o per quanto riguarda il trattamento dei dati da remoto e la geolocalizza-

commenti dal contenuto offensivo. V. *Decisione su ricorso del 30 maggio 2013*, in *www.garanteprivacy.it*, doc. *web* n. 2601399.

[18] Pur concernendo un diverso ambito tecnologico, è significativo il caso delle "*Google cars*" che acquisivano immagini per il servizio *Street View* e che, durante il passaggio sul territorio italiano, hanno raccolto sia dati relativi alla presenza di reti *Wi-Fi* (*wireless fidelity*), sia frammenti di comunicazioni elettroniche trasmesse dagli utenti su alcune reti *Wi-Fi* non protette da protocolli sicuri e da cifratura (c.d. *payload data*). *Google Inc.* ha informato dell'anomalia il Garante per la protezione dei dati personali, che ha bloccato il trattamento dei *payload data* raccolti ed a disposto la trasmissione degli atti all'Autorità giudiziaria per le valutazioni di competenza (v. provvedimento del 9 settembre 2010 intitolato *Comunicazioni "captate" su reti wifi: il Garante ordina a Google Street View il blocco dei dati e trasmette gli atti alla magistratura*, in *www.garanteprivacy.it*, doc. *web* n. 1750529).

[19] Ad esempio, dispositivi come gli "occhiali intelligenti" possono essere indossati anche quando si compiono operazioni delicate come la digitazione del PIN *code* della carta di credito o del Bancomat. Inoltre, un *wearable device* può raccogliere e contenere informazioni, anche delicatissime, su comportamenti tenuti in ambienti specifici (ad esempio, sul posto di lavoro), su attitudini e capacità relazionali, sulle *performance* psico-fisiche e su vari aspetti della vita privata (abitudini e comportamenti di consumo, preferenze su tempo libero, sessualità, ecc.). Si possono solo immaginare le conseguenze che graverebbero sul fruitore ove i suoi parametri vitali — e quindi in generale dati sullo stato di salute — registrati da un *wearable device* fossero, anche solo accidentalmente, trasferiti al datore di lavoro e successivamente utilizzati per determinare i percorsi di carriera, le mansioni o addirittura per orientare le scelte su possibili licenziamenti. Oppure, se tali dati fossero trasferiti, in modo illecito, a società finanziarie per determinare la a priori possibilità di stipulare polizze assicurative, mutui, prestiti, ecc.

[20] V. Garante per la protezione dei dati personali - Schede di documentazione, *Smartphone e tablet: scenari attuali e prospettive operative*, in *www.garanteprivacy.it*, doc. *web* n. 1819937.

[21] Sul tema delle *app* per dispositivi mobili si sono recentemente espresse le Autorità nazionali di protezione dei dati personali partecipanti alla *35ma Conferenza internazionale dei Garanti per la privacy* (Varsavia, 23-26 settembre 2013), con una *Dichiarazione sui rischi di "appificazione" della società*. Il documento, in particolare, afferma come sia *"fondamentale che gli utenti abbiano e continuino ad avere il controllo dei propri dati"*, per *"poter decidere quali informazioni condividere, con chi condividerle e per quali finalità"* (in *www.garanteprivacy.it*, doc. *web* n. 2659319).

zione [22]. Si pensi, ad esempio, ad un'eventuale raccolta di dati sulla posizione e gli spostamenti del fruitore [23], effettuata magari anche a sua insaputa, per poi essere condivisi tramite i *social networks* o il *web* e le conseguenti implicazioni legate alla diffusione di tali informazioni che, peraltro, possono rivelare abitudini personali e informazioni riguardanti la sfera più intima della persona. Problemi, questi, che possono essere amplificati se si considerano le potenziali funzionalità del *wearable devices*.

Lo scenario sopra delineato impone quindi una prima individuazione di alcune regole fondamentali applicabili per assicurare un corretto trattamento dei dati personali riguardanti il fruitore alla luce del d.lgs. 30 giugno 2003, n. 196 (recante il *Codice in materia di protezione dei dati personali*).

In primo luogo, i trattamenti dovrebbero svolgersi rispettando sia il principio di necessità, per cui i sistemi informativi e i programmi informatici devono essere configurati, già in origine, in modo da ridurre al minimo l'utilizzo di informazioni relative a soggetti identificabili (art. 3 del d.lgs. n. 196/2003), sia quello di proporzionalità, in base al quale tutti i dati personali e le varie modalità del loro trattamento devono essere pertinenti e non eccedenti rispetto alle finalità perseguite (art. 11, comma 1, lett. *d*, del d.lgs. n. 196/2003).

Prima della raccolta dei dati e dell'attivazione del *device*, dovrebbe essere fornita al fruitore un'informativa chiara e completa, recante tutti gli elementi richiesti dall'art. 13 del d.lgs. n. 196/2003, al fine di consentirgli un'adesione pienamente consapevole alle iniziative proposte; occorrerebbe altresì acquisire il relativo consenso specifico, informato e distinto nell'ipotesi in cui sia prevista la profilazione (art. 23 del d.lgs. n. 196/2003) [24]. Il consenso dovrebbe essere quantomeno documentato per iscritto a cura del titolare del trattamento, ovvero reso necessariamente per

[22] Le tematiche qui elencate sono state in larga parte oggetto della lettera congiunta che, nel giugno 2013, un gruppo di Autorità nazionali di protezione dei dati personali di diversi continenti, riunite nel *GPEN (Global Privacy Enforcement Network)*, ha inviato a *Google Inc.* per chiedere chiarimenti riguardo ai mezzi di tutela della privacy connessi alla introduzione in commercio dei *Google Glass*, occhiali "intelligenti" che offrono funzioni di ripresa di immagini e audio, realtà aumentata e riconoscimento facciale. Le Autorità, in particolare, hanno chiesto alla Società un sollecito riscontro sulle implicazioni *privacy* legate allo sviluppo di questa nuova tecnologia, nonché sulle misure che intende adottare per garantire il rispetto della vita privata in tutti i Paesi del mondo (v. *Letter to Google regarding Google Glass;* in *www.garanteprivacy.it*, doc. *web* n. 2485687).

[23] In proposito si consulti la *Opinion 13/2011 "On Geolocation services on smart mobile devices"*, redatta dal Gruppo di lavoro Articolo 29 sulla tutela dei dati personali (16 maggio 2011), in *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf*.

[24] Sulle modalità per un corretto trattamento effettuato a tale particolarissimo fine, v. Garante per la protezione dei dati personali, *Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione*, 25 giugno 2009, in *G.U.* n. 159 dell'11 luglio 2009 e in *www.garanteprivacy.it*, doc. *web* n. 1629107.

iscritto dall'interessato, nel caso di dati sensibili (art. 26 del d.lgs. n. 196/2003).

Tali adempimenti si renderebbero necessari al fine di non incorrere nelle sanzioni previste (artt. 15, 161, 162, comma 2-*bis* e 167 del d.lgs. n. 196/2003), profili, questi ultimi, che pongono problemi forse ancora più rilevanti nel caso della rilevazione di dati riguardanti soggetti diversi dai fruitori (v. par. 3, *infra*).

Resterebbero impregiudicati gli ulteriori obblighi che il d.lgs. n. 196/2003 detta ai titolari del trattamento, con particolare riferimento a quelli riguardanti l'esercizio dei diritti degli interessati e il relativo tempestivo riscontro (artt. 7-10), alla selezione dei soggetti che, in qualità di incaricati o responsabili del trattamento, sono autorizzati a compiere operazioni di trattamento sulla base dei compiti assegnati e delle istruzioni impartite (artt. 29 e 30), all'adozione delle misure anche minime di sicurezza (artt. 31-35, 169 e Allegato B) [25], alla notificazione al Garante in caso di eventuale profilazione (artt. 37, comma 1, lett. *d*, e 163), nonché alla comunicazione agli interessati e al Garante dell'eventuale violazione di dati personali da parte del fornitore di servizi di comunicazione elettronica accessibili al pubblico (artt. 32-*bis* e 162-*ter* del d.lgs. n. 196/2003) [26].

In tale quadro, occorre tuttavia tenere presente una precipua caratteristica di funzionamento dei supporti in relazione alla gestione di dati raccolti dai *wearable devices*, vale a dire la circostanza che le informazioni potrebbero essere oggetto di successiva migrazione e immagazzinamento in *repositories* esterne, con tutte le eterogenee problematiche conseguenti all'utilizzo del

[25] Ovviamente, le misure di sicurezza attualmente previste non sono in grado di soddisfare pienamente le esigenze di tutela derivanti dai dispositivi indossabili ed occorrerà pensare ad altre maggiormente aderenti alla mutata realtà tecnologica. Si pensi alle soluzioni già prospettate per gli *smartphone* come *Snapchat*, *app* che consente di inviare foto, video e messaggi che scompaiono pochi secondi dopo essere stati ricevuti.

[26] A tal riguardo, è utile una breve panoramica della disciplina di settore in ambito europeo e nazionale. La *Direttiva 2002/58/CE* (*c.d. direttiva e-Privacy*) prevede che i fornitori di servizi di comunicazione elettronica adottino "*appropriate misure tecniche e organizzative*" per assicurare "*un livello di sicurezza adeguato al rischio esistente*" (art. 4, comma 1). Nella *Direttiva 2009/136/CE* (che ha modificato la *Direttiva 2002/58/CE*) si è tenuto conto, in particolare, del fatto che un evento che coinvolga dati personali, se non trattato in modo adeguato e tempestivo, può provocare un grave danno economico e sociale al contraente (o alle altre persone interessate), tra cui l'usurpazione dell'identità. In Italia, il recepimento delle disposizioni europee è avvenuto tramite il d.lgs. 28 maggio 2012, n. 69, con il quale il Governo ha dato attuazione alla delega prevista nell'art. 9 della legge comunitaria del 2010 (legge 15 dicembre 2011, n. 217). In base al citato decreto, che ha introdotto gli artt. 32-*bis* e 162-*ter* nel d.lgs. n. 196/2003, i fornitori di servizi di comunicazione elettronica sono oggi tenuti a comunicare, senza indebiti ritardi, al Garante per la protezione dei dati personali e, in alcuni casi, al contraente o ad altre persone interessate, l'occorrenza dei predetti eventi, qualificati come "violazioni di dati personali". Il Garante è intervenuto sul tema, in particolare, con il *Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach)* del 4 aprile 2013 (in *G.U.* n. 97 del 4 aprile 2013 e in *http://www.garanteprivacy.it*, doc. *web* n. 2388260).

cloud computing [27] che, allo stato, non trovano ancora un'adeguata soluzione, anche perché necessitano una regolamentazione di carattere internazionale.

Infatti, tra i tanti, l'aspetto forse più critico è la dislocazione delle infrastrutture del fornitore del servizio di *cloud computing* al di fuori dei confini nazionali, aspetto che determina l'impossibilità di conoscere con esattezza l'ubicazione dei propri dati nella "nuvola" ed ha riflessi immediati sia sulla disciplina applicabile in caso di contenzioso tra l'utente e il fornitore, sia in relazione alle disposizioni nazionali che regolano il trattamento, l'archiviazione e la sicurezza dei dati [28].

Nel caso dell'allocazione di dati sulla *cloud* è il fornitore del servizio il soggetto che assume un ruolo rilevante in ordine alle misure necessarie a garantire la sicurezza delle informazioni che gli vengono affidate, mentre il fruitore perde il controllo diretto ed esclusivo sui propri dati; peraltro la dimensione del fornitore finisce inevitabilmente per condizionare la forza contrattuale dei fruitori del servizio e la loro possibilità di esercitare un controllo sui siti e sulle infrastrutture utilizzate per ospitarne i dati, come quelli raccolti tramite *wearable devices* [29].

[27] A seguito del cosiddetto "*Datagate*" (cioè, i presunti casi di monitoraggio e intercettazione di telefonate e comunicazioni in rete effettuati da *FBI* e *NSA-National Security Agency* statunitensi, nel quadro del programma top-secret PRISM, rivelati alla stampa da Edward Snowden nel giugno 2013), che ha visto emergere con rilevanza il tema della sicurezza e riservatezza dei dati personali sul *web*, l'Unione europea ha annunciato di voler disciplinare con norme aggiornate alla rapidità dei cambiamenti tecnologici in atto il settore del *cloud computing*. Le dichiarazioni di intenti sono contenute in un *memo* (15 ottobre 2013), disponibile in *http://europa.eu/rapid/press-release_MEMO-13-898_en.htm?locale=en*. Si rinvia anche alla *Opinion 05/2012 "On Cloud Computing"*, redatta dal *Gruppo di lavoro Articolo 29 sulla tutela dei dati personali* (1 luglio 2012), *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf*; nonché alla *Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions, Unleashing the Potential of Cloud Computing in Europe*, COM(2012) 529 final, Brussels, 27 September, 2012. Sul tema si sono espressi anche i partecipanti alla *34esima Conferenza internazionale delle Autorità di protezione dei dati personali* (Punta Del Este, Uruguay, 23 e 24 ottobre 2012) con una "*Risoluzione sul cloud computing*", disponibile in *http://www.garanteprivacy.it/documents/10160/2150357/Resolution+on+Cloud+Computing.pdf*. A livello europeo, la documentazione in materia è particolarmente nutrita, ma è doveroso un rinvio a quella prodotta, in particolare, dalla *European Union Agency for Network and Information Security-ENISA* (in *www.enisa.europa.eu*), nel cui ambito si sta tentando di affrontare le inedite criticità del *cloud computing*.

[28] V. Garante per la protezione dei dati personali - Schede di documentazione, *Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*, 2012, in *www.garanteprivacy.it*, doc. *web* n. 1819933.

[29] Viviamo in un modo sempre più dominato dai giganti della tecnologia, i c.d. "*over the top*", le cui derive sono state vaticinate nel romanzo "*The Circle*" di Dave Eggers, un versione aggiornata di "*1984*" di George Orwell: qui il "grande fratello", anziché un potere tecnologico statale e opprimente, è rappresentato da un colosso dell'informatica. La morale che affiora dalla lettura del romanzo è che la conoscenza è potere, per cui gli operatori "*over the top*" sempre più controlleranno quella delle persone e le informazioni che le riguardano.

3. Gli aspetti di maggiore criticità. Alla ricerca di termini e modalità per preservare la sfera di riservatezza dei terzi.

La diffusione dei *wearable devices* prefigura una problematica di ancora più difficile soluzione rispetto quelle sopra illustrate: l'individuazione di strumenti per tutelare la privacy dei terzi, cioè dei soggetti i cui dati vengono raccolti dal fruitore quando quest'ultimo interagisce nell'ambiente circostante, captando e successivamente diffondendo informazioni altrui (si pensi alle immagini riprese in automatico da un dispositivo indossabile e poi condivise nei *social networks*) [30]. Gli interessati non solo potrebbero essere del tutto ignari che la propria immagine è riprodotta in foto e filmati diffusi sul *web*, ma non avrebbero comunque possibilità di scegliere se apparire o meno, fornendo così involontariamente informazioni su dove si trovano, con chi, impegnati in quali attività, in quale momento della giornata, criticità — queste — ancora più rilevanti quando coinvolgono i minori [31].

Peraltro, alcuni dispositivi potrebbero essere dotati di applicazioni *facial recognition* (*i.e.* tecniche biometriche che utilizzano strumenti informatici per identificare o verificare l'identità di una persona a partire da una o più immagini che la ritraggono), oltretutto spesso associabili a sistemi di *tagging* automatico. Questo significa che un individuo può essere riconosciuto dal *device* mentre viene fotografato o ripreso in un video e la sua immagine essere successivamente *taggata* e inserita nei *social networks*, a cui si aggiungono magari dati aggiuntivi sulla sua geolocalizzazione. Tali operazioni possono essere effettuate dai *wearable devices* in modo automatico, cioè senza che il soggetto ripreso e spesso lo stesso fruitore del dispositivo medesimo ne siano consapevoli, se non eventualmente a posteriori, quando però l'informazione è già diffusa in rete, e quindi non più controllabile.

Inoltre, ad ogni riconoscimento i dati disponibili sul soggetto possono aumentare e arricchire la precisione dei riconoscimenti successivi, anche se ciò non garantisce la qualità e la correttezza del dato: se le informazioni sono inesatte, imprecise o abbinate erroneamente, alimentano il consolidamento di errate definizioni

[30] Sul tema cfr. K. Michael, *Wearable computers challenge human rights ABC Science*, 24 luglio 2013, in *http://www.abc.net.au/science/articles/2013/07/24/3809675.htm*. Osserva l'autrice che *[...] "The power to exclude, delete or misrepresent an event is with the wearer and not the passive passer-by. There is an asymmetry here that cannot be rectified, unless the passive participant becomes an active wearer themselves. And this is not only unfeasible, but I would argue undesirable. At what point do we say then enough is enough?" [...]*.

[31] Negli ordinamenti legislativi nazionali, non mancano disposizioni a tutela dei minori sul *web*, come la legge federale rubricata *Children's Online Privacy Protection Act (COPPA)* — adottata negli Stati Uniti nel 1998, in vigore dal 2000 ed emendata nel 2012 — riguardante la gestione *online* delle informazioni riguardanti i minori di 13 anni da parte di operatori di siti *web*.

dell'identità *online*, con tutto ciò che ne consegue in termini di danno all'immagine e alla reputazione personali [32].

Occorre quindi verificare se ed entro quali limiti le disposizioni in materia di privacy attualmente in vigore si applicano ai trattamenti di dati personali di terzi effettuati dai fruitori tramite *wearable devices* [33].

In proposito, occorre muovere da una premessa di fondo, vale a dire che il d.lgs. n. 196/2003 è inapplicabile quando le persone fisiche trattano dati personali per "*fini esclusivamente personali*" (art. 5, comma 3). In tale ipotesi il trattamento non è soggetto agli obblighi in materia di trattamento dei dati personali a condizione, però, che le informazioni trattate "*non siano destinate ad una comunicazione sistematica o alla diffusione*", poiché rivivrebbero le disposizioni in materia di privacy. Ad esempio, l'invio occasionale di un'immagine ad amici o familiari soddisfa esclusivamente esigenze di carattere strettamente personale (culturali, di svago o di altro genere) e la relativa comunicazione resta confinata in una sfera circoscritta di conoscibilità; al contrario, la sua trasmissione a un numero di soggetti indeterminati, anche tramite la messa a disposizione tramite la pubblicazione su un sito *web*, integra gli estremi della diffusione e come tale richiede — così come la comunicazione sistematica — l'adozione di tutti gli adempimenti positivizzati dalla disciplina sulla riservatezza.

Va osservato, al riguardo, che la linea di confine tra diffusione e uso personale sul *web* è davvero sottilissima [34]: lo testimonia il caso di una ricorrente che si è vista rigettare la richiesta, presen-

[32] Anche se i fatti non riguardano direttamente l'utilizzo dei *wearable devices*, appaiono emblematici i casi di due cittadini, i quali avevano visto pubblicata da alcuni quotidiani la propria immagine estratta da *Facebook* ed erroneamente associata a persone omonime decedute. In un caso si trattava di un incidente stradale, nell'altro di una vittima del terremoto avvenuto in Abruzzo. Il Garante per la protezione dei dati personali, intervenuto su ricorso degli interessati, ha censurato l'azione dei giornalisti che avevano utilizzato fotografie e dati personali tratti dai *social network* senza verificarne la veridicità e, quindi, senza esercitare con correttezza il diritto di cronaca (v. *Decisioni su ricorso*, entrambe del 6 maggio 2009, in *www.garanteprivacy.it*, doc. *web* n. 1615317 e n. 1615339).

[33] Il Garante per la protezione dei dati personali si è dimostrato un precursore dei tempi quando ha adottato provvedimenti sui terminali applicati alla telefonia mobile che, al pari dei *wearable devices*, consentono di registrare fotografie e filmati tramite diverse tecnologie di rete, quali *Gprs*, *Edge o Umts*, comunicando e diffondendo immagini e suoni in tempo reale. Tali documenti possono offrire un primo insieme di utili elementi di riflessione sui correttivi apportabili all'utilizzo sfrenato dei dispositivi di nuova generazione, fermo restando che andrà comunque verificata, sotto il profilo pratico, la perdurante attualità delle regole così individuate. V., dunque, *Videofonini: cautele per un uso legittimo*, 20 gennaio 2005, doc. *web* n. 1089812; *MMS: le regole anche per gli usi personali*, 12 marzo 2003 doc. *web* n. 29816 (ambedue rinvenibili in *www.garanteprivacy.it*).

[34] È il caso di osservare, al riguardo, che la proposta di regolamento adottato dall'Unione europea per aggiornare e sostituire la direttiva 95/46/CE in materia di protezione dei dati personali (sul quale si rinvia alla nota 60, *infra*) ha effettuato una scelta discutibile, che sconta la difficoltà di disciplinare il *web*, menzionando espressamente, al considerando n. 15, tra i trattamenti effettuati per fini personali anche la diffusione da parte di singoli di dati personali tramite i *social networks*.

tata ai sensi dell'art. 7 del d.lgs. n. 196/2003 al Garante per la protezione dei dati personali, di ottenere la cancellazione, da parte di *Facebook Inc.*, del *tag* che associava il proprio profilo *Facebook* a una foto pubblicata da un altro utente sulla propria pagina *web*, in quanto l'immagine era stata inserita in un profilo "chiuso" [35].

A rigore, gli interessati devono essere comunque informati in modo idoneo [36], ai sensi dell'art. 13 del d.lgs. n. 196/2003, in relazione all'acquisizione di dati da parte dei fruitori che non intendano farne un uso strettamente individuale (in quanto destinati a comunicazione sistematica e diffusione), affinché i primi possano scegliere di sottrarsi alla "cattura" delle immagini da parte dei secondi, allontanandosi dal luogo oggetto di ripresa [37]. Ci si chiede allora come rendere concretamente applicabile tale disposizione, così come tutte quelle previste dal d.lgs. n. 196/2003, al trattamento di dati personali effettuato tramite i *wearable devices*. Considerata la crescente invasività e le caratteristiche tecniche di questi strumenti, non appare del tutto convincente la

[35] La ricorrente si era rivolta al Garante per la protezione dei dati personali in via d'urgenza, chiedendo un provvedimento inibitorio nei confronti di *Facebook*, al fine di ottenere la cancellazione dell'etichetta (*tag*) che collegava il proprio profilo *Facebook* a una foto pubblicata sul profilo di un'altra persona, relativa ad una campagna di sensibilizzazione sull'Aids e l'omosessualità. Secondo la ricorrente, tale associazione era lesiva della proprio immagine, dal momento che la foto era stata pubblicata in un fotoalhum "*contenente espliciti commenti ed inequivocabili riferimenti idonei a svelare l'orientamento sessuale di tutti i soggetti "taggati", compreso*" il proprio. Il ricorso è stato rigettato alla luce dell'art. 5, comma 3, del d.lgs. n. 196/2003: nel caso di specie, infatti, i dati raccolti non sono risultati destinati alla comunicazione sistematica o alla diffusione poiché la pagina *web* nella quale era stata "*taggata*" la ricorrente non risultava essere oggetto di diffusione, essendo stata inserita in un profilo "chiuso", visibile solo a un numero determinato di persone. Così in *Decisione su ricorso, Richiesta di cancellazione online della c.d. etichetta (tag) in un profilo Facebook*, 18 febbraio 2010, in *www.garanteprivacy.it*, doc. *web* n. 1712776.

[36] Va sottolineato che in questa sede si è cercato di individuare, allo stato della disciplina vigente anche di matrice europea, le norme che dovrebbero trovare applicazione alla fattispecie concreta, che proprio per le caratteristiche connaturate alle sue funzionalità provocano serie difficoltà di adattamento delle prime alla seconda. Non si esclude, quindi, che i futuri sviluppi dei dispositivi *wearable* inducano il legislatore ad un aggiornamento della disciplina — ipotesi sulla quale vengono formulate talune considerazioni nei seguenti paragrafi — ovvero conducano l'interprete futuro ad una applicazione in termini diversi o evolutivi rispetto quella qui prospettata.

[37] In via "analogica", è interessante richiamare in merito il caso delle "*Google cars*", i veicoli che circolano nelle città acquisendo immagini fotografiche di luoghi e persone poi pubblicate *online* attraverso il servizio *Street View*. Il Garante per la protezione dei dati personali, infatti, ha imposto a *Google Inc.* di fornire ai cittadini dettagliate notizie sul passaggio delle auto, affinché possano decidere in piena libertà i propri comportamenti ed eventualmente scegliere di non essere ripresi evitando di trovarsi nei luoghi di transito dei predetti autoveicoli. Ciò non solo rendendo le "*Google cars*" facilmente individuabili, attraverso cartelli o adesivi ben visibili, ma anche attraverso un'informativa completa da pubblicare sul proprio sito e da fornire attraverso i mezzi di informazione locali per ogni regione visitata. Così in Provvedimento intitolato *Google Street View: le auto dovranno essere riconoscibili*, 15 ottobre 2010 (in *www.garanteprivacy.it*, doc. *web* n. 1759972). Per tali motivi il Garante ha inflitto a *Google Inc.* una sanzione di un milione di euro (v. ordinanza-ingiunzione del 18 dicembre 2013, doc. *web* n. 2954309).

tesi sostenuta dai produttori per cui un'informativa viene sostanzialmente resa attraverso comportamenti concludenti (come quelli di attivare le funzionalità dei dispositivi indossabili), tenuto altresì presente che ai sensi del citato art. 13 l'informativa deve evidenziare una serie di elementi (finalità, modalità del trattamento, ecc.) che sicuramente non emergono da un semplice gesto che denota unicamente l'attivazione del dispositivo [38].

In linea di principio, occorrerebbe, inoltre, acquisire il consenso libero, preventivo e informato degli interessati (artt. 23 e ss. del d.lgs. n. 196/2003), adempimento non necessario laddove la raccolta di dati venga effettuata in luoghi pubblici o aperti al pubblico. Ciò, sempreché il relativo utilizzo non venga legittimamente inibito in tutto o in parte [39], e fatte salve eventuali limitazioni previste dalla legge, quali, ad esempio, il divieto di diffusione di fotografie quando ciò comporti pregiudizio all'onore, alla reputazione, al decoro della persona ripresa (art. 97, comma 2, della l. 22 aprile 1941, n. 633) o il divieto di diffusione di dati idonei a rivelare lo stato di salute (art. 26, comma 5, del d.lgs. n. 196/2003).

Peraltro agli interessati dovrebbe sempre essere assicurata la possibilità di esercitare i diritti di cui agli artt. 7 e ss. del d.lgs. n. 196/2003 [40], posti a presidio della correttezza del trattamento dei dati che lo riguardano, che dovrebbe avvenire invariabilmente nel rispetto delle pertinenti disposizioni, in particolare dei principi

[38] È proprio questa, invece, la soluzione sostanzialmente prospettata da *Google Inc.* a cui il Congresso USA, tramite il Gruppo bipartisan *Caucus*, ha indirizzato nel maggio 2013 una lettera di richiesta di chiarimenti sulle molteplici funzionalità dei *Google Glass*, con specifico riferimento alle modalità per informare gli interessati, per raccoglierne il relativo consenso e per consentire l'esercizio del diritto di accesso ai dati che li riguardano. Il riscontro fornito dalla Società è stato considerato deludente, che si è limitata ad assicurare che il dispositivo opera in maniera tale da rendere impossibile ai terzi di non capire che il fruitore è in procinto di attivare le sue funzionalità (es. occorre pronunciare determinate parole chiave o premere un pulsante sul fianco degli occhiali per attivare la raccolta di immagini, sarà impossibile spegnere il *display* quando si utilizza la funzione di foto o videocamera e non saranno integrati con alcuna tecnologia di riconoscimento facciale). Per un approfondimento si rinvia al sito del *Congressional Bi-Partisan Privacy Caucus*, in *https://joebarton.house.gov/congressional-bipartisan-privacy-caucus/*.

[39] Negli Stati Uniti, ad esempio, gli occhiali intelligenti sono già proibiti o dichiarati sgraditi in molti locali pubblici come bar, cinema, casinò e *strip club*, non solo per motivi pratici (evitare truffe ai tavoli da gioco o riprese dei film proiettati nelle sale cinematografiche), ma anche e soprattutto per tutelare la privacy degli avventori.

[40] In virtù degli artt. 7-10 del Codice, all'interessato sono riconosciute una serie di situazioni giuridiche soggettive attive, definiti "diritti", strumentali al controllo sul trattamento dei propri dati effettuato da terzi. L'interessato può quindi esercitare, *in primis*, una sequela di diritti di tipo conoscitivo per verificare l'attività del titolare (*i.e.* di ottenere la conferma dell'esistenza dei propri dati, di conoscerne origine, finalità e modalità del trattamento, gli estremi identificativi di titolare, responsabile o incaricati ai sensi dell'art. 7, commi 1 e 2) e di tipo correttivo, al fine di ottenere una esatta rappresentazione della propria identità (*i.e.* diritto di ottenere l'aggiornamento, la rettificazione o l'integrazione *ex* art. 7, comma 3, lett. *a*). Sono altresì previsti diritti di carattere inibitorio, ove si registri un trattamento illecito (*i.e.* di ottenere la cancellazione, la trasformazione in forma anonima o il blocco di cui all'art. 7,

(di difficile applicazione pratica in questo particolarissimo ambito) di liceità, proporzionalità, correttezza e necessità sanciti dall'art. 11.

Va poi sottolineato che, ai sensi del citato art. 5, comma 3, del d.lgs. n. 196/2003, al trattamento effettuato da persone fisiche, anche se a fini esclusivamente personali, comunque "*si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31*". Ne consegue che il fruitore è tenuto al risarcimento di cui all'art. 2050 c.c. se arreca danni, anche non patrimoniali, agli interessati generati dalla mancata adozione di idonee e preventive misure di sicurezza contro i rischi di distruzione o perdita, anche accidentale, dei loro dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'art. 2050 c.c., cui rinvia l'art. 15 del d.lgs. n. 196/2003, come è noto, prefigura la responsabilità per l'esercizio di attività pericolose, ovvero di quelle attività che "*per la loro spiccata potenzialità offensiva*" [41], derivante dalla loro intrinseca natura o dalla tipologia dei mezzi adoperati, comportano la rilevante possibilità del verificarsi di un danno. Di conseguenza, tali attività configurano la responsabilità dell'agente indipendentemente dall'elemento soggettivo, poiché in tal caso la componente psicologica (dolo o colpa) non costituisce un elemento qualificante la fattispecie. L'agente, infatti, è tenuto al risarcimento solo "*se non prova di avere adottato le misure idonee ad evitare il danno*" (art. 2050 c.c.): l'onere della prova, quindi, ricade sull'esercente l'attività pericolosa (nel caso di specie sul fruitore), il quale dovrà dimostrare di aver predisposto tutte le misure normalmente previste, in base ai normali canoni di diligenza e di perizia, per prevenire il danno al fine di escludere il nesso eziologico tra danno ed evento e non incorrere nella prevista responsabilità civile [42]; la predisposizione di tali accorgimenti comunque lo esenterà da responsabi-

comma 3, lett. *b*) e, infine, a carattere potestativo, che trovano applicazione a seguito di un bilanciamento tra contrapposte esigenze (*i.e.* opposizione per motivi legittimi al trattamento e al coinvolgimento in operazioni di *marketing* secondo l'art. 7, comma 4, lett. *a* e *b*).

[41] Così C. M. Bianca, *Diritto civile V - La responsabilità*, Ginffrè, Milano, 2002, pp. 704 e ss., al quale si rimanda per un opportuno approfondimento sui singolari risvolti problematici, evidenziati dalla fattispecie in esame, nell'ambito del nostro ordinamento.

[42] Va precisato, tuttavia, che stante il disposto dell'art. 15, comma 1, del d.lgs. n. 196/2003, in tema di responsabilità per esercizio di attività pericolosa, la presunzione di colpa a carico del danneggiante posta dall'art. 2050 c.c. presuppone il previo accertamento dell'esistenza del nesso eziologico — la cui prova incombe al danneggiato — tra l'esercizio dell'attività e l'evento dannoso, non potendo il soggetto agente essere investito da una presunzione di responsabilità rispetto ad un evento che non è ad esso in alcun modo riconducibile. Sotto il diverso profilo della colpa, incombe invece sull'esercente l'attività pericolosa l'onere di provare di avere adottato "*tutte le misure idonee a prevenire il danno (Cass. 5080/06; Cass. 19449/08; Cass. 4792/01; Cass. 12307/98)*", come sottolineato, da ultimo, dalla Corte di Cassazione, sez. I civile,

lità anche nel caso in cui le cause produttive del danno rimangano ignote.

La nozione di prova liberatoria di cui all'art. 2050 c.c., invocabile *per relationem*, evita la cristallizzazione degli standard di sicurezza: in via generale le misure richieste vengono generalmente individuate in quei provvedimenti che allo stato sono offerti dalla tecnica, anche se non del tutto idonee ad evitare il danno, pertanto l'agente non dovrà limitarsi ad adottare le misure minime come richiamate dall'art. 33 del d.lgs. n. 196/2003, qualora allo stato delle conoscenze tecniche risultano sviluppate delle misure più efficaci [43].

Nella diversa ipotesi in cui il trattamento sia invece finalizzato alla comunicazione sistematica e alla diffusione, nel ventaglio delle ipotesi incriminatici previste dal d.lgs. n. 196/2003, rileva, in particolare, il trattamento illecito di dati (art. 167). Fermo restando l'assorbimento della fattispecie in questione in altra che la contenga e che appaia, rispetto ad essa, più grave secondo quanto stabilito dalla clausola di riserva ("*salvo che il fatto costituisca più grave reato*") contenuta nel primo capoverso dell'art. 167 medesimo, la disposizione stabilisce che il trattamento illecito [44], effettuato con il dolo specifico di ottenere per sé o per altri un profitto o di recare ad altri un danno, "*se dal fatto deriva nocumento*" a terzi, vale a dire un pregiudizio non necessaria-

---

sentenza 28 maggio 2012, n. 8451. In senso conforme, in relazione alla pubblicazione all'albo pretorio di dati idonei a rivelare lo stato di salute di un dipendente da parte di un comune, v. Corte di Cassazione, sez. I civile, sentenza 13 febbraio 2012, n. 2034.

[43] Pertanto, alla luce dei principi generali, si presuppone che laddove il soggetto abbia adottato le misure di cui all'art. 33 del d.lgs. n. 196/2003, non incorrerà nella sanzione di tipo penalistico di cui all'art. 169, che qualifica come fatto costituente reato appunto la mancata adozione degli accorgimenti previsti nell'art. 33 citato. Tuttavia, qualora tali disposizioni siano state superate dall'evoluzione tecnologica, e non ne sia stato tenuto conto nelle modalità di organizzazione dell'attività pericolosa, il soggetto incorrerà comunque nella responsabilità civile *ex* art. 15 del d.lgs. n. 196/2003.

[44] Secondo quanto disposto dal legislatore, la sussistenza del delitto di cui all'art. 167 è rinvenibile nel trattamento effettuato in violazione delle disposizioni di cui agli artt. 18 e 19 (trattamenti effettuati da soggetti pubblici in relazione a dati diversi da quelli sensibili e giudiziari); 23 (relativo alle modalità di prestazione del consenso); 126 (dati relativi all'ubicazione), 130 (comunicazioni indesiderate) ovvero "*in applicazione dell'art. 129*" (disposizione riguardante il rispetto delle modalità di utilizzo dei dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del pubblico, individuate con provvedimento del Garante per la protezione dei dati personali in cooperazione con l'AGCOM). Quest'ultima precisazione consegna all'interprete una formulazione ambigua e poco felice della norma in quanto, da un lato, l'illiceità del trattamento è determinata dall'inosservanza di un provvedimento del Garante (per cui il contenuto precettivo è desumibile solo dalla fonte secondaria e solo da questa si può ricavare la regola di condotta per il caso concreto, lasciando così trapelare un'ipotesi di norma penale in bianco, cui si accompagnano tutti i noti e irrisolti interrogativi dogmatici in ordine all'effettivo rispetto dei principi costituzionali); dall'altro, si profila la possibilità di escludere la punibilità dell'agente *ex* art. 47, comma 3, c.p. per errore sulla legge (*rectius* fonte) extrapenale, richiamata dall'art. 167. Sulla portata delle norme penali in bianco e dell'errore nell'ordinamento penale v., più diffusamente, F. MANTOVANI, *Diritto penale-parte generale*, Cedam, Mi-

mente di carattere patrimoniale, è punito con la reclusione da sei a diciotto mesi.

Quest'ultimo inciso introduce una condizione obiettiva di punibilità all'interno della fattispecie, pertanto l'applicabilità della pena risulta subordinata alla presenza della particolare circostanza (*sub specie* di evento futuro e incerto, concomitante o successivo rispetto alla condotta dell'agente, che si aggiunge ai tipici elementi costituitivi essenziali del reato) di aver arrecato nocumento a terzi [45]. La lesione del bene-interesse tutelato in questo caso è identificabile nel diritto alla protezione dei dati personali dell'interessato; tuttavia, secondo un'interpretazione letterale della norma, nel caso in cui il trattamento illecito viene realizzato mediante comunicazione o diffusione dei dati, il fatto tipico sembrerebbe presentare una maggiore offensività, tant'è che, da un lato, la condotta risulterebbe sempre punibile, a prescindere dalla realizzazione di un pregiudizio a terzi; dall'altro, comporterebbe la diversa, e più pesante, pena nel suo massimo edittale (in quanto colui che ha commesso l'illecito viene punito con la reclusione da sei a ventiquattro mesi ai sensi dell'art. 167, comma 1, secondo periodo). Le medesime osservazioni potrebbero applicarsi, *mutatis mutandis*, in relazione al comma 2, dell'art. 167, che sanziona, "*se dal fatto deriva nocumento*", il trattamento illecito effettuato in violazione di norme poste a tutela di alcuni dati che, per la loro intrinseca particolarità [46], comportano una sanzione variabile da uno a tre anni di reclusione [47].

In tale quadro, spetta all'interprete individuare gli elementi che, ai sensi del d.lgs. n. 196/2003 medesimo, sostanziamo la

lano, 2013, VIII ed., pp. 3 e ss., nonché 369 e ss.

[45] La giurisprudenza si è espressa in diverse occasioni sul concetto di nocumento quale condizione obiettiva di punibilità; *ex multis*, v. Corte di Cassazione, sez. V penale, sentenza 25 giugno 2009, n. 40078 (la cui lettura, per avere piena contezza della vicenda, non può prescindere da Corte di Cassazione, Sezioni Unite Penali, sentenza 27 ottobre 2011, n. 4694). Sui concetti di "titolare" del trattamento e di "danno patrimoniale apprezzabile" arrecato all'interessato, v. Corte di Cassazione, sez. III penale, sentenza 17 febbraio 2011 (dep. 1° giugno 2011), n. 21839; e ancora, v. Corte di Cassazione, sez. III penale, sentenza 28 maggio (dep. 9 luglio 2004), n. 30134.

[46] Vengono infatti sanzionate le operazioni effettuate in violazione degli artt. 17 (trattamento che presenta rischi specifici); 20, 21 e 22 (trattamento di dati sensibili e giudiziari da parte di soggetti pubblici); 25 (divieto di comunicazione e diffusione di dati); 26 e 27 (trattamenti di dati sensibili o giudiziari da parte di privati) e 45 (trasferimento di dati all'estero).

[47] La complessa architettura normativa su cui poggia la norma in questione induce l'interprete a sottolineare come la condotta tipica qui potrebbe manifestarsi sia in forma commissiva, sia in forma omissiva, in corrispondenza della diversa configurazione che il fatto di reato riceve nei primi due periodi delle disposizione incriminatrici. La singolarità della fattispecie in questione emergerebbe altresì sotto altri aspetti: infatti, l'art. 167, commi 1 (primo periodo) e 2, sembrerebbe configurare un illecito di danno, poiché appare necessario che si arrechi un nocumento affinché la condotta assuma rilevanza penale, mentre il comma 1, secondo periodo della norma, nel sanzionare la "*comunicazione o diffusione*" sembrerebbe invece riconducibile alla tipologia degli illeciti di pericolo.

responsabilità dell'agente nel caso concreto, al fine di ricondurre l'evento nell'alveo delle fattispecie sanzionate.

L'indagine, però, si prospetta alquanto ardua in relazione ai *wearable devices*: se è pur vero che il fruitore è il soggetto che effettua il trattamento (e che assumerebbe il ruolo di titolare ai sensi degli artt. 4, comma 1, lett. *f*, e 28 del d.lgs. n. 196/2003), e ferma restando l'antigiuridicità della sua condotta se viola, ad esempio, i principi di liceità e correttezza, è anche vero che lo stesso non è certo in grado di adottare i necessari accorgimenti tecnici per garantire la sicurezza dei dati personali, che sono di stretto appannaggio del produttore. In tal caso, la difficoltà di individuare la reale titolarità — nonché la finalità (personale o meno)- del trattamento, genera il rischio di una sovrapposizione di responsabilità ovvero di zone franche in cui nessuno risponde di eventuali violazioni [48].

Si profilano, quindi, problemi ermeneutici in relazione alle disposizioni del d.lgs. n. 196/2003 che, per come sono attualmente strutturate, non sembrano adattarsi pienamente al trattamento di dati personali tramite i dispositivi indossabili.

4. Costi e benefici del *wearable computing*: un equilibrio perfetto o uno sbilanciamento da livellare?

I profili di criticità emergenti dalla diffusione dei dispositivi indossabili non rappresentano un assioma assoluto, essendo innegabile che i prodotti derivanti dall'avanzamento tecnologico non vanno demonizzati ma, anzi, comportano evidenti benefici in

[48] A conferma della difficoltà di districare la matassa delle responsabilità nell'utilizzo di tali strumenti si veda il noto caso "*Vivi Down*": se in primo grado tre dirigenti di *Google Inc.* sono stati condannati per violazione della privacy in merito a un video caricato nel 2006 su *Google Video*, sostituito poi da *YouTube*, che ritraeva un minore disabile insultato e malmenato da alcuni compagni di scuola (v. Tribunale Milano, sez. IV penale, sentenza 24 febbraio — 2 aprile 2010, n. 1972), in sede di appello tale pronunciamento è stato completamente ribaltato con l'assoluzione degli imputati perché "il fatto non sussiste". Si è sostanzialmente ritenuto, infatti, che ogni violazione perpetrata dagli utenti non può tradursi in una responsabilità del fornitore del servizio, in quanto del trattamento dei dati ne risponde l'*uploader* del video e non la piattaforma di *hosting*, poiché i *provider* non possono selezionare preventivamente i contenuti caricati sulle proprie piattaforme. Nel caso di specie, poi, non è stata ravvisata la sussistenza del dolo specifico, non potendo, secondo la Corte di appello, ritenersi che questo coincida "*con il fine di profitto costituito dalla palese vocazione economica dell'azienda Google*" "*mancando qualsiasi riscontro di un vantaggio direttamente conseguito dagli imputati*", mentre la struttura della norma "*postula la necessaria partecipazione psichica intenzionale e diretta del soggetto al raggiungimento di un profitto*". Inoltre, il trattamento è avvenuto senza che all'interessato fosse fornita l'informativa *ex* art. 13 del d.lgs. n. 196/2003, ma tale comportamento omissivo non è sanzionato dall'art. 167 del d.lgs. n. 196/2003, obbligo che peraltro grava sul titolare del trattamento e non su terzi soggetti, dunque sull'*uploader* del video e non su *Google Inc.* (v. Corte di appello di Milano, sez. I penale, 27 febbraio 2013, n. 8611). Tale orientamento è stato convalidato con l'assoluzione pronunciata anche dalla Corte di Cassazione, sez. III penale, udienza del 17 dicembre 2013 (le cui motivazioni, al momento della stesura del presente saggio, non sono state ancora depositate).

termini di agevolazione delle attività quotidiane. E non solo: l'effetto positivo indotto, nelle relazioni interpersonali, dai dispositivi indossabili risiede anche nella maggiore sicurezza nel sistema sociale generata dal passaggio della sorveglianza "imposta dall'alto" alla "*sousveillance*", cioè alla "vigilanza diffusa dal basso" [49]. Secondo tale orientamento, infatti, la possibilità offerta a chiunque di utilizzare dispositivi che permettono un contatto immediato con il *web*, dove fare confluire le informazioni su tutti, raccolte finanche all'insaputa degli interessati, genera anche un consistente incremento del controllo sociale, che si riflette a sua volta in una maggiore sicurezza personale dei singoli [50].

Per contro, la prevalenza delle esigenze di sicurezza rispetto quelle di libertà individuale rischia di portare ad un consolidamento di un vero e proprio *panoptycon* sociale generalizzato, in cui ognuno controlla gli altri e tutti sono controllati costantemente.

Se è pur vero che già l'utilizzo dei "normali" dispositivi mobili

[49] Ciò in contrapposizione alla sorveglianza che invece evoca, con il suffisso "sor-", l'idea di un controllo di sistema esercitato dall'alto. La *sousveillance* è l'inverso della sorveglianza di "sistema" (governativa, di settore, ecc.): essa si basa sul controllo diffuso, granulare e capillare che crea, attraverso le risorse offerte dal *wearable computing*, una comunità di singoli che, autonomamente, "spiano gli spioni" (*watch the watchers*) capovolgendo la gerarchia tradizionale, contribuendo all'affermazione di un'intelligenza collettiva e a un'info-anarchia, introducendo un nuovo livello (estremo?) di trasparenza nel sistema sociale. Tale assioma, nell'applicazione pratica, può subire dei opportuni temperamenti: si veda il Provvedimento del Garante per la protezione dei dati personali che ha vietato l'uso di *webcam* installate in un asilo nido privato con cui si intendeva consentire ai genitori di monitorare costantemente via *web* l'attività dei figli. La asserita finalità di tutelare l'incolumità dei minori e garantire la tranquillità dei genitori è stata bilanciata con altri interessi fondamentali del bambino, quali la sua riservatezza e il libero sviluppo della personalità (v. *Sistema di videosorveglianza tramite webcam in grado di consentire ai genitori il controllo a distanza dei propri figli minori durante il periodo di permanenza in asilo nido*, 8 maggio 2013, in *www.garanteprivacy.it*, doc. *web* n. 2433401).

[50] Secondo il controverso ricercatore canadese Steve Mann, considerato il padre del *wearable computing*, quest'ultimo ha concretizzato il sogno di una completa sicurezza personale, di una connessione alle macchine senza fili, di una perfetta mobilità e libertà, offrendo la possibilità di poter usufruire di una memoria collettiva e di un'intelligenza umanistica condivisa, come profetizzò in suo celebre saggio intitolato *Wearable computing as means for personal empowerment*, presentato nel 1998 all'*International Conference on Wearable Computing ICWC-98*. Secondo tale scuola di pensiero, il *wearable compunting* esalta le potenzialità dei computer che portano alla costruzione di una realtà mediata, potenziata nelle sue possibilità funzionali, personali, sociali e politiche. In effetti, occorre scindere l'applicazione pratica del *wearable computing* dagli aspetti etici che governano e risiedono alla base di questa, come di ogni altra forma, di espressione umana. Sarebbe infatti estremamente riduttivo inquadrare il *wearable computing* come una mera evoluzione tecnica delle risorse informatiche a disposizione dell'uomo. Ciò in quanto è innegabile che il computer non opera più come uno strumento di mera emulazione dell'intelligenza umana (*Artificial Intelligence*, AI), bensì come una reale estensione di mente e corpo. Il computer non è più un'entità separata, ma agisce in combinazione sinergica con l'essere umano, in modo che entrambi possano compiere al meglio le proprie funzioni e capacità. Si crea, allora, un'interazione costante e senza precedenti con l'individuo, un *feedback loop* formato dalla somma dei fattori coinvolti (uomo-macchina) e che produce una vera e propria "intelligenza umanistica" (*Humanistic Intelligence*, HI).

(*smartphone*, *tablet*, ecc.) configura analoghe problematiche — in quanto anche questi strumenti raccolgono una gran mole di informazioni e sono dotati di fotocamere, *GPS* e connessione *web* [51] — va tenuta presente una differenza fondamentale: la accessibilità continua che caratterizza i *wearable devices*. Infatti, se la fotocamera di uno *smartphone* funziona solo ove venga attivata ed acquisisce unicamente le immagini prescelte dall'utente (si pensi alla moda dilagante dei *selfies*, gli autoscatti effettuati dal fruitore stesso e poi postati sui *social network*), le telecamere installate nei dispositivi indossabili, invece, possono essere attive in modo continuo e funzionare autonomamente, con conseguenze inimmaginabili se utilizzati in luoghi "sensibili" come ospedali, scuole, banche o pubbliche *toilettes*.

Ulteriore fattore problematico riguarda la continua interconnessione dei dispositivi indossabili con il *web*: la rete, per sua natura, non conosce limiti né di tempo, né di spazio e si alimenta dei dati immessi dagli utenti, per lo più privi di contestualizzazione. Essa è un illimitato collettore e diffusore di conoscenza ove le informazioni vengono raccolte, archiviate, veicolate e rese disponibili in assenza di una chiara forma di regolamentazione da parte dei sistemi giuridici tradizionali che ne disciplini l'utilizzo o la durata nel tempo della loro conservazione/messa a disposizione; è un mondo ove il principio di territorialità del diritto (e quindi la sua applicabilità) rischia di essere vanificato proprio dall'assenza di confini e di regole.

Tali intrinseche peculiarità denotano l'evidente pericolo che i *wearable devices* possano trasformarsi anche in uno strumento pesantemente invasivo della sfera privata delle persone: non è poi così inverosimile temere che — sotto il profilo della privacy

---

[51] È opinione diffusa, tra gli addetti ai lavori, che i *wearable devices* non si differenziano da altri strumenti tecnologici, parimenti invasivi della sfera di riservatezza altrui, ma sostanzialmente legittimati e accettati nella percezione comune, come nel caso della videosorveglianza. A ben vedere, il paragone appare sproporzionato se si pensa ad una serie di fattori che caratterizzano (e differenziano) le apparecchiature in questione: in primo luogo l'ampiezza della diffusione, in quanto probabilmente nel prossimo futuro ogni individuo potrebbe essere dotato di uno o più *wearable device*, mentre le telecamere per la videosorveglianza saranno presumibilmente sempre in numero limitato rispetto alla popolazione nel suo complesso. Va poi considerata la pervasività dello strumento, visto che i *wearable devices* si "muovono" nello spazio, insieme al fruitore, mentre le telecamere sono installate in un luogo fisso potendo, al massimo, ruotare su se stesse; nonché la diffusione delle informazioni raccolte, considerato che le videoriprese non vengono automaticamente condivise nei *social networks*, mentre con i dispositivi indossabili questa rientra tra le principali opzioni. Va inoltre ricordato che mentre le disposizioni giuridiche disciplinanti l'uso delle tecnologie sono generalmente molto dettagliate e puntuali per la videosorveglianza, risultano ancora sostanzialmente inesistenti (e quelle in vigore decisamente inadatte) per i *wearable devices*. Infine la possibilità di essere coscienti delle riprese: gli impianti di videosorveglianza devono quasi sempre essere appositamente segnalati, e comunque è più facile accorgersi della presenza di una telecamera ambientale che di un dispositivo indossabile.

personale — i costi, nel tempo, possano di gran lunga prevalere sui benefici, se non si individuano opportune forme di tutela.

5. Primi accorgimenti tecnici proposti dai produttori dei dispositivi indossabili a tutela della privacy.

I timori sopra evidenziati non sembrano essere poi così infondati, visto che già i produttori delle tecnologie *wearable* prevedono che i dispositivi possano avere, in un prossimo futuro, la capacità di "incapsulare" l'utente in una sorta di "bolla" esperienziale per proteggerlo da determinate sollecitazioni provenienti dal mondo esterno.

In altri termini, se appositamente progettato e programmato, un dispositivo indossabile potrebbe funzionare come un filtro in grado di bloccare informazioni indesiderate provenienti dal *cyberspazio* (si pensi allo *spam* pubblicitario o alle comunicazioni offensive). Il filtro potrebbe agire direttamente sulla comunicazione veicolata dal *device*, ma anche su quella che transita su dispositivi collegati, e in alcuni casi può interagire con l'ambiente circostante, virtuale e reale, impedendo il contatto sensoriale con stimoli indesiderati o sgradevoli (ad esempio, si potrebbero impostare gli occhiali intelligenti per "non vedere" certe cose). Così, senza arrivare ad una interruzione della comunicazione in ingresso, il *device* potrebbe consentire di vivere una sorta di "realtà attenuata", in cui determinati messaggi o stimoli non penetrano.

In futuro, una tecnologia indossabile potrebbe altresì renderci, parzialmente o totalmente, invisibili, ovviamente nel *cyberspazio*. È possibile, quindi, immaginare dei capi di abbigliamento *smart* capaci di diffondere radiofrequenze che bloccano la capacità di visionare e interagire con altri dispositivi, per i quali si diventa di fatto virtualmente "invisibili" (si pensi a un soggetto che indossa una camicia "intelligente" e non può essere visto o riconosciuto da chi indossa occhiali "intelligenti").

Pur essendo ancora in larga parte in fase sperimentale, tali opzioni tecnologiche aprono tuttavia scenari interessanti e complessi: il futuro potrebbe fondarsi su una sorta di "antagonismo" digitale, dove si fronteggiano, da un lato, coloro che scandagliano l'ambiente reale e virtuale alla ricerca di informazioni e dati al fine di amplificare il proprio bagaglio conoscitivo, nonché la loro capacità di interconnessione e operatività, e, dall'altro, quei soggetti che, su un fronte opposto, si propongono di difendere la propria privacy dalle ingerenze altrui.

6. Le conseguenze delle innovazioni tecnologiche e il "percorso a ritroso" che dalla protezione dei dati personali (ri)porta alla valorizzazione della riservatezza.

Come è noto il diritto alla privacy o alla riservatezza ha trovato

fondamento nel tradizionale *right to be let alone*, il "diritto a essere lasciati soli", coniato dalla dottrina statunitense nel 1890 [52], allora individuato essenzialmente nello *jus solitudinis*, cioè nel diritto a non subire ingerenze altrui nella propria sfera di riservatezza.

Nel corso del tempo il diritto alla riservatezza si è trasfuso nel più ampio "diritto alla protezione dei dati personali", con cui è stata riconosciuta la pretesa ad una tutela a tutto campo dei dati personali, non più limitata alla riservatezza nei suoi termini essenziali (*rectius* al diritto ad essere lasciato solo e non subire ingerenze illecite nella propria individualità), ma che si estende alla persona nel suo complesso, e che si traduce anche nella c.d. autodeterminazione informativa, intesa quale diritto ad una corretta (ri)costruzione o rappresentazione della propria identità, che non può essere soddisfatta con il semplice diritto alla riservatezza, ma viene incrementata con nuove facoltà volte a controllare la forma, la consistenza e la circolazione delle informazioni personali, che devono rispecchiare esattamente la attuale identità dell'interessato.

Il diritto alla riservatezza, dunque, da libertà negativa, consistente nel diritto a essere dimenticato, nel corso del tempo è stato ampliato, cioè declinato anche in termini di libertà positiva, intesa come potere di controllo sui propri dati personali. Il diritto alla protezione dei dati personali si è evoluto ed arricchito nell'elaborazione giuridica: non più limitato alla mera tutela della riservatezza, ma si è esteso fino a ricomprendere anche l'identità personale, cioè l'interesse del soggetto ad una esatta percezione sociale della propria personalità, che trova concreta attuazione nella libertà di mantenere il controllo sul flusso dei dati e sulle informazioni che riguardano e identificano l'individuo (concezione dinamica) [53]. Ciò in modo che l'informazione oggetto di trattamento costituisca una fedele, e quindi corretta, rappresentazione dell'attuale, integrale ed effettiva identità personale dell'interessato, aggiornata secondo l'immagine riverberata dallo stesso nel mondo delle relazioni sociali nel corso della propria esistenza [54].

[52] Ci si riferisce al noto articolo *The Right to Privacy*, ad opera di SAMUEL D. WARREN e LOUIS D. BRANDEIS, pubblicato sul fascicolo del 15 dicembre 1890 della *Harvard Law Review*.

[53] Sul concetto e la portata dell'identità personale si è anche espressa la Corte Costituzionale evidenziando che essa è un bene *ex se*, indipendentemente dalla condizione personale e sociale, dai pregi e dai difetti dell'interessato. Essa si esplicita nel diritto ad essere sé stesso, che esige il rispetto dell'immagine di partecipe alla vita associata di ognuno, con il relativo bagaglio di idee ed esperienze, convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo. V. Corte Costituzionale, sentenza 24 gennaio-3 febbraio 1994, n. 13.

[54] In ordine all'evoluzione nel tempo della nozione di riservatezza e di identità personale si rinvia a G. FINOCCHIARO, Voce *Identità personale (diritto alla)*, in *Digesto delle discipline privatistiche*, Sez. civ., Agg., Torino, 2010; G. PINO, *Il diritto all'identità personale ieri e oggi. Informazione*,

Tale risvolto del diritto alla privacy è diventato una componente prevalente delle azioni di tutela esercitate dagli interessati, anche a seguito del consolidamento degli strumenti informatici e, soprattutto, di Internet dove confluiscono numerosissime informazioni, per lo più prive di contestualizzazione, cioè di collegamenti alla fonte originaria e ad altre notizie in grado di completare e riflettere il profilo attuale di una persona.

Con l'avvento dei *wearable devices*, non sembra azzardato ipotizzare una sorta di ridimensionamento del diritto alla protezione dei dati personali nelle sue poliedriche sfaccettature: in particolare, la componente riguardante la tutela dell'identità personale, pur mantenendo una sua indubbia rilevanza, verrà verosimilmente compressa da una (antica o nuova?) esigenza preponderante, cioè quella di garantire in via prioritaria la riservatezza *tout court*, cioè di mettere al riparo da intrusioni altrui una sfera intangibile di intimità e riserbo dell'individuo [55]. Ecco allora che si registrerà, presumibilmente, una valorizzazione della concezione originaria del diritto alla privacy nei suoi termini essenziali, ovvero un "ritorno al futuro", per cui la tutela dell'identità personale, o comunque dell'immagine di sé stesso che il soggetto intende rappresentare nell'ambito delle relazioni sociali scevra da eventuali distorsioni operate da terzi, che tanto ha impegnato finora dottrina e giurisprudenza, verrà compressa dalla contestuale espansione del diritto alla riservatezza, cioè dello *ius excludendi alios* rispetto a fatti e circostanze che i terzi non hanno diritto di conoscere [56].

---

mercato, dati personali, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, Tomo I, p. 257; L. Trucco, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Torino, 2004, p. 316; G. Buttarelli, *Banche dati e tutela della riservatezza*, Milano, 1997, pp. 105 e ss.; G. Resta, *Identità personale e identità digitale*, in *Il diritto dell'informazione e dell'informatica*, 1997, p. 511.

[55] Ciò inizia a trovare conferma anche a livello internazionale: ne è nn chiaro esempio una risoluzione ONU con cui gli Stati parte sono stati sollecitati ad attivarsi per prevenire le violazioni del "diritto umano alla privacy", poiché nel mondo *online* i diritti devono godere della stessa tutela offerta loro nel mondo reale. V. United Nations, General Assembly, *The right to privacy in the digital age*, A/C.3/68/L.45/Rev.1, 20 November 2013.

[56] Secondo altri, invece, è in atto un mutamento genetico della privacy per cui da diritto individuale è divenuta "*una negoziazione collettiva tra Stati, imprese e attori della società civile per decidere chi ha il diritto di accedere ai dati personali e con quali finalità. Una negoziazione tra gli utilizzatori per decidere cosa condividere e con chi*" in una realtà dove "*si moltiplicano le pressioni discordanti da parte dei governi nazionali, che, da una parte, impongono di svelare e, dall'altra, di proteggere i dati personali dei loro cittadini*". In tal senso A. Casilli, *Fine della privacy: la grande beffa di Zuckerberg*, in *Corriere della sera-inserto cultura*, 19 gennaio 2014. Per un'analisi di più ampio respiro delle problematiche che intrecciano indissolubilmente privacy e libertà, diritto alla riservatezza del singolo individuo e libertà di informazione, facilità di accesso all'universo telematico e garanzia che quello strumento

7. Non solo tecnologia, ma anche diritto per contemperare i diversi interessi in gioco.

Alla luce degli scenari futuristici sopra delineati, ciò che farà probabilmente la differenza non sarà solo l'evoluzione della tecnologia e dei mezzi di tutela tecnici: a questi deve essere affiancata, in via speculare, la produzione di regole idonee a disciplinare l'utilizzo delle tecnologie indossabili che non abbiano l'effetto, si badi bene, di imbrigliare le potenzialità creative degli sviluppatori delle più moderne tecnologie, bensì di bilanciare i diversi interessi in gioco.

Non si esclude che, anche in tempi brevi ed autonomamente, i produttori e i fornitori dei *wearable devices* e di servizi collegati possano produrre dei codici di autoregolamentazione o delle *privacy policies* [57], così come lo stesso mercato dei fruitori potrebbe elaborare spontaneamente delle forme di "*etiquette*" per auto-regolamentare le modalità d'uso dei dispositivi in questione.

Tuttavia, la gestione degli strumenti indossabili non può essere lasciata esclusivamente alla libera auto-regolamentazione di produttori e fruitori: come si è visto, le disposizioni attualmente in vigore denunciano una intrinseca obsolescenza o inadeguatezza a disciplinare il relativo utilizzo. Occorre quindi iniziare ad ripensare e, conseguentemente, aggiornare la disciplina in materia di protezione dei dati personali, che deve tenere in adeguata considerazione anche i nuovi sviluppi nel campo del *wearable computing* [58].

Questa rivisitazione ordinamentale non può essere operata entro gli angusti confini dei sistemi giuridici nazionali, ma necessita

non diventi un mezzo di dominio delle collettività organizzate, cfr. S. Rodotà, *Intervista su privacy e libertà*, 2005, pp. 153.

[57] Su benefici e limiti legati all'uso di *privacy policies*, si rinvia a C. Burton, *Departing from the reliance on lengthy legalese*, in *Data Protection Law & Policy*, 2013, p. 14. In senso critico cfr., altresì, F. Bernabè, *Libertà vigilata. Privacy, sicurezza e mercato nella rete*, 2012, p. 166, il quale sottolinea come la difficoltà di tutelare la privacy in questi ambiti richiede uno sforzo comune da parte di tutti i soggetti coinvolti: operatori, attori del mondo Internet, autorità preposte alla tutela della privacy. Su questa linea si è mosso anche S. Rodotà, con una accurata riflessione sulla complessità di un fenomeno, quello del mondo digitale, che rivela anche gli scompensi dell'ordinamento, con un diritto invasivo in molti settori e assente dove più se ne avvertirebbe il bisogno, come evidenzia in *La vita e le regole. Tra diritto e non diritto*, 2009, pp. 284.

[58] A conferma della difficoltà di intervenire in tale settore, in proposito si è espresso anche A. Soro, Presidente del Garante privacy, invocando il superamento dei tradizionali strumenti di regolamentazione normativa. Egli, nel quadro della citata iniziativa avviata in seno al *GPEN* sui *Google Glass*, ha affermato che "*Le nuove tecnologie sono state sempre connotate dal binomio "opportunità-rischi", ma certo i Google Glass lasciano prevedere grandi pericoli per la vita privata. Chiunque finisse nel raggio visivo di chi indossa questi occhiali potrebbe, a quanto è dato sapere, venire fotografato, filmato, riconosciuto e, una volta avuto accesso ai suoi dati sparsi sul web, individuato nei suoi gusti, nelle sue opinioni, nelle sue scelte di vita. La sua vita gli verrebbe in qualche modo sottratta per finire nelle micro memorie degli occhiali o rilanciata in rete. Ci sono già norme che vietano la messa online di dati personali senza il consenso degli interessati. Ma di fronte a questi strumenti le leggi non ba-*

di una sinergia a livello internazionale o, meglio ancora, sovranazionale, considerata sia l'ubicazione geografica di gestori e produttori dei nuovi dispositivi (aventi spesso sede al di fuori dei confini nazionali) [59], sia la stretta interrelazione dei dispositivi indossabili con il *web* [60]; ulteriore, apprezzabile fine dovrebbe essere quello di disciplinare compiutamente, al pari di quanto viene effettuato nel mondo reale, anche le relazioni interpersonali germogliate nel *cyberspazio* [61]. L'obiettivo — ambizioso, estremamente delicato e da perseguire in modo tale da non intaccare il principio di neutralità della rete — non è solo quello di preservare una sfera intangibile di riservatezza dell'individuo, ma anche di garantire un corretto utilizzo di dispositivi sempre più avveniristici che proiettano la persona in un mondo immateriale, quale quello di Internet, ma non per questo meno reale, foriero di diritti e doveri reciproci.

Si tratta di un auspicio che dovrebbe trovare sostegno anche presso i produttori delle tecnologie *wearable*, i quali saranno

---

stano: serve un salto di consapevolezza da parte di fornitori di servizi Internet, degli sviluppatori di software e degli utenti. È indispensabile ormai riuscire a promuovere a livello globale un uso etico delle nuove tecnologie" (v. comunicato stampa del 18 giugno 2013).

[59] Illuminante, sul punto, l'esito di un ricorso avverso *Google Italy s.r.l.* instaurato presso il Garante per la protezione dei dati personali, volto ad ottenere la cancellazione di taluni dati personali presenti su una pagina *web* relativa ad un *newsgroup* (in *Decisione su ricorso* del 2 febbraio 2006, *www.garanteprivacy.it*, doc. *web* n. 1244676). V., più recentemente, il parziale "ripensamento" espresso dal Garante su tali tematiche a seguito dell'istruttoria avviata, nell'ambito di una *task force*, appositamente costituita, composta dalle Autorità per la protezione dei dati di Francia, Germania, Regno Unito, Paesi Bassi e Spagna, in merito al complessivo trattamento di dati svolto da *Google Inc.* e dalle altre società del gruppo o al medesimo collegate, specie con riferimento al profilo concernente l'applicabilità a tali trattamenti della direttiva 95/46/CE, nonché delle disposizioni nazionali di recepimento della stessa (v. *Decisione su ricorso del 30 maggio 2013*, sopra citata, nonché comunicati stampa del 20 giugno, del 2 aprile 2013 e del 16 ottobre 2012).

[60] Proprio in questa direzione si muove l'Unione europea, che ha adottato una proposta di regolamento al fine di sostituire la direttiva 95/46/CE in materia di protezione dei dati personali con l'obiettivo, tra gli altri, di instaurare un quadro giuridico più solido e coerente in materia nel territorio dell'Unione. La proposta di regolamento, che verrà affiancato da efficaci misure di attuazione, si propone di consentire altresì lo sviluppo della c.d. economia digitale e dei relativi diritti, in modo da rispondere adeguatamente alle sfide emergenti dalla crescente globalizzazione e dalla natura fortemente innovativa delle tecnologie digitali, nonché dalla radicalità dei loro effetti su economia, società e cultura. V. *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Council of the European Union, 17831/13, Brussels, 16 December 2013. Negli Stati Uniti, punto di riferimento importante dove risiedono molti degli "*over the top*" emergenti come *Facebook*, *Google Inc.*, ecc., non mancano le iniziative di carattere legislativo, come il *Social Networking Online Protection Act* (in *https://www.govtrack.us/congress/bills/113/hr537/text*), all'esame del Congresso, con cui si intende vietare alle imprese di accedere ai dati personali che i dipendenti o gli aspiranti all'assunzione abbiano posto su un *social network*.

[61] Il condizionale è d'obbligo, se si considera l'aspro dibattito, mai sopito, sull'opportunità di regolamentare o meno il *web*. Ipotesi che, comunque, richiede anche un ripensamento degli strumenti normativi tradizionali a nostra disposizione, come sottolineato da S. Rodotà, *Una Costituzione per Internet?*, in *Politica del diritto*, 2010, n. 3, p. 337.

verosimilmente chiamati, in ambito europeo, a rispettare i canoni della *privacy by-design* e della *privacy by-default* [62], principi innovativi ed a spiccata vocazione preventiva, volti ad impegnare i titolari dei trattamenti (specie se operanti nel *web*) ad adottare misure tecniche che garantiscano, sin dalla progettazione del prodotto o dell'infrastruttura informatica, un utilizzo di dati personali conforme alle disposizioni in materia di protezione dei dati personali, elementi che costituiranno non un costo o un aggravio burocratico, bensì un valore aggiunto di cui i fruitori non potranno non tenerne conto nella scelta del loro *device*.

Abstract

Wearable devices are an innovative type of small-sized, or even tiny, computing device that can be worn directly on the user's body and can often operate uninterruptedly and automatically. On account of their technological characteristics, operating mode and the quantity and quality of personal data collected (which may often be of a sensitive nature), these devices raise a number of new and important issues in terms of both user privacy and the privacy of third parties that may be "intercepted" by the field of action of such devices, for example through micro-cameras they are often equipped with. As well as describing the technical features and the possible usages of wearable devices, this paper outlines scenarios of legislation to appropriately handle the personal data collected, processed and stored by these devices; to that end, special consideration is given to the legislation already in force and the need to reconcile the right to free access to information with the right to privacy.

---

[62] V. art. 23 della proposta di regolamento che sostituisce la direttiva 95/46/CE in materia di protezione dei dati personali, *cit.* Si ricorda, inoltre, che il regolamento si propone di estendere i confini della sua applicabilità, in quanto riguarderà anche il trattamento dei dati personali, concernenti persone residenti nell'Unione europea, effettuato da chi non è stabilito nel territorio europeo, purché il trattamento riguardi l'offerta di beni o la prestazione di servizi ai suddetti residenti o il controllo del loro comportamento o, infine, se il titolare del trattamento è comunque stabilito in un luogo soggetto al diritto nazionale di uno Stato membro in virtù del diritto internazionale pubblico (art. 3, par. 2).