Eunomia. Rivista semestrale di Storia e Politica Internazionali
Eunomia VIII n.s. (2019), n. 1, 155-178
e-ISSN 2280-8949
DOI 10.1285/i22808949a8n1p155
http://siba-ese.unisalento.it, © 2019 Università del Salento

MARCO MANCARELLA

La società digitale nel contesto internazionale: tra controllo, libertà e nuovi diritti

Abstract: The digital society is characterized by new forms of surveillance and control, capable of affecting freedom and the rights of the person and giving rise to the need to find a new point of balance between public / private interests and the protection of personal data in national and international contest.

Keywords: Surveillance; Control; Privacy; Society; Digital.

1. *La Rete tra libertà "piena" e controllo "totale"*

Una grande mole di dati informatici, di bit che compongono parole, immagini e informazioni di ogni genere viaggia, quotidianamente e ininterrottamente, tramite i canali capillarmente diffusi di Internet, la nota rete telematica che non unisce meramente i computer dell'intero globo, travalicando confini e annullando di fatto ogni tipo di distanza fisica, ma che è anche dotata di una propria vitalità, nutrendosi di tutto ciò che gli utenti immettono *online*. Dalla sua invenzione e proseguendo con il suo sviluppo, essa ha tradotto il desiderio d'interconnessione globale, divenendo uno strumento indispensabile di contatto e comunicazione.

Il carattere "*open access*" la rende, poi, un fenomeno in cui l'utopica aspirazione alla democrazia pare realizzarsi concretamente. Tuttavia, come ben ci si può attendere, tecnologia e progresso non dischiudono meramente gli scenari incoraggianti dell'automazione, dell'interconnessione e dell'*Internet of Things*, ma veicolano con sé anche alti rischi e insidie per gli *e-citizens* e per la garanzia delle loro libertà fondamentali, ragione per la quale è necessario essere criticamente vigili sulle problematiche emergenti.

Benché Internet appaia il più esemplare modello di democraticità esistente, si denota l'emergere di situazioni a dir poco paradossali, soprattutto di criticità in materia di controllo, avulse alla realizzazione dei principi di uguaglianza e partecipazione cui ci si

è riferiti poc'anzi. Internet non si è proposta, quindi, solo come il più grande spazio pubblico che l'umanità avesse conosciuto, ma anche come «un luogo dove la vita cambia qualità e colore, dove sono possibili l'anonimato e la moltiplicazione delle identità, la conoscenza, l'ubiquità, la libertà piena e il controllo totale. In rete ognuno può essere davvero "uno nessuno e centomila" come diceva Luigi Pirandello, e vedere realizzata l'aspirazione dello Zelig di Woody Allen: "Vorrei essere tante persone. Forse un giorno questo si avvererà"».[1]

La dicotomia libertà "piena" e controllo "totale" è esattamente la sintesi dei pro e contro di cui si discorreva nelle righe precedenti: un binomio esplicativo dei risvolti che l'innovazione porta con sé, una libertà quasi smisurata da una parte e la possibilità di esercitare su più fronti grandi poteri di controllo, a danno dei medesimi individui, dall'altra.

Il controllo totale non è prerogativa del mero e singolo individuo, che si trova a gestire poteri mai avuti in precedenza, ma è anche prerogativa di chi realizza un uso sapiente e intrusivo delle tecnologie dell'informazione per esercitare ogni forma d'ispezione possibile sulle informazioni che gli utenti generano a ogni click. È una forma di controllo, quest'ultima, che può prevedere, peraltro, una raccolta indiscriminata di informazioni anche da remoto, senza "inseguire" il controllato, ma semplicemente consultando le sue attività, i siti *web* visitati, le *e-mail* inviate e ricevute, i dati memorizzati sul *Cloud* e le ricerche effettuate.

Si pensi che, profeticamente, il 1 maggio 1999 un intero numero del noto giornale inglese «The Economist» fu intitolato *The End of Privacy* e in esso si mettevano già all'erta i lettori prevedendo un futuro molto poco rassicurante per i diritti civili di ognuno nell'era della postmodernità: unico imputato è il progresso tecnologico e la vittima più colpita è il diritto alla *privacy*.

[1] S. RODOTÀ, *L'uomo nuovo di Internet*, Lectio Magistralis tenuta a Bordeaux il 28 ottobre 2005 per la Laurea Honoris Causa, disponibile in: http://www.privacy.it/archivio/rodo20051028.html, consultato nel mese di maggio 2019.

Si tratta di un problema tendenzialmente universale che non concerne meramente gli utenti del *web* più abituali: tutti siamo coinvolti, giacché i dati di ognuno sono raccolti in molti più database informatici di quanti potremmo mai immaginare.

Le banche dati annoverano al proprio interno una quantità abnorme di informazioni, quasi indecifrabile e esponenzialmente in crescita. A sostegno di ciò, basti considerare la quantità di dati che, intenzionalmente, tutti i giorni, immettiamo nel sistema partendo dall'utilizzo delle carte di credito fino ai trasferimenti di chiamata e messaggi dal mobile, per non parlare poi dei dati personali raccolti in archivi anagrafici, scolastici e sanitari: una serie di dati molto privati che, incrociati tra loro, ci rendono vulnerabili e ovunque rintracciabili.

In sostanza, la vita quotidiana si svolge barcamenandosi nel flusso ininterrotto di informazioni, generato dalle persone stesse, per fruire di beni, servizi, comodità o semplicemente per puro piacere di condivisione.

Come ci ricorda il noto giurista Rodotà: «La grande trasformazione tecnologica cambia il quadro dei diritti civili e politici, ridisegna il ruolo dei poteri pubblici, muta i rapporti personali e sociali, e incide sull'antropologia stessa delle persone. Quali sono le dimensioni della libertà nell'età della scienza e della tecnologia? È giusto invocare la protezione della vita privata, ma non basta. Il nostro modo di vivere è divenuto un flusso continuo di informazioni, inarrestabile, che noi stessi alimentiamo per avere accesso a beni e servizi. La trasparenza sociale ci avvolge. Le tecnologie dell'informazione non solo si impadroniscono della nostra vita, ma costruiscono un corpo elettronico, l'insieme delle nostre informazioni personali custodite in infinite banche dati, che vive accanto al corpo fisico. Il doppio corpo non è più solo quello del Re medievale, di cui ci ha parlato Ernst Kantorowicz. È ormai attributo di ogni cittadino».[2]

La rinuncia all'aspirazione del tanto agognato spazio privato e intimo, da intendere come inviolabile, e alla protezione del proprio "bagaglio" informativo non possono

[2] S. RODOTÀ, *L'uomo nuovo di Internet*, cit.

costituire, ovviamente, il prezzo da pagare per fruire delle facilitazioni forniteci dalla cosiddetta "Società dell'informazione", emblema sociale e rappresentativo della post-modernità. Locuzione, questa, della "Società dell'informazione, che affonda le sue basi nell'elevato dinamismo che caratterizza la società contemporanea, e che colloca l'informazione in una posizione centrale, attribuendole il ruolo di risorsa strategica che condiziona l'efficienza dei sistemi, nonché fattore di sviluppo sociale ed economico.[3]

Alla luce di tali considerazioni, bisognerebbe, pertanto, chiedersi: occorre ancora insistere nel disciplinare e regolamentare il cyberspazio di Internet, salvaguardando diritti e libertà con adeguate misure legislative, ponendo un baluardo a indebite ingerenze della sfera privata e a lesioni di interessi fondamentali dei singoli? Che tipo d'indicazioni ci fornisce la giurisprudenza sovranazionale sul bilanciamento tra libertà di espressione, comunicazione e protezione dei diritti fondamentali e sulla dicotomia tra sicurezza nazionale e *privacy*? Perché continuare a credere che *privacy* e sicurezza siano concetti antitetici e che gli strumenti di sorveglianza elettronica riescano a prevenire ogni forma di atto criminale e terroristico?

Interrogativi aperti, sui quali, oramai da anni, studiosi di diritto e teorici del cyberspazio hanno intrapreso un lavoro di riflessione ad ampio raggio. Una tutela reale della riservatezza personale non è una battaglia persa in partenza. Senza ombra di dubbio, la struttura sociale è mutata drasticamente negli ultimi decenni ma, paradossalmente, ciò mantiene in auge l'aspirazione a rendere concreta la presa di coscienza da parte delle assemblee legislative degli stati, cui far conseguire la realizzazione di efficaci politiche sul trattamento dei dati valide su territorio europeo e internazionale.

L'esercizio del controllo e della sorveglianza, la tutela della *privacy* e del trattamento dei dati personali, il segreto e la trasparenza sono tematiche fondamentali che stanno

[3] La genesi della locuzione "Società dell'informazione" si riconduce agli studi dell'economista austriaco Fritz Machlup e, successivamente, del sociologo statunitense Daniel Bell. Per un approfondimento della tematica, si rinvia a: V. FROSINI, *Genesi filosofica e struttura giuridica della Società dell'informazione*, Napoli, ESI, 2010; M. CASTELLS, *La nascita della società in rete*, Milano, EGEA, 2002; L. SARTORI, *La società dell'informazione*, Bologna, Il Mulino, 2012; M. MEGALE, a cura di, *ICT e diritto nella società dell'informazione*, Torino, Giappichelli, 2016.

connotando, con sfumature inedite, molti aspetti della Società dell'informazione: la trattazione delle suddette ha abbandonato già da qualche tempo la mera sfera del sapere tecnico, interessando non solo i cultori della materia ma, allo stesso modo, l'opinione pubblica e il cittadino.

L'interesse rivolto a tali argomenti è legato visceralmente all'importanza che essi stessi rivestono per la vita di ogni individuo, in quanto ciascun singolo è costretto ad affrontare apertamente questioni giuridiche, politiche e sociali che influenzano i rapporti interpersonali nella vita offline e *online*. Molte di queste questioni non sono inedite, eppure richiedono di essere riviste, rianalizzate con approcci differenti, evidenziando punti critici nel sistema meritevoli di una riflessione più accurata. Analizzando l'assetto teorico e normativo di questi centri d'interesse è possibile, così, tracciare un quadro critico idoneo a testimoniare lo stato della società digitale, con le sue problematiche, e lo stato dei diritti di libertà; sarà possibile, in tal senso, formulare ipotesi concernenti la realizzazione di eventuali misure applicative e di tutela più mirate.

2. *La società digitale e la continua dialettica tra sorveglianza e controllo*

Il binomio "sorveglianza-controllo" è divenuto di grande attualità nell'era digitale: si pensi alla diffusione della videosorveglianza, alla schedatura delle impronte digitali, al controllo del traffico su Internet, all'avvento dei droni per uso militare e poi civile, all'attività di sorveglianza messa a punto dalle grandi aziende di telecomunicazioni o dalle agenzie d'intelligence internazionali. Pratiche, queste, che hanno tratteggiato uno scenario piuttosto preoccupante in materia di violazione dei diritti fondamentali dell'individuo.

Il confronto tra tecnologie delle libertà e tecnologie del controllo diventa sempre più forte, intaccando il trattamento di nuovi tipi di dati personali, sempre più sensibili, e nuovi aspetti della vita privata. Si è profilata una vera e propria "Società sorvegliata",

così come la definisce il sociologo David Lyon,[4] dove ogni forma di potere statale, e non, si serve delle informazioni degli individui per controllarne i comportamenti, sorvegliarne le abitudini e condizionarne le scelte e le azioni future. L'introduzione delle tecnologie informatiche ha facilitato, in tal senso, il perpetrarsi di pratiche di controllo massivo, con metodologie di sorveglianza subdole, inafferrabili e a tratti spregiudicate.

Tuttavia, ancora prima di Lyon, è stato il sociologo statunitense Gary T. Marx a parlare di sorveglianza come elemento cruciale del neofito assetto societario: in un articolo pubblicato sulla rivista «The Futurist» nel 1985,[5] analizzando il radicale cambiamento registratosi nel passaggio dall'era moderna all'era postmoderna, ha parlato di *New Surveillance* ed ha evidenziato il modo in cui le nuove tecnologie, assumendo un ruolo di spicco nell'attuale società, abbiano, di fatto, scalfito gli ultimi baluardi posti contro il controllo "totale" a tutela dei singoli. Peraltro, ha rilevato come il tipo di sorveglianza sviluppatasi con l'avvento dello stato post-moderno si discosti nettamente rispetto alle forme di controllo adottate e previste in precedenza.

Se un tempo lo stato ricorreva alla raccolta e al trattamento dei dati soprattutto per esigenze legate all'amministrazione e alla burocrazia, lo sviluppo delle nuove forme di controllo e d'ispezione non interessa più il mero stato, ma al contempo agenzie e organizzazioni di svariati settori, aziende commerciali e grandi società economiche, che raccolgono ed elaborano informazioni personali su ognuno di noi, senza alcuna remora, per manipolare e controllare interazioni personali, opinioni, abitudini e preferenze.

Il parallelismo tra ieri e oggi serve a constatare che l'urgenza sociale e giuridica di prevedere misure di tutela reali ed efficaci per i diritti della personalità non è legata al fatto che si fronteggia un fenomeno inedito, anzi tutt'altro: il bisogno di controllo

[4] "Società sorvegliata" è la definizione utilizzata dal sociologo David Lyon per descrivere l'assetto societario nell'era digitale e, dunque, nella post-modernità, dominato dall'avvento di nuove tecnologie che rendono di fatto realizzabile il controllo massivo delle masse e la capacità di controllo da parte dei governi, delle major telematiche e delle agenzie di intelligence. Si veda: D. LYON, *Surveillance Society: Monitoring Everydaylife*, Buckingam-Philadelphia, Open University Press, 2001.

[5] Cfr. G.T. MARX, *The Surveillane Society: The Threat of the 1984-Style Techniques,* in «The Futurist», Bethesda (USA), June 1985, pp. 21-26.

sociale è sempre esistito, così come le attività di raccolta dei dati utili a catalogare individui secondo precisi standard e *status*. Ciò che cambia concerne le modalità con cui la nuova sorveglianza pone in essere tali pratiche, rimarcando in maniera evidente gli elementi che la differenziano rispetto alle sfaccettature assunte dalla stessa in precedenza. È interessante vedere, a tal proposito, come Gary Marx individui ben nove marcate differenze che possono essere così riproposte:

1. la "nuova" sorveglianza, fruendo dei moderni dispositivi tecnologici, supera i limiti tecnici che in precedenza rendevano in pratica impossibile l'estensione del controllo sia al di fuori dei confini dello stato sia all'interno delle mura domestiche, negli spazi più intimi della persona umana;
2. la "nuova" sorveglianza trascende il tempo e in virtù di tale considerazione non si evidenzia alcun rapporto d'immediatezza tra la raccolta dei dati e il loro utilizzo, cosicché i dati possono essere elaborati e poi usati in tempi e situazioni diverse senza che se ne pregiudichi l'attendibilità;
3. una rivoluzione strutturale ha investito l'apparato della sorveglianza: a oggi, essa è ad alta intensità di capitale più che di lavoro. Gli sviluppi tecnici, difatti, hanno modificato profondamente l'economia della sorveglianza tant'è che, con estrema facilità, è possibile rimandare l'informazione a una fonte centrale, rendendo possibili economie di scala dove solo poche persone, con ingenti capitali da investire, possono controllare contemporaneamente diversi luoghi e individui;
4. con la "nuova" sorveglianza si è passati dal sorvegliare individui specifici per altrettante specifiche ragioni a sorvegliare tutti, eseguendo un ininterrotto monitoraggio con il sapiente ausilio di telecamere di videosorveglianza, carte di credito e fedeltà, moduli obbligatori da compilare, sensori e dispositivi di geo localizzazione: strumenti, dunque, che ci rendono degli appetibili obiettivi di controllo;
5. l'indiscriminato controllo effettuato sugli individui, poi, è frutto di una politica volta a prevenire violazioni di diversa natura, rimarcando ancora di più la natura

non meramente burocratica o amministrativa degli intenti che sottostanno all'esigenza odierna d'ispezione;

6. la nuova sorveglianza alimenta il meccanismo dell'auto-vigilanza: gli individui sono sovente motivati a fornire spontaneamente e intenzionalmente informazioni personali per fruire di piccoli benefici o per non essere penalizzati;
7. la "nuova" sorveglianza è "invisibile" e "depersonalizzata": è arduo stabilire il quando si è osservati e chi effettua il controllo, perché spesso la sorveglianza è praticata con dispositivi elettronici difficilmente individuabili;
8. grazie agli strumenti tecnici sempre più invasivi si rende effettiva la capacità di estrarre informazioni in profondità;
9. ampie e nuove categorie di persone diventano soggetti di raccolta e analisi delle informazioni e, come aumenta il numero delle persone osservate, cresce quello dei potenziali controllori. Chiunque può essere osservato o essere potenzialmente un osservatore: qualcuno vigila su di noi e noi vigiliamo sul prossimo, sorvegliando ogni suo atteggiamento o movimento. Ognuno è parte integrante dello stesso sistema di controllo.

Considerato quanto appena esposto, la società digitale sembrerebbe confermare l'ipotesi per cui, per effetto della concorrenza di molteplici fattori e fenomeni di natura tecnologica e non, abbia assunto, come asserito da numerosi sociologi, la natura di una vera e propria società del controllo e della sorveglianza. La diffusione delle nuove tecnologie dell'informazione e della telecomunicazione, insieme all'alto grado di pervasività e convergenza delle stesse, il sempre più frequente utilizzo di database, la globalizzazione e le esigenze sempre più pressanti in materia di salvaguardia dell'ordine pubblico hanno, di fatto, aperto la strada al perpetrarsi di pratiche di controllo esercitate, sovente, in maniera massiccia connotando la società contemporanea come l'emblema rappresentativo del grande "occhio elettronico" che "tutto osserva e tutto scruta".

Il carattere decisamente centrale della nuova forma di sorveglianza è la pervasività, dal momento che, esercitata nei confronti di individui profondamente mutati dal loro essere quotidianamente immersi nel magma delle comunicazioni elettroniche, si dirama

e si diffonde ovunque riproponendo a grandi linee, e seppur con inedite e differenti sfumature, il modello del Panottico elaborato verso la fine del 700 dal filosofo ed economista Jeremy Bentham. Il Panottico è l'archetipo cui spesso si ricorre per descrivere le dinamiche e gli aspetti che contraddistinguono l'era moderna, utilizzato come metafora di un potere invisibile che domina su tutto.[6]

Nello specifico, oggigiorno, ci si trova dinanzi a quello che Poster definisce "*Superpanopticon*",[7] ovvero quel complesso di sorveglianza in grado di controllare in ogni momento, badando a ogni dettaglio, la vita quotidiana di ciascun individuo grazie al sistema di controllo che prende il nome di "Dataveglianza".

Il termine "Dataveglianza", coniato dall'informatico Roger Clarke, con cui s'intende «l'uso sistematico di un insieme di dati personali allo scopo di controllo e monitoraggio delle azioni e comunicazioni di una o più persone, ben riassume la nuova conformazione della sorveglianza, basata principalmente sull'utilizzo di database».[8]

Le intricate vicende politiche e di cronaca come quelle legate ad Assange e Wikileaks o a Snowden,[9] insieme alle innovazioni tecnologiche e informatiche che diffondono dati ed informazioni concernenti i singoli, l'utilizzo massiccio di *Big data* e metadati da parte dei governi, di grandi aziende commerciali e delle *intelligence* di vari

[6] Per tracciare in maniera puntuale il progetto messo a punto dal filosofo Bentham, occorre anche soffermarsi su un'ulteriore fase della progettazione, quella dell'anti-*panopticon*. L'idea di proporre un nuovo modello, rispetto a quello fornito in partenza, nacque nel momento in cui il filosofo comprese che il suo progetto era stato clamorosamente frainteso, facilitando, di fatto, un uso distorto dello stesso. Il modello che aveva messo a punto, difatti, era divenuto un mezzo per opprimere l'individuo e limitarne le sue libertà: esso non era stato creato per evitare che l'individuo si esprimesse nella sua personalità e nelle sue ideologie, ma, piuttosto, per indurlo ad assumere comportamenti etici e giusti, creando un vantaggio per la società. Il Panottico non fu progettato come modello da applicare alle mere carceri, ma piuttosto da estendere a tutti gli ambienti sociali, coinvolgendo cittadini, politici, studenti e lavoratori. Coloro che vivevano all'interno del Panottico non dovevano subire la sorveglianza e assumere comportamenti inetti, ma, al contrario, modificare i propri atteggiamenti al fine di renderli trasparenti e moralmente corretti, in altre parole senza che il guardiano potesse accusare nessuno dei loro gesti. Per un approfondimento del tema: P. TINCANI, *Controllo e sorveglianza*, in R. BRIGHI - S. ZULLO, eds., *Filosofia del diritto e nuove tecnologie*, Ariccia, Aracne, 2015, pp. 19-40.

[7] D. LYON, *The Electronic Eye. The Rise of the Surveillance Society*, Minneapolis, University of Minnesota Press, 1994, p.71

[8] R. CLARKE, *Information Technology and Dataveillance*, in «Communications of the ACM», XXXI, 5, May 1988, p. 501.

[9] Un'analisi dei casi Snowden e Wikileaks è presente in: G. ZICCARDI, *Il computer e il giurista*, Milano, Giuffré, 2015, pp. 97-103.

paesi e i vari sistemi di intercettazione più o meno globali sono solo una delle serie di elementi che hanno contribuito a costruire questa interessante definizione ("Dataveglianza") a cui, però, si fornisce tendenzialmente un'accezione negativa.

In uno scenario dove la raccolta di dati e di ogni forma possibile d'informazione diviene sempre più massiccia in rete, consentendo un'esatta e fedele ricostruzione del profilo di ogni individuo e dove l'esercizio del controllo nel contesto sociale di appartenenza assume forme decisamente diverse rispetto al passato, l'individuo non è solo più trasparente, ma anche sempre più digitalizzato e profilato.

L'evoluzione tecnologica facilita tale processo di "profilazione" e amplia lo spettro delle possibili attività che possono essere svolte con l'ausilio di dispositivi informatici altamente evoluti, come *software* di ultima generazione, che consentono di acquisire costantemente un'ingente mole di dati personali, che vengono processati e immagazzinati in modo del tutto automatico, per fini diversi e spesso a insaputa dei soggetti che in maniera non intenzionale forniscono il loro tacito consenso.

L'art. 4 del Regolamento UE n. 679/2016 (*General Data Protection Regulation - GDPR*), da una definizione di "profilazione": «Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».[10] Di base, il GDPR vieta l'attuazione di pratiche di profilazione, tranne specifiche eccezioni ben disciplinate.[11] Questo denota

[10] Il Considerando 24 del GDPR specifica ulteriormente che, per stabilire se si è in presenza di profilazione, «è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali».

[11] Una persona fisica può essere sottoposta ad un processo decisionale automatizzato, compresa la profilazione se: 1) il trattamento è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare (la necessità deve essere interpretata in modo restrittivo, anche se i garanti europei precisano che motivi di efficienza sono ritenuti sufficienti per giustificare l'utilizzo di sistemi decisionali basati su profilazione, a condizione che non vi siano metodi meno intrusivi che raggiungano lo stesso risultato, ma tale eccezione non si applica in caso di trattamento di dati sanitari; 2) il trattamento

l'attenzione del legislatore europeo alla problematica e la forte distanza tracciata tra il *corpus* giuridico continentale e quello statunitense, caratterizzato, invece, da ampie pratiche di profilazione.[12]

La larga diffusione di sistemi di profilazione non fa che confermare la certezza espressa dallo studioso Mario Losano, secondo il quale «lo sviluppo dell'informatica e delle reti di telecomunicazioni hanno reso ormai trasparente la società. Il cittadino si sente osservato senza possibilità di scampo, come un pesce rosso nella sua boccia di cristallo».[13]

Se prima tali pratiche ricadevano solo su determinate categorie d'individui e ambienti, ora, si rivolgono, invece, all'intera popolazione in maniera del tutto indiscriminata, connotando la sorveglianza come un fenomeno di "massa", prevedendo che informazioni e dati siano "captati" addirittura sin dentro le mura domestiche, prima invalicabile confine tra spazio intimo e spazio pubblico.

È chiaro che, oggi, la sorveglianza di "massa" è una pratica facilmente esercitabile: è possibile condurre attività di raccolta indiscriminata dei *big data* e dei metadati; si può passare da una sorveglianza mirata e particolare a una generale grazie ad operazioni di *data mining*;[14] è possibile superare i vincoli legislativi imposti dagli ordinamenti

è autorizzato da una legge o regolamento, che prevede altresì misure idonee a tutelare i diritti dei soggetti interessati; 3) vi è esplicito consenso al trattamento. Secondo i garanti europei (Linee guida in materia di processi automatizzati e profilazione, WP29, 2018) la profilazione può essere basata anche sui legittimi interessi del titolare del trattamento, alla stregua del marketing diretto. Tuttavia occorre sempre effettuare il bilanciamento degli interessi per valutare l'eventuale prevalenza di quelli del titolare.

[12] Per un approfondimento del rapporto tra Stati Uniti d'America e Unione Europea in tema di protezione dei dati personali, si veda: S. PIETROPAOLI, *Privacy e oblio. La protezione giuridica dei dati personali*, in F. FAINI - S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, Torino, Giappichelli, 2017, pp. 41-65; U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America ed in Europa,* Milano, Giuffrè, 2008.

[13] M.G. LOSANO*, Il diritto pubblico dell'informatica*. *Corso di informatica giuridica*, Torino, Einaudi, 1986, pp.14-15.

[14] Il *data mining* iniziò a svilupparsi nel corso degli anni '80 del secolo scorso e rappresenta l'estrazione di dati, cioè l'attività di selezione, esplorazione e modellizzazione di grandi quantità di dati, attraverso tecniche statistiche, al fine di individuare regolarità o relazioni non note *a priori* e traducibili in informazioni chiare e rilevanti per l'interprete e utilizzatore. Per ogni approfondimento, si consiglia la lettura di: P. TAN - M. STEINBACH - A. KARPATNE - V. KUMAR, *Introduction to Data Mining*, New York, Pearson, 2019; A. DE LUCA, *Big data analitycs e data mining: estrarre valore dai dati*, Milano, Wolters Kluwer, 2018.

eseguendo attività d'intercettazione globale illegali e senza mandato giudiziario. L'oltrepassare i limiti e i vincoli legislativi porta a possibili violazioni di natura non meramente burocratica ma, anche, alla potenziale violazione delle libertà e diritti fondamentali dell'individuo, della possibilità in capo ad esso di costruire liberamente la propria esistenza e del suo legittimo desiderio di poter manifestare la curiosità intellettuale senza condizionamenti o altrui ingerenze.

Il più delle volte carattere cruciale della messa a punto delle attività di sorveglianza è la segretezza, in quanto il tutto avviene all'insaputa dei cittadini, ignari di essere il centro d'interesse di stati e di aziende commerciali.

Il ricorso al "segreto", e spesso alla "menzogna", concerne la possibilità in capo a chi governa d'adoperare tali strumenti per conservare il potere governativo, diffondendo l'idea fallace che ciò sia vitale per "il benessere" dello stato. Il binomio segreto/menzogna sarebbe, in tal senso, fonte di sopravvivenza per la stessa politica: «Stiamo vivendo uno dei periodi più bui dal punto di vista delle attività di sorveglianza: un quadro che, spesso, con il pretesto della difesa preventiva da attività terroristiche e, in generale, con il richiamo alle esigenze di sicurezza nazionale, sta vedendo minato, giorno per giorno, il delicato equilibrio tra sicurezza e libertà».[15]

Secondo il principio di "*information privacy*" è sì importante controllare il flusso dei dati e delle informazioni riguardanti il singolo individuo qualora sia necessario, ma è altrettanto vitale che chi si assume l'onere di processare dati privati tenga conto di ciò che fa, *in primis* ai soggetti direttamente coinvolti.

Nella società odierna, è sempre più faticoso rintracciare il giusto punto di equilibrio tra l'istanza di monitoraggio, atta a supportar le esigenze di comunicazione, sicurezza e difesa dell'ordine e quella, che, invece, mira a difendere il "patrimonio" informativo e la vita privata di ciascun individuo. In realtà non è semplice neanche fornire una definizione unica e universale di "*privacy*", valevole *pro tempore*: il lemma è portatore

[15] G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica,* Milano, Raffaello Cortina Editore, 2015, p. 24.

di diversi e variegati significati che si costruiscono e si articolano con riferimento all'evoluzione della storia, della società e della "cultura" giuridica dei vari paesi.

Proprio in merito all'interesse profuso nell'analizzare l'evoluzione pratica e teorica del diritto alla *privacy* nella *cyber-era*, si palesa una sorta di contrapposizione tra un'interpretazione del concetto di *privacy* elaborata negli Stati Uniti d'America, ad oggi ancora in conflitto con le politiche rigide di sicurezza volute dall'amministrazione governativa post 11 settembre 2001, e le riflessioni sul medesimo tema elaborate in Europa, che mirano a una più reale e concreta tutela e protezione dei dati che ci riguardano e che migrano nel vecchio continente, prevedendo misure punitive e sanzionatrici nei confronti di soggetti che non ottemperano agli obblighi e ai limiti previsti.

Gli Stati Uniti hanno da sempre profuso grandi energie nel mettere a punto un concetto di *privacy*, ma, nei fatti, sono andati incontro a delle difficoltà applicative. Al contrario, l'UE si è dimostrata spesso più immatura nelle elaborazioni teoriche ma più decisa sul versante della protezione reale dei dati, cercando sempre di adeguare le sue politiche di controllo alle nuove necessità, prevedendo l'adozione di legislazioni più restrittive in ambito di spionaggio e d'intercettazione e di forme di tutela più efficaci.[16]

Il GDPR, divenuto applicabile il 25 maggio del 2018, rappresenta, in tal senso, un ulteriore passo in avanti compiuto in materia in ambito europeo.[17]

3. *Il segreto e la trasparenza digitale*

Il termine "segreto" rimanda, dal punto di vista etimologico, a differenti accezioni di significato.

Da sempre il segreto è apparso uno strumento irrinunciabile per ottenere il potere e per provvedere altresì alla sua stessa conservazione e nell'era tecnologica esso assume

[16] Cfr. *ibid.*, p. 15.

[17] Per una disamina completa del contenuto del GDPR: F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, Giappichelli, 2016; G. CIACCI - G. BUONOMO, *Profili di Informatica giuridica*, Milano, Wolters Kluwer, 2018, pp. 141-196.

ancor più inedite sfumature meritevoli di attenzione. Nella moderna società digitale e dell'informazione, caratterizzata da reti, segnali, sensori e impulsi elettronici ovunque diffusi e definita da molti sociologi, "liquida", diventa estremamente difficile custodire segreti di diversa matrice.

I nuovi supporti di memoria, capaci di contenere un'indecifrabile quantità di informazioni, dati e documenti in ridotte porzioni di spazio fisico, garantiscono, grazie alla loro capacità di connettersi in tempo reale alla rete, la diffusione di documenti anche protetti da segreto, mantenendoli disponibili per chi volesse prenderne visione, media compresi.

Se da un lato, in un quadro simile, appaiono critiche le reali possibilità circa il mantenimento di segreti, dall'altro, esso stesso è ricercato con grande veemenza dagli stati e dalle agenzie di *intelligence* che operano nel campo dello spionaggio e del controspionaggio.

Oggi, il segreto ha essenzialmente natura "digitale", è mutato rispetto al passato, trasformandosi in una serie di bit e byte, generando sempre più spunti di dibattito: il più evidente è una sorta di potere sul segreto come appannaggio del cittadino nei confronti dell'autorità, divenuto mezzo per poter sfruttare le medesime strategie governative.

Il quesito da sottoporre all'attenzione è allora il seguente: il cittadino e l'opinione pubblica, appurando un eventuale illegalità di operazioni governative, potrebbero ricorrere alla medesima tecnologia per scardinare segreti che in realtà dovrebbero essere mantenuti tali? Se la risposta fosse affermativa, il segreto cesserebbe di essere un mero vantaggio in mano a chi detiene il potere, divenendo uno strumento con cui prendere di mira il sistema stesso.

Grazie alle nuove tecnologie, il comune cittadino ha non solo la possibilità di poter edificare un proprio spazio "segreto" e privato da tenere debitamente lontano dalle altrui ingerenze, ma ha anche l'occasione di vantare una sorta di diritto di usare le stesse per svelare informazioni o documenti tenuti volutamente nascosti ma di fatto di interesse pubblico. Interessante è a tal proposito la diffusione di progetti di *leaking* e

whistleblowing[18] che hanno mutato il rapporto del diritto e della politica con i temi del segreto, delle rivelazioni e delle le azioni da intraprendere nei confronti di chi rivela informazioni critiche.

Il tema del segreto si ricollega, poi, al dibattito sulla pressante necessità di una maggiore trasparenza nell'era digitale, argomento che ha interessato teorici, giuristi, Stati e gli stessi organi di governo. L'attenzione rivolta a tale esigenza della società democratica è giustificata, a parere di alcuni, dal fatto che essa sembrerebbe essere «il miglior disinfettante per il settore pubblico e per la democrazia in genere».[19] Tuttavia, se essa venisse interpretata come trasparenza radicale e senza controllo, i suoi svantaggi potrebbero rivelarsi addirittura maggiori dei possibili vantaggi.

Secondo lo studioso Giovanni Ziccardi, per comprendere a fondo la tematica in questione, bisognerebbe chiedersi: quali problemi si pongono in concreto se la trasparenza venisse esercitata in maniera radicale? Che tipo di rapporto dovrebbe esserci fra trasparenza, segreto di stato e informazioni pubbliche riservate ma degne d'interesse per il cittadino? Se lo stato adottasse buone politiche di trasparenza, sarebbero realmente un vantaggio per la società? La trasparenza organizzata dai privati e non dallo stato, con corrette piattaforme studiate per indurre gli individui a disvelare episodi di corruzione, malgoverno e simili, è utile o si presta a eventuali distorsioni? La trasparenza dovrebbe concernere solo i dati e le informazioni o rendere note anche le fasi decisorie?[20]

---

[18] Si tratta della segnalazione di condotte illecite effettuata dal *whistleblower*, inteso come dipendente pubblico che intende segnalare illeciti di interesse generale e non di interesse individuale, di cui sia venuto a conoscenza in ragione del rapporto di lavoro, in base a quanto previsto dall'art. 54 bis del d.lgs. n. 165/2001 così come modificato dalla legge 30 novembre 2017, n. 179. Per "dipendente pubblico" si deve intendere il dipendente delle amministrazioni pubbliche di cui all'articolo 1, comma 2, del d.lgs. n. 165/2001, ivi compreso il dipendente di cui all'articolo 3, il dipendente di un ente pubblico economico ovvero il dipendente di un ente di diritto privato sottoposto a controllo pubblico ai sensi dell'art. 2359 del codice civile. Inoltre, la disciplina del *whistleblowing* si applica anche ai lavoratori e ai collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica.

[19] G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica,* p. 21.

[20] Cfr. *ibid.*

Gli anni trascorsi sono stati quelli della tanto discussa trasparenza "mediata", presentata per la prima volta al pubblico da Julian Paul Assange e dai gestori della piattaforma Wikileaks, "mediata" in quanto coadiuvata nella messa in pratica dall'azione di media tradizionali, coinvolgendo testate internazionali, per garantire autorevolezza alle operazioni di divulgazione di documenti riservati e per costruire la "parabola" di una trasparenza responsabile, animata da etica e senso dell'ordine.

Il più delle volte tale processo di trasparenza riguarda informazioni e documenti segreti e il maggior timore è che ciò possa minare sovranità e sicurezza nazionale. Ma se, allo stesso modo, tale materiale informativo interessasse direttamente i cittadini, la richiesta di maggiore trasparenza non sarebbe forse più che legittima? Si pensi ai piani di sorveglianza di massa e d'intercettazione globale delle comunicazioni domestiche o all'attività di profilazione effettuata dalle aziende di telecomunicazioni. In questi casi, forse, la richiesta di una maggiore trasparenza da parte dei soggetti appartenenti a una comunità dovrebbe ritenersi più che legittima.

4. *La libertà "sorvegliata" e gli oggetti del quotidiano come dispositivi di controllo*

La libertà di cui oggi si dispone è perennemente sotto "sorveglianza": telecamere a circuito chiuso sparse per le strade, nei negozi, nelle stazioni, negli aeroporti; le crescenti possibilità di effettuare intercettazioni ambientali e telefoniche; la raccolta e l'elaborazione di tutti quei dati e informazioni che si lasciano alle spalle in seguito all'acquisto di prodotti o merci con le varie carte di credito o fedeltà; mezzi ancora più sofisticati come le tecnologie biometriche; i vari sistemi di geo localizzazione. Le nuove tecnologie informatiche non consentono solo di effettuare controlli sempre più capillari ed estesi di quanto finora sia stato mai possibile bensì di aumentare anche la nostra "tracciabilità" *offline* e *online*.

Le conversazioni, le attività svolte, i gusti e le preferenze personali rappresentano i principali centri di monitoraggio e d'interesse e ogni minima traccia lasciata nei numerosi sistemi informatici con cui s'interagisce nel quotidiano, tramutata in dato,

diviene oggetto di operazioni di elaborazione e memorizzazione svolte da organizzazioni pubbliche e private che ricostruiscono, in tal modo, un profilo dettagliato di ogni individuo.

Per farsi un'idea di quanto sia pervasiva la nuova forma di controllo sociale è sufficiente riflettere sui numerosi oggetti che, interagendo con noi, in maniera diretta o indiretta, tracciano ogni sorta di movimento, la registrano in memoria presso appositi database, mantenendola a disposizione di chiunque ne faccia esplicita richiesta. Per capire meglio, offriamo qualche esempio concreto.

Le transazioni eseguite con apposite carte di credito e carte di fedeltà sono costantemente registrate e monitorate: il monitoraggio delle suddette offre evidenti e indubbi benefici al possessore ma al contempo rende possibile la raccolta di un'infinità di dati utilizzabili per finalità di vario genere come quelle di natura strettamente commerciale e di marketing.[21] L'azione del frequentare i *social network* non consente solo di far conoscere ad amici e conoscenti notizie, avvenimenti privati o pubblici, amplificando di fatto le possibilità di condivisione, bensì, anche, di tenere sempre al corrente chi ci controlla circa l'uso di specifiche applicazioni, la gestione dello spazio *online*, le proprie reti di contatto, le idee e le opinioni espresse, le preferenze di genere e via dicendo. Il beneficio è reale ma, al contempo, veicola con sé effetti "collaterali" come la trasparenza delle informazioni condivise verso le entità private e governative che sfruttano gli strumenti di cui dispongono per vedere come, cosa e quando tutto ciò è condiviso.[22] L'evoluzione dei droni ha spinto il controllo sino all'etere, consentendo di avere a disposizione velivoli privi di pilota in grado di registrare ogni sorta di movimento o dettaglio, prestandosi facilmente ad operazioni di controllo e sorveglianza,

[21] Soprattutto con riferimento alle carte fedeltà, con *Deliberazione del 14 febbraio 2019 - Attività ispettiva di iniziativa curata dall´Ufficio del Garante Privacy, anche per mezzo della Guardia di finanza, limitatamente al periodo gennaio-giugno 2019*, l'Autorità ha stabilito la necessità di indirizzare l'attività ispettiva anche ai trattamenti di dati personali effettuati da società con particolare riferimento all'attività di profilazione degli interessati che aderiscono a carte di fidelizzazione.

[22] Il Garante privacy riserva da sempre particolare attenzione ai pericoli insiti nel trattamento dei dati personali da parte delle piattaforme di social networking. Si vedano le varie iniziative, infografiche, provvedimenti e test di autovalutazione pubblicati alla pagina web: https://www.garanteprivacy.it/temi/social-network, consultata nel mese di maggio 2019.

oltre che di disturbo e inganno.[23] I telefoni cellulari sono considerati mai quanto oggi una sorta di "invisibile filo elettronico" che consentono di seguire implacabilmente ogni nostro minimo movimento,[24] e dunque di localizzare in qualsiasi istante il proprietario anche fuori comunicazione, trasmettendo in permanenza un segnale per indicare la sua presenza alle antenne più vicine. In rete si fa un uso ricorrente di motori di ricerca e di applicazioni che offrono grandi servizi e benefici ma che oramai sono caratterizzati, in modo sempre più frequente, dalla presenza di robot tecnologici in grado di memorizzare le parole chiave utilizzate e gli argomenti maggiormente ricercati, di memorizzare le abitudini individuali e addirittura di spiare dentro le caselle di posta elettronica.

Da questi brevi esempi si può dedurre come i dispositivi che monitorano e analizzano le informazioni personali di ognuno siano molteplici: tecnologie di diverso genere che, nate con l'intento di migliorare la vita pratica dell'individuo offrendo facilitazioni di cui poter disporre, sono affette da una scarsa propensione alla tutela della *privacy* e a quella dello stesso bagaglio informativo di ciascuno.

Per soffermarsi sulla questione della alquanto labile tutela dei dati personali e della *privacy*, sarebbe utile analizzare, in modo più dettagliato, uno dei più pervasivi strumenti utilizzati per finalità di controllo: la tecnologia biometrica.

5. *La tecnologia biometrica*

L'espressione "tecnologia biometrica" si riferisce a qualunque tecnica che usi in modo affidabile caratteristiche fisiologiche o comportamentali per distinguere una persona da un'altra. Fra i tratti biometrici fisiologici più comuni vi sono impronte digitali, geometria della mano, retina, iride e immagini facciali. I tratti biometrici

[23] Il problema "droni" è talmente avvertito dal Garante privacy che ha ritenuto opportuno dedicare una pagina web, completa di normativa o linee guida di garanti europei nel settore: https://www.garanteprivacy.it/temi/droni, consultata nel mese di maggio 2019.
[24] Cfr. S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Milano, CEDAM, 2006, p.74.

comportamentali più comuni includono invece firma, registrazioni vocali e ritmo di battuta su tastiera.[25]

Si tratta, pertanto, di tecnologie, come specifici *software* o apparecchiature informatiche, che consentono di provvedere all'identificazione di un individuo tramite l'acquisizione di dati ricavati da caratteristiche biologiche uniche del corpo umano come appunto la morfologia facciale, le impronte digitali, acquisite da appositi sensori e comparati poi con altre informazioni già carpite in precedenza e conservate in appositi data base.

Oggigiorno la biometria è in forte ascesa e a conferma di ciò basti pensare alla sempre più frequente integrazione delle tecnologie biometriche nei dispositivi personali mobili, come smartphone e tablet, il cui funzionamento, spesso, si basa sull'impiego dei cosiddetti dati biometrici: ad esempio, da almeno un decennio, le impronte digitali sono utilizzate come strumento di autenticazione per l'attivazione di dispositivi elettronici e la Apple ha inserito nel modello *iphone 5s* un sensore per la scansione delle impronte digitali, quale sistema di autenticazione e di sblocco del telefono al posto della password numerica; molti *software* di grafica adottati nei *social network*, come Instagram e Facebook, consentono di provvedere al riconoscimento facciale degli utenti iscritti.

Come giustamente rimarcato da Agata C. Amato Mangiameli, l'accumulo illimitato di dati che la biometria consente, associato alla possibile velocissima combinazione degli stessi, genera «la richiesta di un *habeas data*, ossia di un riconoscimento del diritto del cittadino di disporre dei propri dati personali e di vigilare su chi li usa, e insieme quella di un *habeas corpus* (che tu abbia il tuo corpo: che tu sia padrone della tua persona), ovvero il diritto di disporre del proprio corpo e di impedire che pretese antigiuridiche lo soppongano a nuove e quanto mai sofisticate forme di

[25] Per una riflessione sulla biometria, al fine di comprendere meglio gli attuali confini, si rinvia a: G. PREITE, *Politica e biometria: nuove prospettive filosofiche delle scienze sociali*, Trento, Tangram Edizioni Scientifiche, 2016; S. AMATO - F. CRISTOFARI - S. RACITI, *Biometria: i codici a barre del corpo*, Torino, Giappichelli, 2013.

assoggettamento-oggettivazione».[26] Sorge un "diritto personale di libertà informatica", come riteneva Vittorio Frosini, che consiste «nella pretesa giuridica da parte del cittadino di una tutela dei dati afferenti alla sua vita intima, nella rivendicazione di un'autonomia decisionale dell'individuo, nella facoltà di raccogliere tali dati in una forma dovuta di liceità e di correttezza, nella loro elaborazione ai fini strettamente determinati e consentiti dall'interessato».[27]

Prima di entrare nel vivo di questa breve digressione, è necessario precisare il concetto di "dato biometrico", cui si è fatto cenno nelle righe precedenti, da un punto di vista prettamente giuridico, per delineare, in seguito, la disciplina normativa applicabile a tale categoria di dati, alla luce soprattutto delle nuove disposizioni in materia di protezione dei dati personali introdotte dal cosiddetto GDPR, considerata la prima normativa al mondo ad aver affrontato in modo organico e pratico la protezione dei dati biometrici.

Nel 2012, pur non esistendo ancora una definizione normativa concernente i "dati biometrici", questi venivano convenzionalmente definiti come dati ricavati da «proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche o azioni sono tanto proprie di un

[26] A.C. AMATO MANGIAMELI, *Informatica giuridica*, Torino, Giappichelli, 2015, p. 315. In periodo anteriore all'approvazione del Regolamento UE n. 679/2016, che ha riformato la tutela dei dati personali nel continente, Ugo Pagallo aveva giustamente evidenziato come «un vero e proprio *habeas data* non esista nel modello europeo di tutela della privacy». U. PAGALLO, *Il diritto nell'età dell'informazione*, Torino, Giappichelli, 2014, p. 234; si consiglia l'intera lettura del testo, in quanto ricco di riflessioni filosofico-giuridiche in tema *privacy*, autonome rispetto alla normativa del periodo storico di riferimento. Con il nuovo Regolamento, al contrario, è possibile configurare una reale tutela di un *habeas data*, anche se le Costituzioni, a parere di chi scrive, dovrebbero progressivamente farlo proprio, a tutela del nostro "corpo elettronico", come definito da Stefano Rodotà. Cfr. S. RODOTÀ, *Il mondo nella rete*, Roma-Bari, Laterza, p. 30. Strettamente connessa alla riflessione in tema di *habeas data* si pone quella in materia di identità digitale, le cui fondamenta sono rappresentate dai "dati"; si veda M. MARTONI - M. PALMIRANI, eds., *Internet e identità personale*, in R. BRIGHI - S. ZULLO, eds., *Filosofia del diritto e nuove tecnologie*, Ariccia, Aracne, 2015, pp. 295-308.

[27] V. FROSINI, *La democrazia nel XXI secolo*, Macerata, Liberilibri, 2010, p. 40.

certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità».[28]

La definizione normativa degli stessi è stata formulata, per la prima volta, nell'art. 4, paragrafo 1, n. 14 del GDPR, che definisce i "dati biometrici" come quei «dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici». Il trattamento dei dati biometrici rientra fra quello previsto per le categorie particolari di dati personali, art. 9 GDPR, tra i quali i dati attinenti alla salute.

La raccolta di questi particolari dati personali è resa possibile ricorrendo all'impiego di sistemi informatici di riconoscimento biometrico, il cui funzionamento si basa principalmente su due elementi, ossia, nello specifico, una componente *hardware* che acquisisce direttamente il dato biometrico e una componente software che consente, attraverso l'impiego di algoritmi matematici, di analizzare i dati raccolti e di confrontarli con quelli acquisiti in precedenza e conservati nel database del sistema, al fine di ricondurre il dato raccolto ad una determinata persona e di riconoscerla da tali informazioni.

Come è facilmente intuibile, l'utilizzo di questa delicata tipologia di dati personali richiede la rigida osservanza di una serie di cautele, al fine di evitare che si verifichino dei pregiudizi a danno dei soggetti chiamati direttamente in causa. Se da un lato, i sistemi di riconoscimento biometrico contribuiscono a incrementare, in capo all'utente, un adeguato livello di sicurezza rispetto all'esterno nell'utilizzo dei dispositivi elettronici, dall'altro potrebbero configurarsi, anche, dei gravi rischi per l'interessato, connessi a un'indebita o non autorizzata utilizzazione degli stessi, al di fuori degli scopi specifici per i quali sono stati acquisiti dal sistema.

[28] Gruppo per la tutela dei dati personali - Articolo 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche, WP193*, 27 aprile 2012, disponibile alla pagina: https://www.privacy.it/archivio/grupripareri201203.html, consultata nel mese di maggio 2019.

Costatando la rapida ascesa e la sempre più frequente integrazione di tali metodologie di riconoscimento nei dispositivi di ormai quotidiano e comune utilizzo, il Garante privacy ha assunto, sin dalla loro primordiale comparsa, posizioni piuttosto rigide, appurando, sovente, l'uso spregiudicato e illecito di dati biometrici reso possibile dalle neofite tecnologie.

In considerazione della particolare natura delle informazioni biometriche e dell'assenza di norme specifiche, l'Autorità ha previsto, più volte, con i suoi interventi, una serie di prescrizioni attuabili nello specifico settore delle nuove tecnologie biometriche, integrando di fatto il quadro dei principi generali stabiliti dal codice in materia di protezione dei dati personali.

Già nelle proprie *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati*,[29] l'Autorità garante aveva stabilito che l'utilizzo di dati biometrici poteva essere giustificato solo in casi particolari, tenuto conto delle finalità e del contesto in cui gli stessi venivano trattati, richiedendo in maniera esplicita che tutti i sistemi informativi fossero configurati in modo da ridurre al minimo indispensabile l'utilizzo di dati personali e che il trattamento degli stessi fosse da ritenere non consono, qualora le finalità da perseguire potessero essere raggiunte con modalità che tali da permettere l'identificazione del soggetto solo in casi di estrema necessità.

L'approccio del Garante alla problematica è, però, sostanzialmente mutato con l'emanazione del Provvedimento generale n. 513 in tema di biometria del 12 novembre 2014, parte integrante de *Le Linee guida in materia di riconoscimento biometrico e firma grafometrica*,[30] con le quali ha inteso fornire un quadro di riferimento unitario

[29] GARANTE PRIVACY, *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati*, Deliberazione n. 53 del 23 novembre 2006, disponibile in formato integrale alla pagina web: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1364939, consultata nel mese di maggio 2019.

[30] GARANTE PRIVACY, *Linee guida in materia di riconoscimento biometrico e firma grafo metrica*, allegate al provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014, disponibili in formato integrale alla pagina web: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992, consultata nel mese di maggio 2019.

sulla cui base i titolari possono orientare le proprie scelte tecnologiche, conformare i trattamenti ai principi di legittimità stabiliti dal codice e rispettare elevati standard di sicurezza.

Tra le prescrizioni di maggiore rilevanza si annovera, ad esempio: in primo luogo quella secondo cui il titolare può trattare dati personali esclusivamente per scopi determinati, espliciti e legittimi, di conseguenza i dati possono essere utilizzati soltanto in termini compatibili con la finalità per la quale sono stati originariamente raccolti e conservati per il tempo strettamente necessario a perseguire tale finalità, decorso il quale devono essere cancellati o resi anonimi; in secondo luogo, quella secondo cui il titolare del trattamento, svolto con sistemi elettronici, è tenuto ad adottare mezzi tecnici per proteggere i dati personali trattati con le misure di sicurezza previste dal codice, conservandoli in un'unica banca dati centralizzata oppure memorizzandoli in dispositivi sicuri come *token* o *smart card*, affidati alla diretta ed esclusiva disponibilità degli interessati.

Con l'avvento del GDPR anche il provvedimento sulla biometria sarà di certo oggetto di rivisitazione.

In linea generale, il GDPR, all'art. 9, paragrafo 1, stabilisce che è vietato il trattamento di «dati biometrici intesi a identificare in modo univoco una persona fisica»: s'introduce così, per i dati biometrici, una disciplina normativa particolarmente rigida, caratterizzata da un generale divieto di trattamento. D'altra parte, come per gli altri dati personali rientranti nella precedente definizione di "dati sensibili", tale netta presa di posizione è ammorbidita al ricorrere di una serie di casi ben precisi.

È sempre l'art. 9 del GDPR, infatti, al paragrafo 2, a stabilire che il trattamento dei dati biometrici è consentito quando si verifica, ad esempio, una delle seguenti ipotesi: 1) quando l'interessato ha dato il proprio consenso esplicito al trattamento dei dati personali per uno o più specifici utilizzi, come avviene per il caso dell'autenticazione tramite impronta digitale o della firma grafometrica in banca; 2) quando tale trattamento è effettuato nell'ambito di rapporti di lavoro e di previdenza; 3) quando il soggetto cui i dati si riferiscono si trova in una situazione d'incapacità, fisica o giuridica, di prestare

direttamente il proprio consenso per tale utilizzo; 4) nel settore della sanità pubblica, per finalità di sicurezza sanitaria, per il controllo e l'allerta, per la prevenzione o il controllo di malattie trasmissibili e, in generale, per tutelarsi da altre minacce gravi alla salute delle persone.

Da questi esempi, è palese l'attenzione che il legislatore europeo ha riservato a questa particolare e delicata tipologia di dati personali, dando loro una rilevanza specifica all'interno delle "categorie particolari di dati", tra i quali rientrano quelli che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Con la varietà delle ipotesi sopra esaminate ed elencate, il GDPR permette di superare il divieto, prima generale, di utilizzo dei dati biometrici, precisando che le intenzioni del legislatore europeo non rispondono al non consentire perentoriamente l'uso e la circolazione degli stessi dati personali quanto di vedere rispettati i sistemi rigidi di tutela posti a garanzia degli interessati: con il GDPR viene creato un solido sistema di cautele intorno ai dati biometrici, tale da permetterne un'utilizzazione adeguatamente protetta.

Il dato biometrico diviene l'esempio più concreto di come l'innovazione tecnologica possa incidere sulla libertà dell'individuo che, con gli opportuni accorgimenti informatico-giuridici, diviene titolare di nuovi diritti di tutela e di utilizzo del dato personale. Una nuova forma di sorveglianza e controllo che può però procedere in equilibrio con le libertà individuali.