ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

HUMAN RIGHTS
26 LUGLIO 2023

Sorveglianza di massa, rispetto della vita privata e trattamento di categorie particolari di dati nel quadro multilivello di tutela della persona

di Francesca Mollo
Ricercatrice di Diritto privato
Alma Mater Studiorum - Università di Bologna

Sorveglianza di massa, rispetto della vita privata e trattamento di categorie particolari di dati nel quadro multilivello di tutela della persona*

di Francesca Mollo
Ricercatrice di Diritto privato
Alma Mater Studiorum - Università di Bologna

Abstract [It]: Il contributo ricostruisce il tema della sorveglianza di massa, intrecciato con la tutela della vita privata da un lato, e la protezione dei dati personali dall'altro. Sotto questi profili, si analizza la giurisprudenza della Corte di Giustizia, in raffronto con quella della Corte europea dei diritti dell'uomo. Di qui prende le mosse per indagare i profili di criticità connessi al trattamento di alcune categorie particolari di dati, in particolare i dati genetici e i dati biometrici, il cui trattamento — in particolare sistematico e su larga scala — è suscettibile di definire nuovi modelli di sorveglianza.

Title: Mass surveillance, respect for private life and processing of special categories of data in the multilevel framework of personal protection
Abstract [En]: The contribution reconstructs the theme of mass surveillance, intertwined with the protection of privacy, on the one hand, and the protection of personal data, on the other. Under these profiles, it analyzes the jurisprudence of the Court of Justice, in comparison with that of the European Court of Human Rights. From here it starts to investigate the criticality profiles connected to the treatment of some particular categories of data, in particular genetic data and biometric data, the treatment of which — in particular systematic and on a large scale — is likely to define new surveillance models.

Parole chiave: sorveglianza, tutela della cita privata, protezione dei dati
Keywords: surveillance, privacy protection, data protection

* Articolo sottoposto a referaggio.

1. Considerazioni introduttive

L'odierna società dell'informazione si atteggia sempre più spesso a società della sorveglianza [1] e del controllo, da un lato, e società del rischio [2], dall'altro, il cui spettro, assieme al vorticoso progresso tecnico e tecnologico e al «governo dell'incertezza» [3] degli ultimi decenni, ha provocato una percezione di spaesamento e inquietudine diffusa [4] Il regime di sorveglianza globale vaticinato da George Orwell [5] nell'immagine del Grande Fratello – spesso rievocata dalla dottrina [6] - e che tutto conosce del cittadino, anch'esso globale, immerso nella sua solitudine [7] si realizza primariamente nella conoscenza e nel trattamento massivo dei dati che caratterizza il nostro tempo. «Ormai la sicurezza è al di sopra delle leggi», si è affermato [8]. Si è anzi sostenuto [9], rileggendo Foucault, che le vecchie società disciplinari si sono risolte, per far posto alle cosiddette «società di controllo», in cui «qualunque cosa venga fatta sarà tracciata, ma si può fare qualsiasi cosa», una società sorvegliata in cui non è più ravvisabile una minoranza di persone addette alla sorveglianza della cittadinanza, ma «siamo noi il controllore di noi stessi» [10]. Tale metamorfosi si realizza precipuamente attraverso la trasmissione — spontanea e spesso inconsapevole

[1] Cfr. S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004, p. 174 - 175, in cui si legge che non si può che vivere e convivere con la Società della sorveglianza, oramai divenuta un carattere della postmodernità, in cui intorno alla persona è costruita una gabbia elettronica, invece di quella d'acciaio di weberiana memoria. Secondo l'a. occorre evitare che la società della sorveglianza «si risolva nel controllo autoritario, nella discriminazione, in vecchie e nuove stratificazioni sociali produttive di esclusione, nel dominio pieno di una logica di mercato che cerca una ulteriore legittimazione proprio nella tecnologia. Questo esige processi sociali, soluzioni istituzionali capaci di tener fermo il quadro della democrazia e dei diritti di libertà. È vano confidare nella sola autodifesa dei singoli: le speranze non possono essere affidate alle "strategie da bracconiere" che ciascuno di noi può cercare di praticare».

[2] U. BECK, *La società del rischio. Verso una seconda modernità*, Roma, 2004, in part. p. 63 ss.

[3] A. PUNZI, *La persona nei dati. Ragioni e modelli di una regolamentazione*, in *Il codice del trattamento dei dati personali*, a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, 2007, p. 761 ss.

[4] Di dipendenza universale dell'età contemporanea, derivante dalla crisi dei paradigmi e dei valori assiomatici dell'umanesimo moderno parla B. ROMANO, *Fondamentalismo funzionale e nichilismo giuridico*, Torino, 2004, p. 287 ss.

[5] G. ORWELL, *1984*, trad. it., Milano, 2002.

[6] Cfr. R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, p. 13, in cui si legge di «una versione tristemente tangibile del Grande Fratello di orwelliana memoria, in grado di conoscere e condizionare la persona anche nei più profondi e segreti aspetti della sua vita privata, un timore tutt'altro che infondato». E ancora, «Immagini ormai familiari si rincorrono e si sommano. Il Panopticon di Jeremy Bentham, Il Grande Fratello di George Orwell, la Biopolitica di Michel Foucault (cfr. M. FOUCAULT, *Sécurité, territoire, population*, Paris, 2004: ID., *Sorvegliare e punire. Nascita della prigione*, Torino, 1976) si materializzano nelle grandi banche dati delle società commerciali, dove sono stivate informazioni su centinaia di milioni di cittadini», come affermato da S. RODOTÀ, L*ibertà personale. Vecchi e nuovi nemici*, in *Quale libertà. Dizionario minimo contro i falsi liberali*, a cura di Bovero, Roma-Bari, 2004, p. 54; e ancora «Questi sono dati da valutare con freddezza, ma che delineano modelli di organizzazione sociale i quali possono entrare drammaticamente in conflitto con l'intero sistema delle libertà fondamentali, modificando profondamente la natura dei sistemi democratici».

[7] Z. BAUMAN, *La solitudine del cittadino globale*, Milano, 2003, p. 24.

[8] M. FOUCAULT, *Ormai la sicurezza al di sopra delle leggi*, in ID., *La strategia dell'accerchiamento. Conversazioni interventi 1975-1984*, a cura di S. VACCARO, Palermo, 2009, p. 63.

[9] G. DELEUZE, *Proscritto sulle società di controllo*, 1990 ora in Deleuze, pourparler, trad. it. di S. VERDICCHIO, Macerata, 2000, p. 234-241.

[10] Cfr. D. LYON, *La cultura della sorveglianza*, trad. it. di C. VELTRI, Roma, 2020.

— di informazioni e dati che ci riguardano, per cui «il sorvegliato diventa esso stesso sorvegliante» [11]. Il trattamento massivo di tali dati, incardinato su una struttura circolare del trasferimento di informazioni e sul principio «*make data by data*», pone le basi per una vera e propria «sorveglianza liquida» [12], orientata in senso predittivo [13].

Così nella «società dell'accesso» [14] la persona è sempre più digitalizzata, profilata e trasparente; si viene delineando una società dell'integrale trasparenza che rievoca la metafora dell'«uomo di vetro» [15], che legittima la pretesa di altri (nella fattispecie specifica, dello Stato) di richiedere e ottenere ogni informazione e che implica la classificazione – quindi la divisione in classi, già di per sé foriera di disuguaglianze – come «sospetto, cattivo cittadino, nemico dello Stato» di chiunque rivendichi di mantenere spazi di intimità [16]. In effetti, il binomio accesso-segretezza è strettamente correlato con il potere [17] ed il suo esercizio, laddove «i nuovi poteri sono quelli che riducono la persona a oggetto, dal quale vengono costantemente estratte, con le tecniche più diverse, tutte le possibili informazioni, non solo per le tradizionali, anche se continuamente dilatate, forme di controllo, ma sempre più intensamente per costruire profili e identità, per stabilire nessi e relazioni, di cui ci si serve soprattutto per finalità economiche, per ritagliare dalla persona quel che interessa al mercato» [18]. Ciò segna il passaggio da una sorveglianza mirata ad una generalizzata, la cui essenza non è più solo e tanto quella cui la radice etimologica rimanda di «vegliare su», e che non è più – quantomeno non solo - prerogativa degli Stati per perseguire interessi di portata generale, ma si configura sempre di più quale sorveglianza privata, svolta nel mondo dei consumi e della logica di mercato, «da cui fluidità è posta direttamente in relazione con la

[11] Cfr. B-C. HAN, *Psicopolitica*, trad. it. di F. BUONGIORNO, Milano, 2016. Il filosofo coreano sottolinea come l'età che stiamo vivendo e quella della psicopolitica, fondata sul controllo digitale, un controllo che ha bisogno di fare uso della nostra libertà, perché ci richiede di esporci continuamente di "denudarci" sui social condividendo pensieri intimi, fotografie, video etc.

[12] Z. BAUMAN, D. LYON, *La sorveglianza nella modernità liquida*, Bari, 2015: «L'espressione "sorveglianza liquida", più che una definizione esauriente della sorveglianza, è soprattutto un orientamento, un modo di contestualizzarne gli sviluppi nella modernità fluida e inquietante di oggi. La sorveglianza tende a farsi liquida soprattutto nella sfera dei consumi. Nel momento in cui frammenti di dati personali estratti per un determinato scopo divengono facilmente utilizzabili per altri scopi, gli antichi punti di riferimento vengono meno. La sorveglianza si diffonde in modi fino ad ora impensabili, reagendo alla liquidità e contribuendo al tempo stesso a riprodurla».

[13] Cfr. Garante per la protezione dei dati personali, provvedimento del 24 novembre 2016 n. 488, doc. *web* n.5796783 (consultabile al sito istituzionale *www.garanteprivacy.it*), che ha bloccato un progetto di banca dati privata per la misura del «*rating* reputazionale» tramite incrocio di dati immessi volontariamente sulla piattaforma e dati recuperati dalla rete mediante operazioni di *webcrawling*.

[14] J. RIFKIN, *L'era dell'accesso*, Milano, 2001, p. 17 ss.

[15] Per una interessante analisi della figura dell'«uomo di vetro» in relazione ai totalitarismi e al rispetto della vita privata si veda S. NIGER, *Le nuove dimensioni della privacy*, Padova, 2006, p. 33 - 35.

[16] S. RODOTÀ, *Tecnopolitica*, Roma-Bari, 2004, p. 175. Nello stesso senso, ID., *La vita e le regole. Tra diritto e non diritto*, Milano, 2006, p. 104.

[17] Cfr. N. BOBBIO, *Il futuro della democrazia*, Torino, 1995, p. 215 ss.

[18] S. RODOTÀ, *Il mondo nella rete, Quali i diritti, quali i vincoli*, Roma-Bari, 2014, p. 27 ss.

possibilità di disporre liberamente di una massa crescente di informazioni» [19], in una sempre più stretta alleanza tra logica di mercato e logica della sicurezza.

Ecco che il valore attribuito delle informazioni [20] cresce esponenzialmente per i grandi attori economici e politici a livello globale [21], mentre pare pericolosamente decrescere in misura pressoché proporzionale per i titolari di dette informazioni [22], che sembrano non avvedersi adeguatamente del fatto che «nella società digitale noi siamo i nostri dati» [23].

I dati costituiscono una traccia della persona, frammenti della stessa che ne rivelano caratteristiche e peculiarità, anche attinenti alla vita privata, e che nella loro complessità e combinazione/ricombinazione consentono di ricostruire il sistema di relazioni, di vita, di abitudini e di interessi che la caratterizzano; ecco perché nella c.d. «dittatura dell'algoritmo» [24], conoscere la logica del trattamento dei propri dati consente di esercitare un controllo – seppur in realtà non diffusivo – sugli stessi di fronte al processo di «spoliazione tecnologica» che reca con sé tutti i rischi, sempre più concreti e preoccupanti, di una spersonalizzazione dell'uomo. Una vera e propria eclissi dell'identità nella «comunità informazionale e della comunicazione» [25], in cui la persona rischia di perdere il sé – espropriato dalla società

[19] S. RODOTÀ, *Tecnopolitica*, cit., p. 136.

[20] «Il comportamento di tutti gli esseri può essere ricostruito in termini di scambio dell'informazione», come si legge in WIENER, *Introduzione alla cibernetica*, Torino, 1996, p. 84 ss.

[21] JOINSON, MCKENNA E POSTMES (a cura di), *Oxford Handbook of Internet Psychology*, Ulf-Dietrich Reips..

[22] Tale aspetto pare doversi sottolineare alla luce del c.d. *privacy paradox*, ovvero alla diffusa e paradossale incongruenza della condotta degli utenti di Internet che, pur formalmente preoccupati della tutela della propria riservatezza, rilasciano su base sistematica i propri dati in conseguenza di un vero e proprio «analfabetismo della *privacy*». Cfr. R. D'ORAZIO, *Protezione dei dati by default e by design*, in *La nuova disciplina europea della privacy*, a cura di Sica, D'Antonio e Riccio, p. 88.

[23] Si vedano, in questo senso, le parole del *Presidente dell'Autorità Garante dell'Autorità per la Protezione dei Dati Personali, Antonello Soro, in occasione della Giornata europea della protezione dei dati del 28 gennaio 2015, nell'ambito del convegno «Il pianeta connesso, la nuova dimensione della Privacy», i cui Atti sono rinvenibili sul sito istituzionale del Garante.*

[24] S. RODOTÀ, *Il mondo della rete*., cit., spec. p. 37.

[25] A. PUNZI, *op. cit*., p. 763, che richiama sul punto J. HABERMAS, *Fatti e norme. Contributi a una teoria discorsiva del diritto e della democrazia*, Milano, 1996.

dell'informazione in ossequio al principio della trasparenza, intesa come fine e non più come mezzo [26], tanto nella propria individualità che negli aspetti relazionali [27].

Così la sorveglianza non conosce più spazio e tempo, ma anzi «non vuole conoscere più confini, né ostacoli alla utilizzazione di qualsiasi tecnica. Si impadronisce dello spazio, fisico e virtuale, si appropria dei corpi, attribuendo peraltro un ruolo sempre più centrale alle tecniche biomediche» [28]. Di qui la centralità, e le criticità connesse, di alcune categorie particolari di dati, come i dati genetici e biometrici, come si vedrà.

2. La questione della sorveglianza nell'evoluzione della nozione di *privacy*

Il tema della protezione dei dati appare intimamente connesso e intrecciato con il tema del controllo fin dalle sue origini. D'altra parte, per comprendere il passaggio dal *Right to privacy* di Warren e Brandeis [29] al diritto alla protezione dei dati personali, inteso come controllo sui propri dati e difesa dal controllo che altri può esercitare anche attraverso tali dati, occorre porre mente alla rilevante differenza in punto al ruolo ed alla presenza dello Stato tra sistema americano e sistema europeo. In estrema sintesi e per semplificare, se nel mondo americano al centro del sistema vi era l'autonomia dei privati e la libertà individuale, la storia europea si è giocata sulla dialettica sovrano-sudditi prima, sulla realtà dello Stato assoluto poi, sul rapporto tra Stato-nazione e cittadini dopo la Rivoluzione francese, fino ad arrivare alle

[26] Si veda J. BENTHAM, *Panopticon ovvero la casa d'ispezione*, Venezia, 2009, in part. p. 36., che ben rappresenta il concetto di sorveglianza costante ancorché potenziale, e che va ad investire l'insieme delle relazioni sociali, da cui si può evincere che la sorveglianza è idonea a generare assetti nuovi dei poteri. Come evidenziato da M. FOUCAULT, *Sorvegliare e punire. Nascita della prigione*, trad. it., Torino, 2014, p. 225, «il dispositivo panoptico non è semplicemente una cerniera, un ingranaggio tra un meccanismo e una funzione; è un modo di far funzionare delle relazioni di potere entro una funzione, e una funzione per mezzo di queste relazioni di potere». Nel pensiero di Bentham, i fini cui la sorveglianza tende possono essere raggiunti mediante la costruzione dei relativi edifici «ove gli individui che devono essere controllati saranno il più assiduamente possibile sotto gli occhi delle persone che devono controllarli. L'ideale, se questo è lo scopo da raggiungere, esigerebbe che ogni individuo fosse in ogni istante in questa condizione. Essendo questo impossibile, il meglio che si possa auspicare è che in ogni istante, avendo motivo di credersi sorvegliato, e non avendo i mezzi di assicurarsi il contrario, creda di esserlo»; è altresì importante «che per una porzione di tempo. la più lunga possibile, ogni uomo sia realmente sotto sorveglianza». Si tratterebbe perciò di «di una società trasparente, al tempo stesso visibile e leggibile in ciascuna delle sue parti; che non ci siano più zone oscure, zone regolate da privilegi del potere reale o dalle prerogative di questo o di quel corpo, o ancora dal disordine; che ciascuno, dal punto di vista che occupa, possa vedere l'insieme della società; che i cuori comunichino gli uni con gli altri, che gli sguardi non incontrino più ostacoli, che regni l'opinione, l'opinione di tutti su tutti». Cfr, M. FOUCAULT, *Introduzione*, in J. BENTHAM, *Panopticon*, cit., p. 14.

[27] Cfr. S. RODOTÀ, *Il mondo della rete.* cit., p. 37, in cui l'Autore sottolinea la necessità di «sottrarre la persona alla "dittatura dell'algoritmo", emblema di una società della spersonalizzazione, nella quale scompare la persona del decisore, sostituito appunto da procedure automatizzate; e scompare la persona in sé considerata, trasformata in oggetto di poteri incontrollabili. (...) Alle tecnologie dell'informazione e della comunicazione, infatti, è stata attribuita una virtù, quella di rendere la società più trasparente proprio per quanto riguarda la possibilità di controlli diffusi sul potere, su qualsiasi potere. Ma quando l'algoritmo diviene il fondamento stesso del potere esercitato da un soggetto, com'è nel caso assai enfatizzato di Google, e tutto ciò che lo riguarda è avvolto dalla massima segretezza, allora siamo davvero di fronte alla nuova versione degli *arcana imperii*, che non tutelano soltanto l'attività d'impresa, ma si impadroniscono, direttamente o indirettamente, della vita stessa delle persone».

[28] Cfr. S. RODOTÀ, *Tecnopolitica*, cit. p. 177.

[29] S. D. WARREN - BRANDEIS, *The Right To Privacy*, in *Harvard Law Rev.*, 1890, 4, p. 193.

derive autoritarie e totalitarie del primo Novecento, caratterizzate dal diffondersi di forme sempre più pervasive di controllo, orientate ad una vera e propria sorveglianza capace di distinguere e classificare (nel senso etimologico del termine, composta da «classe» e «facere») sulla base delle informazioni sugli stessi [30], operazione poi facilitata dall'evoluzione tecnologica.

In particolare, sono gli anni Settanta della *privacy* a porre per la prima volta le questioni più problematiche sul punto.

L'avvento, infatti, degli elaboratori elettronici e delle banche dati [31], e la loro veloce e capillare diffusione riempivano infatti di nuova attualità la questione della *privacy*, comportando «una vera e propria rivoluzione copernicana nei metodi di elaborazione, selezione e ricerca dei dati» [32], fondata sull'archiviazione e raccolta di masse di informazioni, suscettibili di essere rielaborate, indicizzate, classificate, trattate e reperite, utilizzando una capacità di calcolo impensabile fino a quel momento e scardinando la stessa nozione di tempo, dal momento che l'informazione poteva circolare rapidamente quanto mai prima. Uno sconvolgimento così forte nel rapporto che l'uomo poteva instaurare con le informazioni non poteva non indurre anche una rivoluzione culturale e sociale dell'epoca, tanto da segnare il diffondersi di una vera e propria «sindrome da elaboratore» [33]. Con la medesima rapidità comincia a mutare anche la qualità stessa dei dati, dal momento che le nuove potenzialità connesse all'elaborazione elettronica degli stessi consentivano un nuovo utilizzo di quei dati, suscettibile di incidere in modo sempre più pervasivo nella sfera giuridica dell'individuo [34]. Questo nuovo potere dei dati e sui dati consente di far emergere un profilo complessivo della persona dall'intreccio dei medesimi e costituire una rete di relazioni intorno alla stessa, che ne permette, attraverso «*l'inferential relational retrieval*, di cui parla Paul Baran» [35], una valutazione pressoché completa e un controllo da parte di chi disponga del

(30) Cfr. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali.*, cit., p. 52, in cui si afferma che «In sostanza, è proprio la crisi del primo dopoguerra che apre lo scenario europeo del controllo globale dei cittadini (…)», fenomeno da leggere in connessione con l'evoluzione tecnologica del tempo, infatti «In USA, la tecnologia della stampa spinse a 'costruire' il diritto alla *privacy* come limite (…). In Europa, lo sviluppo della tecnologia del controllo, con la sua sempre più penetrante capacità di raccogliere, trattare, archiviare dati sui comportamenti delle persone, riporta i cittadini alla condizione di sudditi dello Stato totalitario», per cui «quello che nel mondo americano nasce come Right to *privacy* (…), nel continente europeo si afferma invece come "Diritto alla protezione dei dati personali", inteso come diritto di libertà, legato al diritto dell'individuo a non essere sottoposto a controlli e raccolta di informazioni sulla propria vita senza il suo consenso o senza che sussistano ragioni di prevenzione o repressione (...)».

(31) Per una ricostruzione delle problematiche relative alle banche dati oggi alla luce del reg. UE n. 2016/679 cfr. G. PALAZZOLO, *La banca dati e le sue implicazioni civilistiche in tema di cessione e deposito alla luce del Reg. (UE) n. 2016/679*, in *Contr. e impr.*, 2017, 2, p. 613 ss.

(32) S. NIGER, *op. cit.*, p. 63.

(33) S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit., p. 9.

(34) GIACOBBE, *Banche dati e tutela della persona*, in *Ann. Messina*, 1984, p. 21 ss.; ID., *Riservatezza* (*diritto alla*) voce, in *Enc. dir.*, XL, 1989 in cui l'a. afferma che «La peculiarità anche sotto il profilo giuridico, che il problema presenta per effetto dell'esistenza di queste nuove tecniche di elaborazione dei dati, va ricercata non tanto o non soltanto sotto il profilo quantitativo, bensì sul terreno della diversità qualitativa».

(35) S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit. p. 14.

mezzo adeguato. Un processo inesorabile, che è stato colto dalla dottrina che ha posto l'accento sul nesso tra l'uso degli elaboratori elettronici e un processo di immiserimento del cittadino, una riemersione della figura del suddito e un prepotente imporsi di quella del consumatore [36].

Diventano disponibili enormi masse di informazioni suscettibili di essere usate «per estrarre profili individuali e di gruppo, per individuare comportamenti prevalenti, con la concreta possibilità di definire criteri di normalità e di cercare di imporli» [37], tanto che l'attenzione si sposta verso una nuova dimensione della persona e acquista così centralità il c.d. «corpo elettronico» [38], che sta di fronte al «nuovo potere di dominio sociale» creato per questa via sull'individuo, il «potere informatico» [39].Nella nuova società della sorveglianza così creata intorno al moderno «uomo di vetro» [40], la difesa della libertà informatica dinanzi all'assalto di poteri pubblici e privati diviene un obiettivo da perseguire [41].

Questa metamorfosi della persona nel suo corpo elettronico, che già reca in sé il germe dello «spossessamento e frantumazione» della persona, la cui unità verrà spezzata con il successivo avvento di Internet, pone già allora le basi per la costruzione di una nuova dimensione della persona fondata sui suoi dati [42] e di una «nuova antropologia», destinata a tributare sempre maggiore centralità alla *digital person* [43] e all' identità digitale dell'individuo, concetto fluido di cui nel tempo si impossessa l'informatica [44].

Orbene, a questo «corpo elettronico», diviene quindi necessario ed imprescindibile estendere quelle garanzie di libertà personale attribuite alla persona, di modo che dall' *habeas corpus* [45] si passi all' *habeas data* [46]. Ormai diventa evidente come nella «democrazia elettronica», in cui alle tecniche dell'informazione

(36) N. BOBBIO, *Stato, governo, società. Frammenti di un dizionario politico*, Torino, 1985, p. 21, in cui si legge che «l'uso degli elaboratori, permette e sempre più permetterà ai detentori del potere di vedere il pubblico assai meglio che negli Stati del passato. Ciò che il novello Principe può venire a sapere dei propri soggetti è incomparabilmente superiore a ciò che poteva sapere dei suoi sudditi anche il monarca più assoluto del passato». In questo modo «si immiserisce la figura del cittadino, mentre riemerge quella del suddito e si impone prepotentemente quella del consumatore. Non è soltanto lo spazio virtuale ad essere trasformato. Anche lo spazio reale, i tradizionali luoghi pubblici – strade, piazze, parchi, stazioni, aeroporti – vengono sempre più sottoposti ad un controllo capillare, scrutati implacabilmente, segnando così il passaggio da una sorveglianza mirata ad una generalizzata».

37 S. RODOTÀ, *Repertorio di fine secolo*, cit., p. 192.

38 ID., *Tecnologie e diritti*, cit., p. 41.

39 V. ZENO ZENCOVICH (a cura di), *La tutela dei dati personali. Commentario alla L. 675/96*, Padova, 1997, p. 5.

40 S. RODOTÀ, *Tecnopolitica*, cit., p. 175 e ID., *La vita e le regole*, cit., p. 104.

41 T. E. FROSINI, *La democrazia nel XXI secolo*, Macerata, 2010, p. 41, in cui si legge che «la libertà di custodire la propria riservatezza informatica [che] è divenuta anche la libertà di comunicare ad altri le informazioni trasmissibili per via telematica, cioè la libertà di usufruire delle reti di trasmissione senza limitazioni di frontiere, una libertà di espressione della propria personalità valendosi dei sistemi di comunicazione automatizzata».

42 S. RODOTÀ, *Antropologia dell'homo dignus*, cit., p. 547 ss.

43 Cfr. S. RODOTÀ, *Il mondo nella rete*, cit., p. 42.

44 G. ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. e impr.*, 2017, 3, p. 723 ss.

45 Cfr. S. RODOTÀ, *Libertà personale. Vecchi e nuovi nemici*, in *Quale libertà. Dizionario minimo contro i falsi liberali*, a cura di BOVERO, Roma-Bari, 2004, p. 52.

46 S. RODOTÀ, *Il nuovo habeas corpus: la persona costituzionalizzata e la sua determinazione*, a cura di Rodotà e Tellachini, in *Trattato di Biodiritto*, tomo *Ambito e fonti del biodiritto*, diretto da S. RODOTÀ e P. ZATTI, Milano, 2010, p. 229; ID, *Il mondo nella rete*, cit., p. 69.

viene demandato il compito di costruire dal basso una nuova democrazia dei cittadini e alle tecniche della sorveglianza quello di creare dal basso un meccanismo capillare di sorveglianza sugli stessi [47], sia necessario elaborare uno «statuto dell'informazione» [48].

Parallelamente alla metamorfosi della persona anche la *privacy* muta di significato, perdendo di significato generale come mero diritto ad essere lasciato solo, e sempre più trasfigurandosi come diritto di mantenere un controllo sulle proprie informazioni [(49)], che costituiscono, per così dire, il DNA nella nuova *digital person*.

Il tema della sorveglianza ricollegata al controllo dei dati si rivela una preoccupazione da sempre ricorrente della giurisprudenza multilivello.

Già la Corte costituzionale tedesca, in una importante pronuncia del 1983 in materia di autodeterminazione informativa, aveva fondato il proprio sindacato di costituzionalità, incentrato sul valore della dignità dell'uomo, proprio sulla necessità di «impedire un passo importante, forse decisivo, per la trasformazione della Germania federale in uno stato di sorveglianza». Chiamata a pronunciarsi sulla costituzionalità di una legge sul censimento approvata dal Parlamento federale nel 1982, con una nota e importante decisione del 1983 [50], aveva segnato un'evoluzione nella nozione di *privacy* e protezione dei dati personali, giungendo al riconoscimento un diritto all'autodeterminazione informativa (*informationelle Selbstbestimmungsrecht*) radicato nell'art. 2 comma 1, che sancisce il principio della libertà individuale, letto in combinato disposto con l'art. 1, comma 1 della *Grundgesetz* sulla dignità dell'uomo. Il ricorso al sindacato di costituzionalità veniva inteso come l'ultima possibilità per «porre un limite alla "fame di dati" dello Stato e impedire un passo importante, forse decisivo, per la trasformazione della Germania federale in uno "Stato di sorveglianza", trasformazione che avrebbe comportato la vanificazione di quelle garanzie che si riassumono nella formula "Stato di diritto"» [51]. Richiamando sul punto alcune proprie precedenti significative sentenze [52], la Corte riconosceva allora il diritto all'autodeterminazione sulle informazioni, inteso come la «facoltà del singolo di decidere essenzialmente da sé circa la cessione e l'uso dei propri dati personali», segnando con ciò un'importante evoluzione giurisprudenziale rispetto alla precedente cosiddetta «teoria delle sfere (*Sphärentheorie*)», fondata sull'assunto che l'intensità della tutela della persona dovesse essere inversamente proporzionale alla «socialità» del comportamento. La Corte afferma altresì che «non c'è nelle condizioni della moderna elaborazione dei dati alcun dato senza importanza, ha rilievo

[47] S. RODOTÀ, *Controllo e privacy della vita quotidiana*, cit.
[48] G. ALPA, *Privacy e Statuto dell'informazione*, cit., p. 119.
[49] S. RODOTÀ, *Repertorio di fine secolo*, cit., p. 189 e ID., *Tecnopolitica*, cit., p. 101.
[50] *Bundesverfassungsgericht*, sentenza 15 dicembre 1983, in *Entscheidungen des Bundesverfassungsgerichts*, 1984, 65, p. 1-71.
[51] G. SARTOR, *Tutela della personalità e normativa per la «protezione dei dati». La sentenza della Corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del «Datenschultz»*, in *Inf. e dir.*, 1986, p. 98 - 99.
[52] Per una disamina di tali precedenti, si veda V. ROPPO, *I diritti della personalità*, in *Banche dati, telematica e diritti della persona*, a cura di G. ALPA e M. BESSONE, p. 73 ss.

al fine di determinare il significato di un dato per il diritto della personalità, la conoscenza del suo contesto di utilizzo (…) solo quando vi sia chiarezza sugli scopi per i quali dati sono stati richiesti, e sulle possibilità di connessione e di utilizzo che sussistano, è possibile rispondere alla domanda circa l'ammissibilità di una limitazione del diritto all' autodeterminazione informativa» [53].

Con ciò anticipando una preoccupazione che rimarrà ricorrente nella giurisprudenza della Corte europea dei diritti dell'uomo, e che negli ultimi anni è divenuta oggetto di un serrato dialogo della stessa con la Corte di Giustizia dell'Unione europea.

3. Il tema della sorveglianza connesso alla questione del controllo sui dati nel dialogo tra Corte di Giustizia e Corte europea dei diritti dell'Uomo

Nel contesto di tale circuito di dialogo tra le Corti europee in tema di diritti [54], è anzitutto interessante notare come sia la stessa Corte di Giustizia a istituire e rafforzare il solido collegamento tra la protezione dei dati personali e l'interpretazione dell'art. 8 CEDU. Ciò emerge, ad esempio, dalla sentenza *Digital Rights Ireland*, su cui *infra,* che sottolinea [55] la possibilità che «la giurisprudenza della Corte europea dei diritti dell'uomo relativa all'art. 8 CEDU possa fornire indicazioni interpretative rilevanti ai fini dell'interpretazione» dell'art. 8 CDFUE in materia di protezione dei dati [56]; nonché dalle conclusioni

[53] *Bundesverfassungsgericht*, sentenza 15 dicembre 1983, in *Entscheidungen des Bundesverfassungsgerichts*, 1984, 65, p. 45. A p. 43 si legge anche che «un ordinamento sociale ed un ordinamento giuridico (…), nel quale i cittadini non potessero sapere da chi, come, quando, in quale occasione sono conosciute informazioni che ti riguardano, sarebbero incompatibili con il diritto all'autodeterminazione informativa. Chi è incerto se comportamenti devianti siano registrati, memorizzati durevolmente, utilizzati e trasmessi come informazione, sarà portato ad evitare quei comportamenti. Chi ritiene che la sua partecipazione ad una riunione o ad una iniziativa civica possa essere registrata dalle autorità e che da ciò possano derivare per lui dei rischi, rinuncerà forse ad esercitare i corrispondenti diritti fondamentali (…). Ciò pregiudicherebbe non solo le possibilità di realizzazione dell'individuo, ma anche l'interesse generale, in quanto l'autodeterminazione è una condizione elementare di una società libera e democratica (...)».

[54] Il tema è ampiamente studiato in dottrina. Nell'impossibilità di richiamare in maniera esaustiva la bibliografia inerente, ci si limita qui a richiamare i seguenti: P. GIANNITI, *La CEDU e il ruolo delle Corti*, in *Commentario del Codice civile e codici collegati Scialoja- Branca- Galgano*, Bologna, 2015; R. COSIO e R. FOGLIA (a cura di), *Il diritto europeo nel dialogo delle Corti*, Milano, 2013; A. BARBERA, *Le tre Corti e la tutela multilivello dei diritti*, in *La tutela multilivello dei diritti*, a cura di Bilancia e De Marco, Milano, 2005; M. CARTABIA, DE WITTE, PÉREZ e TREMPS (a cura di), *Constitución europea y Constituciones nacionales*, Valencia, 2005; GROSSI, *L'Europa del diritto*, Roma-Bari, 2007; O. POLLICINO, *Allargamento ad est dello spazio giuridico europeo e rapporto tra Corti costituzionali e Corti europee. Verso una teoria generale dell'impatto interordinamentale del diritto sovranazionale?*, Milano, 2010; E. FALLETTI e V. PICCONE (a cura di), *L'integrazione attraverso i diritti. L'Europa dopo Lisbona*, Roma, 2010; M. FRAGOLA (a cura di), *La cooperazione fra Corti in Europa nella tutela dei diritti dell'uomo*, Napoli, 2012; B. RANDAZZO, *La CEDU. Nel sistema costituzionale italiano*, Milano, 2012; E. MALFATTI, *I "livelli" di tutela dei diritti fondamentali nella dimensione europea*, Torino, 2013; V. SCIARABBA, *Tra fonti e Corti. Diritti e principi fondamentali in Europa: profili costituzionali e comparati degli sviluppi sovranazionali*, Padova, 2008; G. MARTINICO, *L'integrazione silente. La funzione interpretativa della Corte di Giustizia e il diritto costituzionale europeo*, Napoli, 2009; O. POLLICINO - V. SCIARABBA, *La Corte di Giustizia dell'Unione europea e la Corte europea dei diritti dell'uomo quali Corti costituzionali*, in *Sistemi e modelli di giustizia costituzionale*, a cura di L. MEZZETTI, Padova, 2011, II; D. TEGA, *I diritti in crisi. Tra Corti nazionali e Corte europea di Strasburgo*, Milano, 2012; L. TRUCCO, *Carta dei diritti fondamentali e costituzionalizzazione dell'Unione europea. Un'analisi delle strategie argomentative e delle tecniche decisorie a Lussemburgo*, Torino, 2013.

[55] Cfr. punto 21, questione n. 2 lett. *e*) della sentenza richiamata.

[56] Più in generale, sul tema della equivalenza/comparabilità tra le tutele approntate in difesa dei diritti fondamentali a livello comunitario e della CEDU si vedano G. ZAGREBELSKY, *L'UE e il controllo esterno della protezione dei diritti e delle*

dell'Avvocato generale nel noto caso *Google Spain* [57], in cui si evidenzia che «conformemente all'art. 52, par. 3, della Carta, la giurisprudenza della Corte europea dei diritti dell'uomo sull'art. 8 della CEDU è rilevante tanto ai fini dell'interpretazione dell'art. 7 quanto ai fini dell'applicazione della Direttiva in conformità con l'art. 8 della Carta».

La questione della sorveglianza [58] legata al controllo dei dati è ampiamente affrontata dalla Corte europea dei diritti dell'uomo (si veda *infra*), ma vale ora la pena di istituire intanto un confronto con i ragionamenti della Corte di Giustizia in tema. Non può quindi non venire in rilievo, sul punto, la prima di quel trittico di sentenze [59] in materia di *privacy* e protezione dei dati personali, assunte tra il 2014 e il 2015, che hanno contribuito all'«emersione, sempre più prepotente, (…), di un vero e proprio digital right to *privacy*» [60], poi confluito nel Regolamento generale di protezione dei dati personali (GDPR) [61], in cui gli artt. 7 e 8 della Carta si pongono per la Corte di Giustizia nel bilanciamento tra esigenze di sicurezza e protezione dei dati nella dimensione interna della loro circolazione. [62] quali veri e propri «fari», immagine evocativa

libertà fondamentali in Europa. La barriera elevata dalla Corte di Giustizia, in *DUDI*, 2015, p. 1 ss.; DE SCHUTTER, *Bosphorus Post-Accession: Redefining the Relationships between the European Court of Human Rights and the Parties*, in *The EU Accession to the ECHR*, edited by Kosta, Skoutaris e Tzevelekos, Oxford, 2014, p. 177 ss.; DOUGLAS e SCOTT, *The Relationship between the EU and the ECHR Five Years on from the Treaty of Lisbon*, in *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years Old and Growing*, edited by De Vries, Bernitz e Weatherill,Oxford, 2015.

[57] Sentenza della Corte di Giustizia (Grande Sezione) del 13 maggio 2014, *Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, causa C-131/12. Tra i commenti, *ex multis,* G. RESTA e V. ZENO ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield",* Roma, 2016; T. E. FROSINI, *Diritto all'oblio e Internet, in www.federalismi.it*, 10 giugno 2014; F. PIZZETTI, *La decisione della Corte di giustizia sul caso Google Spain: più problemi che soluzioni, in www.federalismi.it 10 giugno 2014;* G. E. VIGEVANI*, Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano,* in *Danno e resp.*, 2014, 7, p. 751 ss.; C. BLENGINO, *La Corte di giustizia e i motori di ricerca: una sentenza sbagliata, in www.medialaws. eu,* 19 maggio 2014; *O.* POLLICINO e M. BASSINI, *Reconciling Right to Be Forgotten and Freedom of Information: Past and Future of Persona Data Protection in Europe,* in *DPCE*, 2014, 2, p. 641; M. BASSINI, *Il diritto all'oblio ai tempi di Internet: la Corte di giustizia sui motori di ricerca,* in *Quad. cost.,* 2014, 3, p. 730.

[58] Sul tema della sicurezza e della sorveglianza cfr G. RESTA, *La sorveglianza elettronica di massa il conflitto regolatorio USA/UE*, in *Dir. inform.*, 2015, 4-5, p. 697 ss.; G. BUTTARELLI, *Privacy, sicurezza e nuove tecnologie al bivio di nuove scelte strategiche*, in federalismi.it, 2015, (14 gennaio 2015); M. OROFINO, *Diritto alla protezione dei dati personali sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Riv. dir. dei media*, 2018; G. SARTOR e DE AZEVEDO CUNHA, *op. cit.* Si vedano anche G. DE VERGOTTINI, *Guerra e Costituzione*, Bologna 2004; ID., *Il bilanciamento tra sicurezza e libertà civili nella stagione del terrorismo*, in *Sicurezza: le nuove frontiere*, a cura di Aa.Vv., 2005, p. 110; T. GIUPPONI, *Contro il "diritto alla sicurezza". Immigrazione, sicurezza e autonomie territoriali nella più recente giurisprudenza della Corte costituzionale*, in *Studi in onore di Giuseppe de Vergottini*, a cura di Aa.Vv, Padova, 2015, I, p. 719 ss.

[59] Cfr. O. POLLICINO e M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *Dir. inform.*, 2015, che parla di «trittico di decisioni».

[60] O. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Dir. inform.*, 2014, p. 7 ss.

[61] Per un approfondimento sul ruolo e influenza della giurisprudenza della Corte di Giustizia sui contenuti del nuovo regolamento, cfr. A. MANTELERO, *Il futuro regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella digital economy*, in *Dir. inform.*, 2014, p. 681 - 701, nonché G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, cit., p. 779 ss.

[62] Cfr L. TRUCCO, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. it*, 2014, p. 1855 sulla funzione nomopoietica della Corte di Giustizia a partire dalla Carta di Nizza. Cfr. anche M. CARTABIA (a cura di), *I diritti nazione. Universalità e pluralismo dei diritti fondamentali nelle corti europee*, Bologna, 2007, p. 29 ss.

suggerita proprio dalla Corte nei numerosissimi passaggi in cui afferma di ragionare «*in the light of the Charter*».

La Corte si è infatti occupata della circolazione dei dati personali nella «dimensione interna» nel noto caso *Digital Rights Ireland*, con sentenza, resa l'8 aprile 2014 [63], con riferimento al regime di conservazione dei dati previsto dalla dir. 2006/24/CE, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, esaminando la questione della validità alla luce degli artt. 7, 8, nonché 11 della Carta in tema di libertà di espressione, che, vale qui la pena di sottolineare, non è stato neppure esaminato dalla Corte di Giustizia, ritenendolo assorbito nelle precedenti.

In particolare la Corte, chiamata a giudicare in primo luogo su quale sia il rapporto tra il «diritto dell'Unione», di cui fa menzione il par. 3 dell'art. 52 della Carta, e la normativa in materia di protezione dei dati, nonché sulla necessità di tener conto, nell'interpretazione dell'art. 8 della Carta stessa, dei cambiamenti derivanti dalle norme successive di diritto derivato, sulla portata dei limiti alle restrizioni che il diritto derivato può apportare in relazione all'ambito dei diritti fondamentali, nonché infine sulla possibilità che «la giurisprudenza della Corte europea dei diritti dell'uomo relativa all'art. 8 CEDU possa fornire indicazioni interpretative rilevanti ai fini dell'interpretazione di quest'ultimo articolo» (punto 21, questione n. 2 lett. *e*), esordisce con la constatazione che l'obbligo di conservazione dei dati contenuto nella disciplina portata al suo esame solleva questioni relative alla protezione della vita privata, in considerazione del fatto che i dati conservati, considerati nel loro complesso, sono suscettibili di consentire di «trarre conclusioni molto precise riguardo la vita privata delle persone», permettendo, in ultima analisi di tracciare un quadro completo e fedele dell'identità individuale e relazionale della persona, quale essa si esplica nell'ambito della propria vita privata [64].

---

[63] Per alcuni commenti, L. TRUCCO, *Data retention*: *la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. it.*, 2014, 8-9, p. 1850 ss.; R. FLOR, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. «data retention» contraria ai diritti fondamentali. Una lunga storia a lieto fine?,* in *Riv. Trim. di Diritto penale contemporaneo*, 2014, 2, p. 178 ss.; M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE*: *prospettive ed evoluzioni future del sistema europeo di data retention, in Il Dir. UE*, 2014, 4, p. 803 ss.; F. FABBRINI, *The European Court of justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.*, in *Harvard Human Rights J.*, 2015, 28, p. 65; S. SCAGLIARINI, *La Corte di Giustizia bilancia il diritto alla vita privata e lotta alla criminalità: alcuni "pro" e alcuni "contra",* in *Dir. inform.*, 2014, p. 873 ss.; C. CASCIONE, *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione "data retention" della Corte di giustizia e gli echi del "Datagate",* in *Nuov giur. civ.*, 2014, 1, p. 1044 ss.; E. A. ROSSI, *Il diritto alla "privacy" nel quadro giuridico europeo ed internazionale alla luce delle recenti vicende sulla sorveglianza di massa,* in *Dir. com. scambi internaz.*, 2014, p. 331 ss.

[64] Analoghe considerazioni si ritrovano anche nella giurisprudenza costituzionale tedesca. Cfr. *BverfG*, 2 marzo 2010, I, Bvr 256/08, 1 BvR 263/08, 1 BvR 586/08., in cui la Corte costituzionale tedesca, nel dichiarare l'incostituzionalità della normativa tedesca di recepimento della Direttiva del 2006 per contrasto con l'art. 10.1 del *Grundgesetz,* ha considerato particolarmente grave l'ingerenza prodotta dalla sorveglianza delle comunicazioni nella vita privata degli utenti intercettate, perché le relazioni sociali di ciascuno sarebbero potute essere agevolmente ricostruite, proprio muovendo dai dati personali sul traffico telematico o telefonico.

La Corte, pertanto, ravvisa nel sistema approntato dalla direttiva un'ingerenza «di vasta portata e (...) e particolarmente grave» [65] nei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta, sottolineando come l'obbligo di conservazione dei dati costituisca di per sé un'interferenza nel diritto al rispetto della vita privata, mentre l'accesso costituisca «un'ingerenza supplementare in tale diritto fondamentale», richiamando significativamente sul punto la giurisprudenza della Corte EDU sull' art. 8 CEDU [66] in tema di memorizzazione di dati a fini di creazione di dossier. Ciò perché, imponendo la conservazione delle informazioni e permettendone l'accesso alle autorità, la direttiva deroga al regime di tutela del diritto al rispetto della vita privata istituito dalla normativa in materia di protezione dei dati personali, indipendentemente dal carattere sensibile dell'informazione o degli eventuali inconvenienti o pregiudizi subiti dagli interessati a seguito di tale ingerenza, finendo per ingenerare nelle persone interessate «la sensazione che la loro vita privata sia oggetto di costante sorveglianza» [67], amplificata peraltro dal fatto che tale conservazione e utilizzo ulteriore possono essere effettuati senza che l'utente ne sia neppure informato [68].

Sottolinea in primo luogo come la conservazione, pur costituendo un'ingerenza particolarmente grave in tali diritti, non permettendo di venire a conoscenza del contenuto delle comunicazioni elettroniche in quanto tale, «non è tale da pregiudicare il (...) contenuto» essenziale del diritto al rispetto della vita privata, così come non è idonea di per sé a pregiudicare neppure il contenuto dell'art. 8. D'altra parte, le limitazioni contenute nella direttiva rispondono indubbiamente, nel ragionamento della Corte, ad un obiettivo di interesse generale perseguito dall'Unione, contribuendo alla lotta contro la criminalità e contro il terrorismo internazionale in particolare, dal momento che «l'art. 6 della Carta enuncia il diritto di ogni persona non solo alla libertà, ma altresì alla sicurezza» (par. 44).

Giungendo poi ad effettuare il vaglio di proporzionalità dell'ingerenza constatata, sottolineato ancora una volta il «ruolo importante (…) svolto dalla protezione dei dati personali sotto il profilo del diritto

[65] Cfr. par. 37 della sentenza.

[66] Corte EDU, sentenze *Leander c. Svezia* 26 marzo 1987, nonché *Rotaru c. Romania* n. 28341/1995, e *Weber e Saravia c. Germania*, n. 54934/00, richiamate al punto 35 della sentenza. È qui interessante notare come il richiamo alla giurisprudenza della Corte EDU da parte della Corte di Giustizia, particolarmente in questa materia, non sia affatto isolato, ma costituisca soltanto una battuta del dialogo incessante tra le corti sul punto. Nella stessa sentenza *Digital Rights Ireland* la Corte a più riprese cita la giurisprudenza EDU, in particolare al punto 47 in relazione alla declinazione del principio di proporzionalità nell'ambito dei diritti fondamentali (richiamandosi alla sentenza EDU *S e Marper c. Regno Unito*, nn. 30562/04 e 30566/04 par. 102), nonché al punto 54 in relazione alla necessità di prevedere regole chiare e precise disciplinanti la portata, l'applicazione e requisiti minimi delle misure che incidono sulla tutela dei dati personali, per scongiurare il rischio di abusi e gli eventuali accessi e usi illeciti di dati (qui, tra le altre, richiamando invece la sentenza Corte EDU *Liberty e altri c. Regno Unito*, n. 58243/00 del 1 luglio 2008), e infine al punto 55 in relazione ai trattamenti automatizzati di dati personali.

67 Cfr. par. 37 della sentenza.

[68] Sullo sfondo di questa vicenda, e più in generale degli sforzi recente della Corte di giustizia, si colloca proprio la problematica della sorveglianza globale. Cfr. anche ROSSI DAL POZZO, *Protezione dei dati personali e diritti fondamentali della persona: le nuove norme sui "codici di prenotazione" (PNR)*, in *Riv. dir. int. priv. proc.*, 2016, 4, p. 1020 ss.

fondamentale al rispetto della vita privata» [69], al fine di accertare se la restrizione peraltro riguardante «la quasi totalità della popolazione europea» operi entro i limiti dello stretto necessario, la Corte si sofferma su tre profili: la mancanza generale di limiti alla conservazione dei dati nella dir. 2006/24/CE, l'assenza di alcun criterio oggettivo che permetta di delimitare l'accesso a tali dati da parte delle autorità nazionali, nonché la durata stessa della conservazione.

Sulla base della valutazione di questi tre profili, la Corte conclude che «adottando la dir. 2006/24/CE, il legislatore dell'Unione ha ecceduto i limiti imposti dal principio di proporzionalità alla luce degli artt. 7, 8, 52 par. 1 della Carta», dal momento che la stessa da un lato non prevede norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali in questione, tali da garantire che essa sia effettivamente limitata a quanto strettamente necessario; né prevede garanzie sufficienti che consentano una protezione efficace dei dati contro i rischi di abusi, accessi ovvero utilizzi illeciti degli stessi.

Preme qui sottolineare che il profilo della durata della conservazione appare problematico agli occhi della Corte, dal momento che la direttiva prevedeva un obbligo di conservazione per un periodo almeno semestrale senza far riferimento ad ulteriori criteri discretivi e obiettivi cui ancorare tale durata, così come il fattore tempo gioca un ruolo fondamentale nella conservazione dei dati anche nella interpretazione della Corte EDU, come si vedrà. [70]

Sulla scorta delle stesse premesse, poi, la Corte di Giustizia è intervenuta pure successivamente, ancora una volta, nella propria affermazione quale «giudice dei diritti» che contribuisce a fondare l'Unione Europea come «ordinamento a protezione avanzata» [71], nel dicembre 2016 [72], a istituire un solido collegamento tra riservatezza e comunicazioni elettroniche, affermando che «la Direttiva 2002/58/CE , relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, interpretata alla luce degli artt. 7, 8 e 11 nonché dell'art. 52, par. 1, della Carta dei diritti fondamentali, osta a una normativa nazionale la quale, a fini di lotta contro la criminalità: *a*) preveda una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e all'ubicazione di tutti gli utenti; *b*) non limiti l'accesso delle autorità nazionali competenti alla sola lotta contro la criminalità

[69] Sul punto, la Corte di Giustizia richiama significativamente la Corte EDU nel caso *Marper c. Regno Unito* del 2008 in materia di *privacy* genetica, su cui *infra*.

[70] Cfr. ad esempio, Corte EDU, M.K., c. Francia, 18 aprile 2013, ric. 19522/09, in particolare par. 27, menzionato dalla sentenza *Digital Rights*, su cui si veda A. SCARCELLA, *Diritto al rispetto della vita privata e conservazione di dati personali*, in *Cass. pen*., 2013, p. 2848 ss., nonché ID., *Conservazione delle impronte digitali degli assolti e violazione dell'art. 8 CEDU*, in *Dir. pen. proc*., 2013, p. 812 ss.

[71] Cfr. B. CAROTTI, *La Corte di Giustizia costruisce un ponte tra riservatezza e comunicazioni elettroniche*, in *Giorn. dir. amm*., 2017, 4, p. 479 ss., che valorizza l'immagine di un «ponte» tra le due, nell'ambito dell'Unione quale ordinamento dotato di strumenti di protezione rafforzata, richiamando sul punto U. BECK, *Case Comment: C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 SSHD v Tom Watson & Others*, in *Eutopia Law*, 13 gennaio 2017, su https://eutopialaw.com., laddove afferma che «*the Cjeu reiterated its judgment,in Digital Rights Ireland and Schrems*, *that generalised and indiscriminate surveillance is not permissible under EU law*».

72 Corte UE, 21 dicembre 2016, nelle cause riunite C-03/15 e C-698/15, *Tele2SverigeAB c. Post-och Telestyrelsen, e Secretary of State for the Home Department c. Tom Watson et al.*

grave e non ne sottoponga l'esercizio al controllo preventivo di un giudice o di un'autorità amministrativa indipendente; *c*) non richieda che i suddetti dati siano conservati nel territorio dell'Unione», mantenendo ancora una volta una lettura sostanziale dei diritti fondamentali in connessione con la tecnologia delle comunicazioni nella società dell'informazione, e inquadrando la questione della conservazione dei dati nel prisma di un triangolo di libertà: libertà di domicilio e di vita privata, ricavabili dagli artt. 7 e 8, nonché di espressione, di cui all'art. 11, fondando con ciò un ancor più stretto legame tra riservatezza, sorveglianza e libertà di espressione, in una logica che ricorda molto i ragionamenti della Corte EDU (su cui *infra*) nell'opera di interpretazione dell'art. 8 CEDU.

Sul punto, però, il possibile «dialogo con la CEDU», a fronte - ancora una volta - di un ampio richiamo da parte della Corte di Giustizia alla giurisprudenza CEDU [73], è stato sostanzialmente interrotto dalla dichiarazione di irricevibilità di una terza questione, che era stata sollevata, concernente la lettura degli artt. 7 e 8, in particolare sulla compatibilità con l'art. 8 CEDU di una loro interpretazione riduttiva, che consenta agli Stati un controllo generalizzato e privo di ragioni concrete, questione già ridimensionata anche dall'Avvocato generale Saugmandsgaard (parr. 75 e 76) alla luce della considerazione del fatto che «in assenza di adesione dell'Unione a tale Convenzione, quest'ultima non costituisce uno strumento giuridico formalmente integrato nell'ordinamento giuridico dell'Unione» [74], pur facendo parte i diritti fondamentali della CEDU del diritto dell'Unione in quanto principi generali a norma dell'art. 6, par. 3 TUE.

Il tema appare centrale da sempre nella giurisprudenza della Corte europea dei diritti dell'uomo sulle violazioni dell'art. 8, ad esempio in relazione alle attività di intercettazione di comunicazione e di sorveglianza per finalità di sicurezza. Sul punto, si è registrata un'inversione di tendenza nella giurisprudenza della Corte europea dei diritti dell'uomo, successiva alla giurisprudenza della Corte di Giustizia, segnatamente al caso *Digital Right Ireland*, ma ancor di più al successivo caso *Schrems* [75], in cui la Corte ripropone le medesime argomentazioni fornite nel primo caso nel bilanciamento tra esigenze di sicurezza e protezione dei dati personali nella dimensione esterna della loro circolazione (flusso transfrontaliero con gli USA). Proprio la sentenza *Schrems* (e la successiva *Schrems II* [76]) si iscrivono in un filone di giurisprudenza che, assieme ai crescenti interventi per la regolazione delle reti e alle operazioni di sorveglianza così condotte, rivela il collegamento con la contesa fra «due super-potenze internazionali (...) per il controllo di una risorsa essenziale quale le reti globali di telecomunicazioni». In tale contesto, lo strumento impiegato dall'Unione Europea è stato proprio una regolazione fortemente territoriale con

[73] Sul punto, B. CAROTTI, *La Corte di Giustizia costruisce un ponte tra riservatezza e comunicazioni elettroniche*, cit., p. 488.
[74] In tema, cfr. anche parere reso dalla Corte di giustizia il 18 dicembre 2014 (2/13).
[75] Tanto da essere definita il c.d. «*follow up*» di Schrems. Cfr. O. POLLICINO e BASSINI, *op. cit.*, p. 101.
[76] Corte di Giustizia dell'Unione europea, 16 luglio 2020, causa C-311/18.

effetti indirettamente (ma programmaticamente) ultratraterritoriali. In linea con tale impostazione, la Corte UE si erge nei casi sopracitati a strenua difesa dei diritti fondamentali per proclamare la c.d. «sovranità digitale» dell'Unione [77].

4. Segue. La prospettiva della Corte europea dei diritti dell'Uomo in tema di *mass surveillance*

Come accennato, il tema della sorveglianza ricorre con frequenza, se non insistenza, nella giurisprudenza EDU, nodo problematico riconnesso al rispetto della vita privata di cui all'art. 8 CEDU, messo in pericolo a più riprese da illegittime interferenze, su cui l'attenzione della Corte si rivela da sempre massima.

Si segnala in tema la sentenza *Leander c. Finlandia* del 1987, in un caso di raccolta e memorizzazione di dati in un registro segreto di polizia, in cui ancora non si fa alcun riferimento alla protezione dei dati personali, limitandosi la Corte a vagliare se tale memorizzazione costituisca un'ingerenza giustificabile alla luce del comma 2 dell'art. 8, e concludendo per un'assenza di violazione in tal senso.

A poco più di un decennio di distanza, invece, nella sentenza *Rotaru c. Romania*, la Corte in un caso analogo di memorizzazione di dati relativi alla affiliazione politica e risalenti alla gioventù del soggetto interessato, con conseguente creazione di un dossier che lo riguardava, muta orientamento, assumendo a referente esterno di valutazione inerente la protezione dati personali (come accadrà poi in altre pronunce successive) la Convenzione del Consiglio d'Europa n. 108 del 1981, sottolineando «la rispondenza di un'interpretazione estensiva della nozione di vita privata e quella elaborata dalla Convenzione del 1981, il cui scopo è garantire il rispetto della vita privata con riferimento ai trattamenti automatizzati» [78]. Proprio valorizzando tale riferimento e il suo collegamento con l'art. 8 CEDU, la Corte afferma che anche dati pubblici possono rientrare nella sfera privata del soggetto se sistematicamente acquisiti, memorizzati e utilizzati dalle pubbliche autorità, per cui è ravvisabile un'ingerenza laddove vi siano tre condizioni, consistenti nella memorizzazione dei dati, nel loro utilizzo da parte dell'autorità, nonché nella impossibilità di confutare tali informazioni da parte dell'interessato. Tale ingerenza viene ritenuta non giustificabile dalla Corte alla luce del carattere generalizzato, indistinto e sistematico con cui le autorità trattano i dati *de quibus*, nell'assoluta assenza di criteri oggettivi di selezione e individuazione delle informazioni e dei soggetti, nonché di procedure e di meccanismi di controllo di tali operazioni, tali da implicare concretamente «il rischio di minare, persino distruggere, la democrazia per difenderla», creando

[77] V. ZENO ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in *La protezione transnazionale dei dati personali. Dai "Safe Harbour principles" al "Privacy Shield"*, a cura di G. RESTA e V. ZENO-ZENCOVICH, p. 7-9. Cfr. Anche G. RESTA- F. SIMONETTI, *La c.d. sovranità digitale e il progetto Gaia-X*, in *Contr. e impr./Europa*, 2022, 3, p. 479 ss. A questo «ampliamento massimo» del «margine di protezione dei dati personali e della privacy degli individui» è attribuita una precisa finalità di «reazione» alle politiche statunitensi di *mass surveillance* da O. POLLICINO e BASSINI, *op. cit.*, p. 75-76.

[78] Cfr. anche la sentenza della Corte EDU 16 febbraio 2000, n. 27798/95, *Amann c. Svizzera*.

di fatto un sistema di sorveglianza su base indiscriminata e generalizzata, e svelando con ciò le stesse preoccupazioni e critiche mosse dalla Corte di Giustizia in *Digital Rights Irelands*, nonché andando più indietro nel tempo, dalla Corte costituzionale tedesca del 1983 (su cui *supra*).

D'altra parte, è dato ravvisare, proprio in concomitanza con la sopra richiamata giurisprudenza della Corte di Giustizia in tema, una vera e propria inversione di tendenza nell'atteggiamento della stessa corte EDU. Nel 2010, infatti, nel caso *Kennedy c. Regno Unito*, la Corte, pronunciandosi sulla compatibilità con l'art. 8 CEDU di alcuni sistemi di captazione delle informazioni su base generalizzata e sistemica implementati dal Regno Unito, aveva rigettato la questione in assenza di allegazione da parte del ricorrente di una violazione specifica, assumendo e mantenendo quella prospettiva di *individual justice* che da sempre l'aveva contraddistinta. Ma nel 2015, nel caso *Zakharov c. Russia* [79], tale interpretazione subisce una vera e propria battuta d'arresto, nella misura in cui viene riconosciuto, in accordo con le precedenti statuizioni in tema dei giudici di Lussemburgo, che la mancata allegazione di un pregiudizio o una conseguenza ricollegata al sistema di sorveglianza non costituisce un ostacolo per concludere sulla incompatibilità con l'art. 8 CEDU del sistema russo di captazione delle comunicazioni su base generalizzata e non ancorato a criteri oggettivi né a procedure di controllo specifiche.

Impostazione poi mantenuta nelle più recenti sentenze della Corte di Strasburgo in tema di sorveglianza di massa.

Ci si riferisce qui, anzitutto, alla sentenza del 5 marzo 2020, resa nel caso *ARM / Hambardzumyan* (ric. 43478/11), riguardante una denuncia della ricorrente di assenza di valido mandato giudiziario per sottoporla a sorveglianza segreta durante le indagini penali sulle accuse di corruzione, incluso l'utilizzo di apparecchiature di registrazione durante un incontro con il ricorrente, l'intercettazione di conversazioni telefoniche e la videoregistrazione della consegna del denaro della tangente, dato in banconote contrassegnate; in tale occasione la Corte ha criticato, in particolare, che il mandato fosse troppo vago, privo di dettagli circa l'oggetto della misura di sorveglianza, nonché l'insufficiente controllo giudiziario.

Anche di recente, con sentenza 8 marzo 2021, nel caso *MDA/Bostan (ric. 52507/09*), in relazione ad una perquisizione condotta dalla polizia presso l'abitazione del ricorrente nell'ambito di un procedimento per contravvenzione nei confronti di una terza persona, senza mandato o permesso giudiziario, contrariamente al diritto interno.

E ancora, può farsi richiamo alla celebre sentenza del 25 maggio 2021 resa nel caso *UK./Big Brother Watch and Others* (ric. 58170/13). La questione riguardava alcune carenze nel regime di sorveglianza segreta, tra cui l'intercettazione di massa e l'ottenimento di dati sulle comunicazioni da fornitori di servizi di comunicazione nel Regno Unito prima del 2018, sotto il profilo della violazione degli articoli 8 e 10

[79] Corte EDU, sentenza del 4 dicembre 2015, *Roman Zakharov c. Russia*, n. 47143/06.

CEDU. Pur ritenendo che la Convenzione non proibisca l'uso dell'intercettazione in massa di per sé per proteggere gli interessi di sicurezza nazionale e altri interessi nazionali essenziali contro gravi minacce esterne, la Corte ha sottolineato la necessità di "salvaguardie *end-to-end*" e ha definito l'approccio da seguire in tali casi. La Corte ha rilevato che, nonostante le sue salvaguardie, comprese alcune solide, il precedente quadro giuridico nel Regno Unito, la *Regulation of Investigatory Powers Act (RIPA)* 2000, in vigore fino al 2018, non conteneva sufficienti "end-to-end salvaguardie" per fornire adeguate ed efficaci garanzie contro l'arbitrarietà e il rischio di abusi. Successivamente, l'*Investigatory Powers Act* (IPA) ha sostituito il precedente quadro giuridico RIPA, introducendo un "doppio blocco" che richiede che i mandati per l'uso dei poteri investigativi siano autorizzati da un Segretario di Stato e approvati da un giudice dell'Ufficio del commissario per i poteri investigativi e garantendo un solido controllo indipendente sull'utilizzo di tali poteri.

Ancora, la Corte EDU nel caso *SWE/Centrum for Rättvisa* (ric. 35252/08), con sentenza del 25 maggio 2021, in relazione al presunto rischio che le comunicazioni della fondazione ricorrente venissero intercettate ed esaminate tramite segnali di intelligence, in quanto comunicava quotidianamente con individui, organizzazioni e società in Svezia e all'estero via e-mail, telefono e fax, spesso su questioni delicate, ha rilevato, in particolare, che il regime delle intercettazioni in blocco presentava tre carenze. In primo luogo, l'assenza di una norma chiara sulla distruzione del materiale intercettato che non conteneva dati personali; l'assenza di un requisito nel *Signals Intelligence Act* o in altra legislazione pertinente che, quando si decide di trasmettere materiale di intelligence a partner stranieri, si tenga conto degli interessi privati delle persone; e l'assenza di un effettivo riesame *ex post*. Di conseguenza, il sistema non soddisfaceva il requisito delle tutele "*end-to-end*", oltrepassava il margine di discrezionalità lasciato allo Stato convenuto al riguardo e, nel complesso, non metteva in guardia dal rischio di arbitrarietà e abusi [80].

Infine, una questione strettamente connessa con la sorveglianza è quella della *privacy genetica*, un tema a più riprese affrontato dalla Corte Edu. Sul punto, riveste un rilievo significativo la sentenza *Marper c. Regno* unito del 2008, richiamata anche dalla Corte di giustizia nella sopracitata sentenza *Digital Rights Ireland* [81], in tema di creazione di banche dati genetiche e del DNA a fini di giustizia. La Corte, in questo caso, afferma che la conservazione delle impronte digitali e dei campioni biologici di DNA, a prescindere dall'effettivo utilizzo degli stessi da parte delle autorità, rappresenta un'ingerenza nella vita privata dei soggetti, attesa la sicura qualificazione delle impronte e dei campioni di DNA alla stregua di dati sensibili nella nozione contenuta dalla Convenzione del 1981. Proprio in questa pronuncia è contenuta l'enunciazione chiara e forte da parte della Corte EDU che la protezione dei dati «è fondamentale per il

[80] Cfr. Report settembre 2022, *Personal data protection, Thematic factsheet, Department for the Execution of Judgments of the European Court*, consultabile al link https://www.coe.int/en/web/execution.
[81] Cfr. par. 47 della sentenza.

rispetto della vita privata» (par. 103). E proprio su queste premesse la Corte poi sottolinea come la giustificazione prevista dall'art. 8 comma 2 della CEDU debba essere ancorata, per porsi in termini di necessarietà della misura per una società democratica, a regole chiare, dettagliate, oltre che a garanzie minime, che nel caso concreto il Regno Unito non assicurava affatto, dal momento che non venivano previste regole minime e neppure criteri di cancellazione o distruzione dei dati genetici. La Corte, anzi, in uno dei passaggi più interessanti della sentenza [82] si dice addirittura «sorpresa» dal carattere generale e indifferenziato con cui in Inghilterra opera il meccanismo di conservazione di tali dati, laddove invece uno Stato che intendesse porsi in un'ottica pionieristica dal punto di vista dell'evoluzione tecnologica nel campo, dovrebbe prendersi anche in carico la responsabilità di compiere dei bilanciamenti [83], che nel caso concreto non sono stati compiuti affatto, con tutti i conseguenti rischi, anche in termini di stigmatizzazione sociale riconnessi al trattamento dei dati per i soggetti, tra l'altro minori all'epoca dei fatti [84].

In tema di conservazione di materiale genetico, la Corte si è pronunciata anche più di recente con la sentenza del 13 giugno 2020 nel caso *UK. vs Gaubran* (ric. 45245/15), in un caso riguardante la conservazione a tempo indeterminato dei dati personali del ricorrente (profilo del DNA, impronte digitali e fotografia) acquisiti in relazione a una condanna scontata in Irlanda del Nord per un reato di guida in stato di ebbrezza, in cui la Corte europea ha ritenuto che il carattere indiscriminato dei poteri di conservazione, unito all'assenza di garanzie sufficienti, eccedesse il margine di discrezionalità accettabile dello Stato al riguardo. Ancora, medesime censure la Corte ha mosso con sentenza del 14 agosto 2020 nel caso *SER vs. Dragan Petrovic* (ric. 75229/10)*, in relazione* al prelievo di un campione di DNA, avvenuto nel contesto di una perquisizione durante un'indagine per omicidio.

5. I rischi per i diritti e le libertà della persona nell'ottica di tutela della vita privata connessi al trattamento di categorie di dati particolari. I dati genetici

Come si ha avuto modo di sottolineare in chiusura del paragrafo precedente, conducendo l'analisi la giurisprudenza di Strasburgo sul punto, la questione della sorveglianza è spesso collegata al trattamento di categorie particolari di dati.

[82] Par. 119 della sentenza.
[83] Par. 112 della sentenza.
[84] Il fattore tempo risulta rilevante anche nella giurisprudenza di Strasburgo, come pure aveva assunto rilevanza nelle pronunce della Corte di giustizia *Digital Rights Ireland*, su cui *supra*, con riferimento alla conservazione dei dati prevista dalla dir. 24 del 2006 e *Google Spain* con riferimento invece all'attualità della notizia di cui si chiedeva la deindicizzazione. In particolare, la Corte di Strasburgo ha adottato un orientamento maggiormente restrittivo rispetto al trattamento di dati risalenti anche nel caso *Haralambire c. Romania* del 27 ottobre 2009, in cui ha constatato il diritto dei singoli all'accesso ai dossier formati dei servizi segreti all'epoca della dominazione sovietica, al fine di contestarli e rettificarne il contenuto. Allo stesso modo Corte EDU *Turek c. Slovacchia*, 16 febbraio 2006.

Infatti, nel quadro del processo di *datification* [85] — in cui tutto diviene riconducibile a informazione [86] — e della società sempre più governata dalla dittatura dell'algoritmo [87], l'obiettivo principale di indagine da parte dei detentori di dati non sono più i singoli, bensì i comportamenti collettivi di «gruppi a geometria variabile, plasmati e rimodellati in continuo degli algoritmi» [88]. Con ciò, viene sostanzialmente a prevalere una dimensione collettiva del dato, da tutelare non meno di quella individuale

In tale contesto, una categoria particolarmente delicata di dati è costituita dai dati genetici, che presenta profili di problematicità, a più riprese sottolineati e rimarcati dal Garante per la protezione dei dati personali [89] in relazione ai *test* genetici [90].

I dati genetici, siccome connotati da ricca e univoca capacità informativa nonché caratterizzati da un valore costitutivo della sfera privata ben più forte di ogni altra categoria di informazioni personali [91], sono «i più sensibili e, quindi, debbano essere tutelati più di ogni altro» [92], dal momento che si atteggiano quali dati affatto peculiari sotto diversi profili. Ciò che viene qui in rilievo è la dimensione informazionale dei dati genetici, in cui il rapporto con i dati genetici, precipua espressione della personalità e dell'identità dell'individuo, risulta connotato da una corrispondenza, di tipo univoco, tra i medesimi ed il titolare del campione genetico trattato, cui esso appartiene [93].

In primo luogo, i dati genetici si caratterizzano per una particolare stabilità, data dalla loro immodificabilità ed inalterabilità in tutto l'arco della vita di un individuo, finanche immortalità [94],

---

[85] Di *datification*, datasfera e datacrazia parla R. D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio e V. Ricciuto, Torino, 2019, p. 65.

[86] A. MANTELERO, *op. cit*., p. 144, che richiama sul punto L. FLORIDI, *The 4th revolution: how the infosphere si reshaping human reality*, Oxford, 2014, p. 96.

[87] S. RODOTÀ, *Il mondo nella rete*, cit., p. 37 ss.

[88] «Occorre prendere atto che l'obiettivo principale di indagine da parte dei detentori di dati non sono più singoli, bensì i comportamenti collettivi di "gruppi a geometria variabile, plasmati e rimodellati in continuo degli algoritmi". Cfr. A. MANTELERO, *op. cit*., p. 144 e ss.

[89] Cfr. già *Relazione annuale per il 2002 del Garante per la protezione dei dati personali, intitolata: Nuovi diritti, riservatezza, dignità della persona: a sei anni dalla l. 675*, accessibile in www.garanteprivacy.it. I rischi di discriminazione sociale insiti nell'uso senza regole dei test genetici erano già stati portati all'attenzione del Garante all'inizio del nuovo millennio, tanto da costituire oggetto di un convegno sul tema «i nostri dati genetici» a Roma il 21 luglio 2000 dal Garante, dal Comitato nazionale per la bioetica e Legambiente.

[90] In tema, F. DAGNA BRICARELLI, *I test genetici*, in *Trattato di biodiritto* diretto da S. RODOTÀ e P. ZATTI, *Il governo del corpo*, a cura di S. CANESTRARI, G. FERRANDO, MAZZONI, S. RODOTÀ, P. ZATTI, I, Milano, 2011, 371 ss.; C. CASONATO, C. PICIOCCHI, P. VERONESI (a cura di), *Forum BioDiritto 2009. I dati genetici nel biodiritto*, Padova, 2011.

[91] Sulla attitudine dei dati genetici a condizionare potenzialmente momenti importanti della vita privata e familiare dell'individuo, si veda G. FERRANDO, *Profili giuridici dei test genetici e decisioni riproduttive*, relazione alla Conferenza internazionale di Roma (21-22 marzo 2002) su *Implicazioni giuridiche e psicosociali della genetica umana*, nonché S. RODOTÀ, *La vita e le regole*, Milano, 2006, in part. 164 ss.

[92] S. RODOTÀ, *Se la società impone la schedatura genetica*, su *La Repubblica* del 13 gennaio 2005.

[93] In tema, sotto lo specifico profilo del governo del corpo, si veda P. ZATTI, *Il corpo e la nebulosa dell'appartenenza*, in *Nuova giur. civ. comm*., 2007, II, 1 ss.; ID., *Di là dal velo della persona fisica. Realtà del corpo e diritti "dell'uomo"*, in *Liber Amicorum per Francesco D.Busnelli, Il diritto civile tra principi e regole*, II, Milano, 2008, 121 ss.

[94] Si segnala, più in generale, che il tema della tutela post-mortale dei dati e il regime dei dati personali nella fase successiva alla morte del soggetto costituisce uno degli argomenti oggi maggiormente dibattuti, soprattutto nel quadro del diritto

sopravvivendo addirittura allo stesso, a differenza delle altre informazioni e degli altri caratteri biologici, che, appartenendo sostanzialmente alla linea somatica della persona, sono destinati a morire con essa. Tale caratteristica deriva dalla loro attitudine informativa riferibile non solo al soggetto interessato, ma a tutti gli appartenenti allo stesso gruppo biologico, per cui i dati genetici rappresentano il tramite biologico tra le generazioni, collocando il soggetto, nella sua unicità, in una relazione inequivoca con altri soggetti, con cui sussistono legami parentali di ascendenza e di discendenza, evidenziando la linea di continuità delle generazioni e delle stesse etnie [95].

Da ultimo, ai dati genetici sono ricollegabili peculiari attitudini predittive, come pure ha avuto modo di sottolineare la Corte di Cassazione [96], intese a definire l'evoluzione della vita della persona, la diagnosi ed anche previsione di malattie destinate a manifestarsi in futuro, suscettibili di incidere sulla costruzione della personalità individuale ed indurre determinate strategie di comportamento, sia dell'interessato, che di terzi, specialmente nell'ambito di attività connotate da carattere economico.

Il Regolamento UE del 2016 in tema di protezione dai dati personali all'art. 4, par. 1 definisce i «dati genetici» come «i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica», ricomprendendo sostanzialmente i dati biologici e i campioni biologici, a mente del *considerando* 35, tra i «dati relativi alla salute», intesi come «i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute» [97], in linea peraltro con la disciplina europea che introduce norme per la protezione dei dati raccolti per lo svolgimento di attività comprendenti l'impiego di tessuti e cellule umane [98].

Il regolamento per questi dati (così come per i dati biometrici, che pure consentono o confermano l'identificazione univoca dell'individuo) crea una sotto-categoria all'interno della più ampia categoria dei dati particolari disciplinati dall'art. 9, per i quali la liceità del trattamento è ancorata al requisito alternativo

dell'economia digitale. Cfr. G. RESTA, *La successione nei rapporti digitali e la tutela post-mortale dei dati personali*, in *Contr. e impr.*, 2019, I, 85 ss.

[95] Sui dati genetici quali informazioni che non riguardano solo l'individuo, ma anche ascendenti e discendenti, in quanto informazioni personali che ciascuno di noi condivide strutturalmente con altri, nonché sul loro utilizzo nella medicina predittiva S. RODOTÀ, *Tra diritto e società. Informazioni genetiche e tecniche di tutela*, in *Riv. crit. dir. priv.*, 2000, p. 584.

[96] Cfr. Cass. 13 settembre 2013, n. 21014.

[97] La riconducibilità delle informazioni tratte dal DNA dell'individuo alla categoria dei dati personali, nel rispetto dei principi di finalità, proporzionalità, pertinenza e non eccedenza, era stata peraltro già dichiarata dal Gruppo di lavoro per la protezione dei dati- Art. 29 in occasione del parere 6/2000 sul problema del Genoma, approvato il 13 luglio 2000 (5062/00/IT/Definitivo - WP 34), nella parte in cui veniva sottolineata «l'importanza della riservatezza in quanto diritto fondamentale, e la conseguente necessità di applicare le nuove tecnologie genetiche con salvaguardie adeguate alla protezione di tale diritto.

[98] Dir. 2004/23/CE, sulla definizione di norme di qualità e di sicurezza per la donazione, l'approvvigionamento, il controllo, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di tessuti e cellule umani.

del consenso esplicito oppure della necessità, consentendo agli Stati membri di introdurre garanzie supplementari (art. 9, par. 4). Il consenso è quindi alternativo ad altre condizioni – indicate dallo stesso art. 9 reg. UE 2016/679, tra cui l'ipotesi in cui il trattamento sia necessario per motivi di interesse pubblico o per ragioni correlate alla sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi; ovvero il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; o ancora sia necessario in relazione all'esercizio del diritto di difesa o per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro, della sicurezza sociale e protezione sociale [99].

Nel quadro degli obblighi generali incombenti sul titolare del trattamento *ex* art. 24, e delle misure di sicurezza adottabili *ex* art. 32 del GDPR — letti in un'ottica di responsabilizzazione (o *accountability*) dello stesso — il livello di misure dovrà essere in questo caso molto elevato, trattandosi di trattamento che riguarda dati personali «particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali»[100].

Posto che nell'odierna società dell'informazione basata sui *Big Data* emerge una sostanziale difficoltà nell'individuare l'*an*, il *quando* e il *quomodo* (inteso in termini di finalità) dei singoli concreti trattamenti cui i dati vengono sottoposti, Il legislatore europeo della *privacy* mostra ampia consapevolezza delle proporzioni massive che il fenomeno circolatorio dei dati è venuto assumendo negli ultimi decenni, avendo ben presente che «la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo», e ha reso «disponibili al pubblico su scala mondiale informazioni personali» (*considerando* 6 GDPR), che consentono di effettuare «trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato (…) per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti». (*considerando* 91 GDPR), con particolare riferimento al monitoraggio del comportamento dell'interessato attraverso tecniche di trattamento che ne consentano l'analisi, anche in termini predittivi, sotto il profilo delle preferenze, usi comportamentali o posizioni personali (*considerando* 24 e 71 GDPR).

[99] In ambito nazionale, l'art. 2 *septies* del d. lgs. 10 agosto 2018, n. 101 attua l'art. 9, par. 4 del regolamento, prevedendo che il trattamento dei dati biometrici, genetici e relativi alla salute sia subordinato all'osservanza di misure di garanzia, stabilite dal Garante con provvedimento adottato con cadenza almeno biennale.
[100] Cfr. *considerando* 51 reg. UE 2016/679.

In tale contesto, assumono centrale rilevanza e maggiore complessità, in particolare, i profili di tutela dei diritti e delle libertà degli interessati sotto il profilo del trattamento di dati su larga scala di categorie di dati personali, tra cui i dati genetici. Ad essi si riferisce la previsione che rende obbligatoria la valutazione d'impatto[101] sulla protezione dei dati contenuta nella lett. *b)* dell'art. 35 del GDPR, ulteriormente specificata dal provvedimento adottato dal Garante per la protezione dei dati nell'ottobre 2018 [102]. In particolare, per i profili che qui rilevano, le categorie più problematiche di trattamento previste dal provvedimento del Garante, oggetto peraltro di puntuali osservazioni da parte dell'*European Data Protection Board*, erano proprio quelle relative al trattamento effettuato attraverso l'uso di tecnologie innovative, al trattamento dei dati biometrici nonché dei dati genetici, in relazione ai quali nella versione originaria dell'elenco il Garante italiano aveva mostrato di considerare suscettibili *ex se* di presentare rischi elevati per i diritti e le libertà degli interessati, in considerazione della tipologia di trattamento nel primo caso e della peculiarità dei dati oggetto di trattamento negli altri due, mostrando una certa sensibilità e preoccupazione rispetto al tema del trattamento dei dati genetici. In altre parole, nell'ottica di tutela abbracciata dal GDPR si adotta una logica preventiva, che demandi la gestione dei rischi potenzialmente sussistenti per i diritti degli interessati a monte in capo al titolare del trattamento, in ossequio al principio di precauzione[103].

In questa sede, con particolare riferimento alla questione della sorveglianza che qui ci occupa, preme sottolineare alcuni profili di criticità ulteriori.

In primo luogo, i dati genetici sono suscettibili di essere combinati con alcuni tipi di *Big Data*, come i dati fenotipici, quali stile di vita, abitudini, contatti personali, carta di credito o dati sanitari in senso ampio o altri dati relativi a circostanze di spazio/tempo, ovvero, più in generale, attinenti lo stato socio-

[101] Sulla valutazione di impatto si veda TORINO, *La valutazione d'impatto*, in *I dati personali nel diritto europeo*, a cura di V. CUFFARO, R. D'ORAZIO E V. RICCIUTO, Torino, 2019, 855 ss.

[102] Cfr. Garante della protezione dei dati personali, doc. *web* n. 9058979 dell'11 ottobre 2018, contenente l'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del reg UE n. 2016/679, pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018. Si vedano anche le osservazioni rese in proposito: *European Data Protection Board, Opinion 12/2018 on the draft list of the competent supervisory authority of Italy regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)*, adottata il 25 settembre 2018 e notificato il 2 ottobre 2018, disponibile al sito *web https://edpb.europa.eu/*.

[103] Il principio di precauzione, espressamente previsto con riferimento alla materia ambientale dal Trattato sul funzionamento dell'Unione Europea all'art. 191, ha assunto portata generale a partire dalla comunicazione della commissione COM (2000), 1, del 2 febbraio 2000 sul principio di precauzione, in cui la Commissione Europea ha dichiarato applicabile detto principio «a qualunque misura di gestione dei rischi». Cfr. sul punto, F.D. BUSNELLI, *Il principio di precauzione e l'impiego di biotecnologie in agricoltura*, in *Regole dell'agricoltura e regole del cibo*, a cura di GOLDONI e SIRSI, Pisa, 2005, 115 ss.; ARBOUR, *A proposito della nebulosa. Principio di precauzione – responsabilità civile*, in *Liber amicorum per FRANCESCO D. BUSNELLI, Il diritto civile tra principi e regole*, Milano 2008, I, 13; nonché R. PARDOLESI, *Il principio di precauzione a confronto con lo strumento dell'analisi economica del diritto*, in *Gli strumenti della precauzione: nuovi rischi, assicurazione e responsabilità*, a cura di Comandè, Milano, 2006, 13.

economico. Da tale incrocio è possibile derivare profili precisissimi degli individui, e per di più ad alto potenziale predittivo.

In tale prospettiva, pur mantenendo i dati anonimi [104] facendo ricorso a tecniche di anonimizzazione [105] e di criptazione (come previsto pure dal sopracitato provvedimento del Garante), suscitano perplessità, nell'ottica di sussistenza di un rischio elevato per i diritti e delle libertà delle persone fisiche, i casi di *screening* genetici di massa, effettuati per ragioni di ricerca, per i potenziali effetti di discriminazione di un'intera comunità che dovesse evidenziare una predisposizione per talune particolari patologie [106].

Per questa via, la mappatura genomica e la decodificazione del codice genetico umano sarebbero infatti suscettibile di configurare una delle tappe verso la società della sorveglianza; proprio quella degenerazione della società dell'eguaglianza e della partecipazione guardata con sospetto e preoccupazione a più riprese dalla giurisprudenza della Corte di Strasburgo e di Lussemburgo.

In secondo luogo, una criticità è ricollegata alla questione del tempo di conservazione di tali dati, che costituisce un nodo problematico centrale nel bilanciamento degli interessi in gioco e che in linea di principio deve essere proporzionato alle finalità di raccolta degli stessi. Sul punto, non può non farsi un riferimento storico alla Convenzione n. 108 del 1981, che conteneva previsioni specifiche, in ottica di limitazione della conservazione dei dati a tutela dei diritti e delle libertà dell'interessato, volte a contenerne la durata ad un tempo non superiore a quello necessario per il conseguimento delle finalità del trattamento, rivelando ancora una volta come il principio di conservazione dei dati personali sia sottoposto a limiti che dipendono strettamente dalle finalità per cui essi sono stati raccolti e trattati, per cui il principio di conservazione dei dati è avvinto da uno stretto nesso strutturale con la finalità del trattamento, in relazione al quale va valutato in termini di proporzionalità [107]. Anche sotto il profilo informativo, l'art. 13 GDPR prevede, in tema di informazioni da fornire qualora i dati personali siano raccolti presso l'interessato, che il titolare del trattamento fornisca all'interessato specifiche informazioni relative al «periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo», esplicitamente qualificate siccome necessarie per garantire un trattamento corretto e trasparente.

---

[104] Si tenga presente però che anonimizzazione e pseudonomizzazione scontano non solo un elevato costo di messa in opera, ma soprattutto rischiano di far venir meno l'interesse stesso della ricerca a causa del minor valore dell'informazione risultante dal processo stesso, rischiando di vanificarne parzialmente l'utilità, specialmente negli studi longitudinali ed epidemiologici. Cfr. BERNES, *La protezione dei dati personali nell'attività di ricerca scientifica*, in *Le nuove leggi civili commentate*, 2020, I, 175 ss.

[105] Cfr G. D'ACQUISTO e M. NALDI, *Big Data e privacy by design,* Torino, 2017, 37.

(106) Cfr. A. SANTUOSSO e I. A. COLUSSI, *Diritto e genetica delle popolazioni*, in *Il governo del corpo*, I, *Trattato di biodiritto* diretto da S. RODOTÀ e P. ZATTI, cit., p. 357 ss.

[107] Sul punto, cfr. anche Art. 29 WP, *Opinion* 1/2014 *on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, 536/14/EN, WP 211, 27 febbraio 2014.

Da tutto quanto precede, emerge con evidenza come il trattamento dei dati genetici, sia in massimo grado suscettibile di comportare un elevato rischio per i diritti e le libertà degli individui [108], atteso anche che la genetica porta a conseguenze radicali la tendenza di «far nascere libertà e scelta dove prima era soggezione e immodificabili leggi di natura». [109]

Appare però opportuno qui sottolineare quali sfumature assuma la questione laddove il trattamento — anche massivo, sistematico e su larga scala — di queste categorie particolari di dati avvenga per finalità connesse alla salute, nel quadro di un bilanciamento operato con i diritti ricollegabili all'art. 32 Cost.

6. Segue. Il delicato equilibrio nel bilanciamento con esigenze connesse alla salute

Il *Considerando* 53 del GDPR chiarisce che «le categorie particolari di dati personali che meritano una maggiore protezione dovrebbero essere trattate soltanto per finalità connesse alla salute, ove necessario per conseguire tali finalità a beneficio delle persone e dell'intera società, in particolare nel contesto della gestione dei servizi e sistemi di assistenza sanitaria o sociale, (…) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in base al diritto dell'Unione o nazionale che deve perseguire un obiettivo di interesse pubblico, nonché per studi svolti nel pubblico interesse nell'ambito della sanità pubblica».

Ed è proprio sulla base della necessarietà per motivi di interesse pubblico nel settore della sanità pubblica – di cui alle lettere g) e i) dell'art. 9 GDPR, che poggia il DL 10 maggio n. 30, convertito con modifiche in Legge 2 luglio 2020, n. 72, recante «Misure urgenti in materia di studi epidemiologici e statistiche sul SARS-COV-2 (COVID-19)» [110], che ha autorizzato il trattamento dei dati personali, anche genetici e relativi alla salute, per fini statistici e di studi scientifici svolti nell'interesse pubblico nel settore della sanità pubblica.

---

[108] Cfr. S. RODOTÀ, *Tra diritto e società. Informazioni genetiche e tecniche di tutela*, cit., 571 - 604. Nel diritto statunitense, si veda legge federale *Genetic Nondiscrimination Information Act* (GINA), che vieta la discriminazione genetica nei settori assicurativo e del lavoro, a far data, rispettivamente, dal 21 maggio e dal 1° novembre 2009. Sull'influenza dell'informazione genetica nel ragionamento giuridico nei tribunali statunitensi e sull'incidenza dell'influenza genetica, quale informazione predittiva, sulla discriminazione di determinate categorie di persone, NELKIN, *Informazione genetica: bioetica e legge*, cit., p. 491.

[109] S. RODOTÀ, *La vita e le regole*, cit., p. 165.

[110] Motivato dalla «necessità di disporre con urgenza di studi epidemiologici e statistiche affidabili e complete sullo stato immunitario della popolazione, indispensabili per garantire la protezione dall'emergenza sanitaria in atto», il decreto legge 10 maggio 2020 n. 30, convertito, con modificazioni, dalla legge 2 luglio 2020, n. 72, recante «Misure urgenti in materia di studi epidemiologici e statistiche sul SARS-COV-2 (COVID-19)», ha infatti «autorizzato il trattamento dei dati personali, anche genetici e relativi alla salute, per fini statistici e di studi scientifici svolti nell'interesse pubblico nel settore della sanità pubblica, nell'ambito di un'indagine di sieroprevalenza condotta congiuntamente dai competenti uffici del Ministero della salute e dall'Istituto nazionale di statistica (ISTAT), in qualità di titolari del trattamento e ognuno per i profili di propria competenza». Il legislatore ha in particolare disposto che «Il trattamento dei campioni e dei relativi dati è effettuato per esclusive finalità di ricerca scientifica sul SARS-COV-2 individuate dal protocollo di cui al comma 1, nel rispetto delle prescrizioni del Garante per la protezione dei dati personali individuate nel provvedimento del 5 giugno 2019».

Del resto, come non ha mancato di sottolineare anche di recente il Garante per la protezione dei dati personali [111], la pandemia ha mostrato «quanto stretto sia il legame tra salute, privacy e digitale», dimostrando altresì «quanto sia determinante per la democrazia l'equilibrio tra esigenze di sanità pubblica e la limitazione dei diritti individuali», atteso che i dati sanitari, così come i dati genetici, esprimono l'essenza della privatezza del corpo, delle sue patologie in atto e potenziali delle sue vulnerabilità e carenze e pertanto sono suscettibili di esporre i singoli a discriminazioni e classificazioni. Ecco perché, nell'ottica dell'Autorità garante, «sulla sinergia tra salute, innovazione e privacy si gioca una sfida determinante nel segno della centralità della persona».

Deve qui sottolinearsi come i dati sanitari sono attualmente oggetto di grande attenzione da parte del legislatore europeo, e al centro di una imminente e poderosa riorganizzazione normativa attraverso la Proposta di Regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari, intesa a creare uno spazio europeo dei dati sanitari (*European Health Data Space, EHDS*) [112], nel quadro della strategia europea, in cui è stata proposta l'istituzione di spazi comuni europei di dati specifici per dominio. Destinato ad affrontare sfide specifiche all'ambito sanitario relative all'accesso ai dati sanitari elettronici e alla loro condivisione, esso «costituisce una delle priorità della Commissione europea nel settore della sanità e sarà parte integrante della costruzione di un'Unione europea della salute. Nell'ottica del legislatore europeo, lo spazio europeo dei dati sanitari creerà uno spazio comune in cui le persone fisiche possano facilmente controllare i propri dati sanitari elettronici. Consentirà inoltre a ricercatori, innovatori e responsabili delle politiche di utilizzare tali dati sanitari elettronici in un modo affidabile e sicuro che tuteli la privacy» [113]. Alla luce della constatazione che la pandemia da Sars-CoV2 ha messo in luce ancora di più l'importanza dei dati sanitari elettronici per lo sviluppo di una strategia in risposta alle emergenze sanitarie, il legislatore europeo mira così a garantire alle persone fisiche nell'UE un maggiore controllo sui propri dati sanitari elettronici, nonché a creare un quadro giuridico fondato su meccanismi di governance dell'UE e degli Stati membri affidabili e su un ambiente di trattamento sicuro, consentendo con ciò a ricercatori, sanitari e responsabili delle politiche e regolatori, di accedere a dati sanitari elettronici pertinenti per favorire il miglioramento della diagnosi, delle cure e del benessere delle persone fisiche. D'altra parte, un siffatto quadro giuridico contribuirebbe alla creazione di un autentico mercato unico per i prodotti e i servizi di sanità digitale tramite l'armonizzazione delle norme, con un incremento in termini di efficienza dei sistemi di assistenza sanitaria. Lo spazio europeo dei dati sanitari, infatti, dovrebbe

[111] Intervista al Presidente del Garante per la protezione dei dati personali Pasquale Stanzione dell'8 ottobre 2020 sul ruolo dei dati e privacy nella sanità, rinvenibile sul sito istituzionale dell'Autorità garante.
[112] Proposta di Regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari COM(2022) 197 final del 3 maggio 2022) , intesa a creare uno spazio europeo dei dati sanitari (*European Health Data Space, EHDS*)].
[113] Cfr. relazione alla proposta, p. 1.

contribuire a migliorare l'accesso a diversi tipi di dati sanitari elettronici, tra cui cartelle cliniche elettroniche, dati genomici, registri di pazienti etc., e il loro scambio.

Si propone, quindi, un modello di gestione e condivisione di tali dati, improntato ad accessibilità, controllo e portabilità, sia nell'ambito dell'erogazione dei servizi di cura e assistenza ai cittadini (uso primario dei dati)**,** sia nell'ambito delle attività di ricerca e sviluppo e di definizione delle politiche sanitarie, per stimolare innovazione e consentire alle imprese di competere sui mercati globali (uso secondario dei dati), stabilendo meccanismi predeterminati per l'altruismo dei dati in ambito sanitario. Proprio sull'uso secondario si sono appuntate alcune critiche, mosse dall' *European Data Protection Board* (EDPB) e *European Data Protection Supervisor* (EDPS) in un parere congiunto sulla bozza di regolamento [114], in relazione al fatto che l'articolo 2.2 lettera d) della proposta di regolamento definisce l'uso secondario dei dati specificando che «tra i dati utilizzati possono figurare dati sanitari elettronici personali originariamente raccolti nel contesto dell'uso primario, ma anche dati sanitari elettronici raccolti ai fini dell'uso secondario». Nonostante il Regolamento del 2016 non contenga una definizione di uso secondario, esso si riferisce al «trattamento ulteriore» all'art. 5.1, lettera b), pertanto i Garanti suggeriscono di chiarire il collegamento tra le due definizioni, soprattutto tenendo conto del fatto che il Regolamento introduce un regime specifico in relazione al trattamento ulteriore.

D'altra parte, preso atto che, in linea con il *Considerando* 37 della proposta, il «(…) regolamento fornisce la base giuridica ai sensi dell'articolo 9, paragrafo 2, lettere g), h) e j), del regolamento (UE) 2016/679 per l'uso secondario dei dati sanitari, stabilendo le garanzie per il trattamento, in termini di finalità lecite, di una governance fidata per fornire l'accesso ai dati sanitari (attraverso organismi di accesso ai dati sanitari) ed il trattamento in un ambiente sicuro, nonché le modalità di trattamento dei dati», le Autorità rilevano che l'art. 34, par. 1 della proposta fornisce un elenco di finalità per le quali i dati sanitari elettronici possono essere trattati per uso secondario, che comprendono — ma non esclusivamente — lo scopo della ricerca scientifica relativa ai settori della salute o dell'assistenza, rilevando perciò l'assenza di un'adeguata delimitazione delle finalità elencate nella norma predetta.

Nella stessa ottica garantista si colloca, in relazione ai dati sanitari, a livello nazionale, anche il Garante per la protezione dei dati personali. Recentemente infatti, nell'agosto 2022, ha fornito parere negativo sullo schema di decreto da adottare assieme al Ministro delegato per l'innovazione tecnologica e la transizione digitale, di concerto con il Ministro dell'economia e delle finanze, sull'Ecosistema Dati Sanitari (EDS) [115]. L'Autorità condivide, in generale, la necessità di introdurre strumenti volti ad agevolare lo

[114] *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*, reso il 12 luglio 2022.

[115] Parere al Ministero della Salute sullo schema di decreto da adottare assieme al Ministro delegato per l'innovazione tecnologica e la transizione digitale, di concerto con il Ministro dell'economia e delle finanze, sull'Ecosistema Dati Sanitari (EDS) - 22 agosto 2022 [9802752].

sviluppo di servizi sanitari digitali offerti ai cittadini, ma evidenzia come sia doveroso che, nella loro realizzazione, vengano rispettati i diritti fondamentali delle persone, non ravvisando una piena tutela, giudicati non sono risultati coerenti con la normativa di settore. In particolare, segnala il Garante, l'Ecosistema Dati sanitari (EDS), previsto dalla riforma del FSE con l'obiettivo di garantire il coordinamento informatico e assicurare servizi omogenei sul territorio nazionale, «comporta di fatto la duplicazione di dati e documenti sanitari già presenti nel FSE e determina la costituzione della più grande banca dati sulla salute del nostro Paese». Un tale database raccoglierebbe, a livello centralizzato, senza alcuna garanzia di anonimato per gli assistiti, dati e documenti sanitari relativi a tutte le prestazioni sanitarie erogate sul territorio nazionale. Inoltre, per come è attualmente previsto dallo schema di decreto, l'EDS si presenta, secondo il Garante, come "una scatola vuota", rinviando a successivi decreti la definizione di aspetti essenziali per la sua regolazione. Considerata la delicatezza di tale trattamento, che realizza un trattamento sistematico su larga scala anche attraverso l'uso di algoritmi, il Garante ha quindi chiesto al Ministero di riformulare lo schema di decreto, indicando i contenuti e le specifiche modalità di alimentazione della banca dati, nonché i diritti riconosciuti alle persone.

7. I dati biometrici quali oggetto di trattamenti suscettibili di definire nuovi modelli di sorveglianza

Su altro versante, l'atteggiamento del Garante appare poi particolarmente restrittivo nel ritenere necessaria una valutazione di insieme per evitare che «singole iniziative aventi ad oggetto il trattamento di dati particolari come quelli biometrici, sommate fra loro, definendo un nuovo modello di sorveglianza, introducano di fatto un cambiamento non reversibile nel rapporto tra individuo ed autorità».

Con particolare riferimento al sistema *Sari real time* [116], progettato e sviluppato come soluzione mobile tale da poter essere installata direttamente presso il sito dove sorge l'esigenza di disporre di una tecnologia di riconoscimento facciale in grado di coadiuvare le forze di polizia nella gestione dell'ordine e della sicurezza pubblica, oppure in relazione a specifiche esigenze di polizia giudiziaria, il Garante, con provvedimento del 25 marzo 2021, ha reso un parere negativo, dimostrando anzi una spiccata preoccupazione in ordine all'«evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui».

In particolare, richiamando gli articoli 8 CEDU, nonché 7, 8 e 52 CDFUE, l'Autorità ha ritenuto allo stato non sussistente una base giuridica idonea a consentire il trattamento dei dati biometrici nel caso concreto, fondato su un algoritmo di riconoscimento facciale che consente di analizzare in tempo reale i

[116] Provvedimento del Garante n. 127 del 25 marzo 2021, doc. web numero 9575877.

volti dei soggetti ripresi confrontandole con una banca dati predefinita per lo specifico servizio denominata "*watch-list*" [117].

Più in generale, con specifico riferimento ai dati biometrici, già oggetto di particolare attenzione del Garante per la protezione dei dati personali vigente la normativa precedente [118], occorre qui sottolineare come siano necessarie misure di garanzia specifiche. *Medio tempore*, l'art. 22 co. 11 del D.lgs. 101/2018 sembra suggerire la possibilità di continuare ad utilizzare i dati biometrici in conformità alle Linee guida sulla biometria adottate nel 2014, adattando la base giuridica a quella indicata dal Regolamento [119].

Ancora più di recente, l'Autorità garante ha adottato un interessante provvedimento in tema di trattamento dati biometrici [120], con cui ha comminato una sanzione particolarmente elevata a *Clearview AI Inc.*, in ragione dell'assenza di una base giuridica del trattamento di immagini, avvenuto senza il consenso e il mancato riscontro alle richieste degli interessati, specificatamente sull'accesso ai dati [121]. Alla prima richiesta di informazioni dell'Autorità la società rispondeva di non effettuare il monitoraggio degli interessati all'interno dell'Unione secondo quanto stabilito dall'articolo 3, par. 2, lett. b) del Regolamento, in quanto lo stesso presuppone un'osservazione che sia continua e perdurante nel tempo, mentre il servizio in questione non offre la possibilità di monitorare e tracciare le persone nel tempo, ma offre esclusivamente la funzionalità di ricerca delle immagini, come un semplice motore di ricerca, offrendo un'istantanea dei risultati. D'altra parte, Clearview sostiene come anche la valutazione della base giuridica che legittimi il trattamento rientri nella responsabilità del cliente che ha sottoscritto l'account e non della Società, dal momento che il potere decisionale circa i risultati delle ricerche svolte attraverso la piattaforma spetta al cliente stesso.

---

[117] Cfr. anche provvedimento n. 54 del 26 febbraio 2020, reperibile sul sito istituzionale dell'autorità, doc. web numero 9309458.

[118] Garante, provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014 e relativo allegato A recante *Linee guida in materia di riconoscimento biometrico e firma grafometrica*.

[119] L'articolo sopra richiamato, infatti, prevede espressamente che per il trattamento dei dati biometrici e genetici, le norme esistenti continuano a trovare applicazione in quanto compatibili, sino all'adozione delle misure di garanzia da parte del Garante. Si tenga altresì presente che, più in generale sul punto, sebbene non si riscontrino indicazioni in tal senso all'interno del Regolamento, l'Autorità italiana ha escluso esplicitamente che i dati biometrici possano essere trattati sulla base del legittimo interesse del titolare. Cfr. Provvedimento 22 febbraio 2018, recante *Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento (UE) 2016/679*.

[120] Garante per la protezione dei dati personali, *Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022*, doc. web 9751362.

[121] Come si legge nel par. 3 del provvedimento, le caratteristiche del servizio sono le seguenti: Clearview costituisce una piattaforma che fornisce un servizio di ricerca di immagini all'interno di un database offerto dalla Società stessa. Le immagini contenute nel database vengono raccolte da fonti pubbliche attraverso tecniche di *web scraping*, ovvero una tecnica di estrazione dei dati da siti web, successivamente elaborate, estraendo le caratteristiche identificative del volto, trasformate in rappresentazioni vettoriali costituite da 512 vettori e sottoposte poi ad *hashing*, in modo da consentire l'indicizzazione nel database a fini di ricerca. I modelli biometrici creati verranno poi comparati con l'immagine oggetto di ricerca, secondo una comparazione *one-to-many*; inoltre le foto possono essere associate a metadati, ovvero informazioni, e non vengono cancellate anche se sono state rimosse dalla fonte originaria o se è stato limitato l'accesso; di modo che esse non vengono modificate, né aggiornate, risultando al contrario come presenti e istantanee del momento in cui viene svolta la ricerca.

Ponendosi l'attività predetta quale «mera raccolta di dati», le conclusioni che vengono tratte dalla ricerca sarebbero quindi, nell'ottica della convenuta, il risultato dell'operato delle forze dell'ordine che, grazie ai risultati forniti dal servizio, conducono ulteriori indagini investigative, condotte dagli organi inquirenti (e non dal software; quindi, non si potrebbe ritenere che si tratti di un monitoraggio attraverso mezzi automatizzati) [122].

Il Garante, con riferimento all'attività di monitoraggio, ritiene che il servizio offerto da *Clearview* non sia sovrapponibile a quello di un motore di ricerca, in quanto consistente in un'operazione di rielaborazione delle immagini per ricavarne dati biometrici al fine di effettuare la comparazione tra immagini; le informazioni relative alle immagini vengono altresì arricchite nel tempo grazie alle ulteriori immagini che vengono aggiunte, così da evidenziare altresì i cambiamenti degli individui nel corso del tempo. L'attività svolta da *Clearview* consiste, quindi, nella classificazione degli individui, ma anche nell'estrazione dei dati biometrici e nell'acquisizione di informazioni ulteriori riguardanti gli interessati.

Oltre alle violazioni riguardanti l'assenza di una valida base giuridica del trattamento (artt. 6 nonché 9 del Regolamento) e dei principi applicabili al trattamento — segnatamente i principi di liceità, correttezza e trasparenza, di limitazione delle finalità — non viene neppure rispettato il principio del limite di durata della conservazione, non essendo rinvenibile il tempo di conservazione. Al contrario, il fatto che il database venga aggiornato in modo costante fa presupporre che le immagini e i metadati associati ad esse vengano conservati senza limite di tempo, rimanendo peraltro le immagini all'interno del sistema anche se sono state cancellate dalla fonte originaria o se la fonte è stata resa privata.

E proprio con riferimento all'utilizzo di database privati di riconoscimento facciale da parte delle autorità di contrasto e dei servizi di *intelligence*, come *Clearview* (ivi esplicitamente richiamato), il Parlamento europeo ha espresso «profonda preoccupazione» nella risoluzione del 6 ottobre 2021 [123].

In effetti, e in estrema sintesi, tre sono i punti che vengono in rilievo nella stessa: in primo luogo, l'invito alla Commissione ad «interrompere il finanziamento della ricerca o diffusione della biometrica o di programmi che potrebbero portare alla sorveglianza di massa indiscriminata nei luoghi pubblici» (punto 31); in secondo luogo il rilievo dei profili di criticità del trattamento di dati genetici e DNA (punto 29); nonché una presa di posizione netta a favore del divieto di qualsiasi sistema di *scoring* su larga scala di

[122] In riferimento alla profilazione richiama le linee guida del Gruppo di lavoro Articolo 29, *Linee guida sul Processo decisionale individuale automatizzato e Profilazione ai fini del Regolamento 2016/679* (wp251rev.01), in cui vengono elencate le fasi attraverso le quali si esplica l'attività di profilazione: raccolta dei dati; analisi automatizzata per ricercare le correlazioni; applicazione delle correlazioni emerse per predire i comportamenti futuri. La Società ritiene che, anche se le prime due fasi sono presenti nell'attività svolta da Clearview, l'ultima non sarebbe presente, in quanto se anche fossero individuate delle caratteristiche future, sarebbe ascrivibile ad un comportamento del cliente del servizio, da qualificarsi quale titolare del trattamento.

[123] Risoluzione del parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale il suo utilizzo da parte delle autorità di polizia giudiziaria in ambito penale (2020/2016 (INI).

cittadini, sulla considerazione che «qualsiasi forma di "*citizen scoring*" normativo sul larga scala da parte delle autorità pubbliche (…) conduce alla perdita di autonomia, indebolisce il principio di non discriminazione e non può essere considerato conforme ai diritti fondamentali, in particolare la dignità umana». Facendo leva sul principio di finalità, il Parlamento raccomanda un controllo democratico rigoroso e una supervisione indipendente per qualunque tecnologia basata su intelligenza artificiale che venga utilizzata da parte delle autorità di contrasto e giudiziaria, in particolare se destinata alla sorveglianza e alla profilazione di massa; prende atto con grande preoccupazione del potenziale di determinate tecnologie impiegate in tali settori per la sorveglianza di massa e sottolinea altresì «l'esigenza giuridica di prevenire la sorveglianza di massa tramite le tecnologie di IA, che per definizione non corrisponde ai principi di necessità e proporzionalità, e di vietare l'uso delle applicazioni che potrebbero risultare in tale sorveglianza» [124].

Sulla base di queste premesse e preso atto dei diversi tipi di utilizzo di riconoscimento facciale a fini di sorveglianza, il Parlamento chiede «un divieto permanente dell'utilizzo dei sistemi di analisi o riconoscimento automatico degli spazi pubblici di altre caratteristiche umane quali l'andatura, le impronte digitali, il DNA, la voce e altri segnali biometrici e comportamentali»; nonché una moratoria sulla diffusione di sistemi di riconoscimento facciale per le attività di contrasto con funzioni di identificazione, a meno che queste non siano usate strettamente a fini di identificazione delle vittime dei reati, almeno finché le norme tecniche non si potranno considerare »pienamente conformi con i diritti fondamentali» (punti 25,26 e 27).

Una lettura, quindi, che intende restituire centralità alla persona e che, in tale ottica, esprime forte preoccupazione per la deriva che alcuni meccanismi, più o meno velatamente, di sorveglianza di massa, rischiano di prendere nell'odierna società informazionale e digitale.

8. Conclusioni

Si è dunque visto come l'utilizzo di tecniche di riconoscimento biometrico, da un lato, e il trattamento dei dati genetici dall'altro, siano suscettibili di configurare una delle tappe verso la società della sorveglianza, proprio quella degenerazione della società dell'eguaglianza e della partecipazione guardata con sospetto dalla Corte europea dei diritti dell'uomo, dalla Corte di Giustizia dell'Unione europea, così come dai Garanti (a livello nazionale ed europeo).

È stato autorevolmente evidenziato dal Presidente emerito del Garante Europeo Buttarelli come, più in generale, la protezione dei dati personali abbia consentito l'individuazione di una «dimensione ulteriore

[124] Sottolineando peraltro come l'approccio adottato da alcuni paesi terzi sotto il profilo delle tecnologie di sorveglianza di massa, interferendo in modo sproporzionato con i diritti fondamentali, non possa essere seguito dall'Unione Europea. (Punto7).

della personalità», che «si configura come una precondizione per il pieno godimento di altri diritti fondamentali [125]. In una società globalizzata e digitalmente interconnessa, solo un corretto trattamento dei dati consente una «giusta esplicazione delle scelte di vita» dei soggetti, singoli e aggregati, integrando un irrinunciabile punto di partenza, finanche quale «unico *a priori* del diritto» [126]. Se così è, questa dimensione della personalità, per la sua valenza prodromica al pieno ed effettivo esercizio degli altri diritti fondamentali rappresenta una «espressione particolarmente forte - quasi metonimica - della dignità personale, meta-valore riassuntivo dell'impianto assiologico sui cui si innestano le situazioni giuridiche costituzionalmente protette» [127].

In questo quadro, un approccio *data driven* appare dunque il più appropriato, non solo in funzione del miglioramento di diagnosi e cura nel quadro dell'impiego di dati genetici e dati biometrici (o, come si è accennato, anche in ambito sanitario), ma proprio come approccio di processo che restituisca centralità alla persona, la cui identità viene in gioco sotto vari profili.

Ancora una volta, la prospettiva da adottare fa leva sulla tecnica del bilanciamento [128] tra principi confliggenti, da sempre criterio «che preserva da precipitosa realizzazione di un valore a scapito di altri e dispone al controllo critico di razionalità mediante il *test* di universalizzabilitá» di fronte alla pericolosa «rivendicazione come diritto di qualunque pretesa soggettiva, cioè di qualunque desiderio, espressione di una concezione dell'esistenza individualistica (ciò che esiste solo il singolo con le proprie aspirazioni) e relativistica (non esiste nessun criterio oggettivo di giudizio esterno al soggetto)» e all'estensione dei

[125] Cfr. G. ALPA, *Diritto privato europeo*, Milano, 2016, p. 182-183; G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997.

[126] Cfr. E. DEL PRATO, *Dignità e solidarietà: spigolature di un civilista*, in *Rivista Italiana per le Scienze Giuridiche*, 2019, 10, p. 455.

[127] N. LIPARI, *Diritto civile e ragione*, Milano, 2019, p. 183 ss., ove la «clausola di dignità» è posta come «presupposto morale (...) per l'esercizio dei diritti definiti fondamentali», «fondamento della giuridicità medesima»).

[128] Si vedano le sempre attuali riflessioni sulla prudenza nel bilanciamento di G. ZAGREBELSKY, *Il diritto mite*, 1992, p. 200, in cui «quello che può apparire come l'arbitrio degli interpreti e l'incertezza del diritto non dipendono affatto, fondamentalmente, da una o da un'altra concezione dell'interpretazione del diritto ma da molto più profonde condizioni nelle quali il diritto è chiamato ad operare. (…) Se ciò comporta conseguenze negative sulla certezza del diritto, occorre avere chiaro che esse non sono lo stravolgimento, ma la conseguenza dei sistemi giuridici attuali. (…) La fissità, che è un aspetto della certezza, non è dunque più un elemento portante degli attuali sistemi giuridici e al deficit di certezza che ne deriva non si potrebbe porre rimedio con una più adeguata teoria dell'interpretazione (...)».

cosiddetti «diritti desiderio» [129], bilanciamento che deve essere effettuato secondo ragione [130], avendo sempre come punto di riferimento la dignità della persona [131].

Proprio la dignità della persona occorre mettere al centro di ogni azione e considerazione per evitare il rischio di una degenerazione della sovranità digitale in autoritarismo digitale, foriero di controllo, di censura dei contenuti, oltre che di profila azione dell'identità dei singoli e dei gruppi di individui.

Del resto, anche l'attuale dibattito in tema di neurotecnologie ed interazione macchina-cervello umano, da un lato, nonché di tecnologie IA *ChatGPT* — su cui proprio di recente è intervenuta in senso garantista l'*Authority* con provvedimento dell'11 aprile 2023 [132] — dall'altro, dimostrano come le risposte alle questioni più urgenti su questi temi vadano ricercate non perdendo mai di vista l'essenza stessa dell'uomo in quanto tale.

[129] P. GIANNITI, *Problematiche connesse alla tendenza espansiva dei diritti fondamentali*, in *I diritti fondamentali nell'unione europea. La carta di Nizza dopo il trattato di Lisbona*, a cura di P. GIANNITI, Bologna, 2013, 218 ss. che richiama sul punto EPIDENDIO e PIFFER, *Rapporti tra diritti fondamentali, giudici e politici* (quotidiano *online* il[sussidiario.net](sussidiario.net), 24 - 21 marzo, nonché 7 aprile 2011, giungendo alla conclusione di una necessità di «recuperare una visione globale del reale e, in particolare, la dimensione relazionale dei diritti individuali, il che significa che, rispetto ad ogni nuovo diritto fondamentale, occorre cercare di comprendere se l'interesse che sottende assume una rilevanza tale da giustificare una sua attrazione nella sfera della giuridicità, cioè nella dimensione relativa alla ripartizione proporzionata di beni esteriori all'interno di un gruppo socialmente organizzato».

[130] Cfr. P. GIANNITI, *ult. op. cit.*, 223, in cui cita in proposito F. GALGANO, *Democrazia politica e legge della ragione*, in *Contr. e impr.*, 2007, 393 ss., laddove afferma che «si postula, con la proclamazione dei diritti dell'uomo, l'esistenza di un ordine giuridico che, come ha praticato la scuola del diritto naturale, riprende la propria fonte dalla natura stessa dell'uomo. Le Corti costituzionali proseguiranno l'opera: dalla ragione, che è madre del diritto ricaveranno il criterio di ragionevolezza, quale criterio di valutazione della legittimità della legge ordinaria», nonché ID., *Globalizzazione dell'economia e universalità del diritto*, in *Pol. dir.*, 2009, 177 ss., in cui si legge che «si è cominciato con il sindacato alla stregua del criterio della ragionevolezza le deroghe al principio costituzionale di eguaglianza, giudicate come ammissibili solo se ragionevoli; si è proseguito con il giudicare illegittimo il trattamento legislativo uniforme di situazioni tra loro diverse quando la ragionevolezza avrebbe richiesto un trattamento differenziato; infine, la ragionevolezza è stata assunta come autonomo criterio di valutazione delle leggi, a prescindere dal principio di uguaglianza».

[131] Nel senso che la protezione dei diritti inviolabili deve essere assunta come criterio principale atto ad orientare l'interprete nell'esegesi del sistema normativo e nell'opera di bilanciamento stesso tra diritti fondamentali, nell'ottica di tutelare in pieno rispetto della dignità della persona umana, cfr anche, ad esempio, R. PARDOLESI, in nt. a Trib. Milano, 28 settembre 2016, in *Foro it.*, 2016, I, 3594, che sottolinea come tale impostazione sia l'unica compatibile con il principio personalistico e con la visione della persona umana quale valore etico in sé, per cui è vietata ogni strumentalizzazione della medesima «per alcun altro fine eteronomo ed assorbente», compreso, quindi l'interesse economico o la libertà di iniziativa economica.

[132] Garante per la protezione dei dati personali, provvedimento dell' 11 aprile 2023, doc. web n. 9874702, consultabile sul sito istituzionale del Garante.