MASTER UNIVERSITARIO DI II LIVELLO

“DATA PROTECTION OFFICER E TRANSIZIONE DIGITALE (DPOTD)”

A.A. 2024-2025

Tesi

Il valore del consenso dell’interessato nel trattamento dei dati relativi alla salute

Relatore

Prof.ssa Danila Iacovelli

Studente Master

Dott.ssa Leila Colucci

Il valore del consenso dell'interessato
nel trattamento dei dati relativi alla salute

INDICE

CAPITOLO III

INTRODUZIONE

Tra le varie categorie particolari di dati personali, i dati relativi alla salute svolgono un ruolo di particolare importanza[1]. Per la rilevanza di questo tipo di dati sensibili, in termini di intimità del potenziale informativo e di stretto legame con l'identità della persona e il suo vissuto, da un lato, e di utilità e benefici per la collettività nel loro trattamento, dall'altro, è ad essi viene prestata specifica attenzione.

Il trattamento dei dati relativi alla salute è forse quello che più richiede un'attenta opera di bilanciamento da parte del legislatore, trattandosi di attività in cui maggiormente emerge la contrapposizione fra il diritto alla riservatezza dell'interessato, anche in una prospettiva di garanzia e difesa contro potenziali discriminazioni, e l'interesse comune, pubblico o di terzi, all'informazione stessa e ai vantaggi che ne derivano[2].

Tale trattamento di dati personali, infatti, risulta in stretta connessione con il diritto alla salute e partecipa alla sua tutela[3].

La tematica è stata affrontata anche nel diritto internazionale.

La Convenzione sui diritti dell'uomo e la biomedicina del 1997, c.d. Convenzione di Oviedo[4], sancisce espressamente, nel Capitolo III, "Vita privata e diritto all'informazione",

---

[1] *In primis*, per il funzionamento del sistema sanitario. V. M.A. SANDULLI, *Introduzione*, in A. THIENE e S. CORSO (a cura di), *op. cit.*, 1 ss.,

[2] C. PERLINGIERI, *eHealth and Data*, in SENIGAGLIA, C. IRTI e BERNES (a cura di), *op. cit.*, 127 ss.; DI MASI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 75, d.lgs. 30 giugno 2003, n. 196, 1235 s. V. SORO, *Persone in rete. I dati tra poteri e diritti*, Roma, Fazi Editore, 2018, 105.

[3] Sul diritto alla salute P. PERLINGIERI, *Il diritto alla salute quale diritto della personalità*, in *Rass. dir. civ*., 1982, 1020 ss., ora in ID., *La persona e i suoi diritti. Problemi del diritto civile*, cit., 101 ss.; ID., *Il diritto civile nella legalità costituzionale*, cit., 360 ss. Nella vasta produzione sull'argomento si ricorda PEZZINI, *Il diritto alla salute: profili costituzionali*, in *Diritto e società*, 1983, 21 ss.; CARAVITA, *La disciplina costituzionale della salute*, in *Diritto e società*, 1984, 21 ss.; ALPA, voce «Salute (diritto alla)», in *Noviss. Digesto it*., app. VI, Torino, Utet, 1986, 913 ss.; D'ARRIGO, voce «Salute (diritto alla)», in *Enc. del dir*., agg. V, Milano, Giuffrè, 2001, 1009 ss.; R. FERRARA, *Il diritto alla salute: i principi costituzionali*, in ID. (a cura di), *Salute e sanità*, nel *Trattato di biodiritto* diretto da Rodotà e Zatti, Milano, Giuffrè, 2010, 3 ss.; CORDIANO, *Identità della persona e disposizione del corpo. La tutela della salute nelle nuove scienze*, Roma, Aracne, 2011, 1 ss.; MORANA, *La salute come diritto costituzionale. Lezioni*, 4a ed. Torino, Giappichelli, 2021; CUTTAIA, *Il recupero della centralità del diritto alla salute. Prospettive di riforma del Servizio Sanitario Nazionale*, Torino, Giappichelli, 2022, 1 ss.; MORRONE e MINNI, *La salute come valore costituzionale e fonte di diritti soggettivi alla luce della giurisprudenza costituzionale*, in ALPA (a cura di), *La responsabilità sanitaria. Commento alla l. 8 marzo 2017, n. 24*, 2a ed., Pisa, Pacini, 2022, 120 ss

[4] Convenzione per la protezione dei Diritti dell'Uomo e della dignità dell'essere umano nei confronti dell'applicazioni della biologia e della medicina, firmata a Oviedo il 4 aprile 1997, la cui ratifica da parte dell'Italia è stata autorizzata con l. 28 marzo 2001, n. 145. Pur non essendo la Convenzione formalmente ratificata, mancando ancora il deposito dello strumento di ratifica, il suo contenuto si intende trasmesso

all'art. 10, il diritto di ciascuno a che sia rispettata la propria vita privata, allorché si tratti di informazioni relative alla propria salute, e il diritto a conoscere ogni informazione raccolta sulla propria salute e a veder rispettata una propria volontà di segno contrario, diritto al cui esercizio è possibile, a titolo eccezionale, che la legge preveda, nell'interesse del paziente, delle restrizioni[5]. Nel Rapporto esplicativo del Consiglio d'Europa alla Convenzione, è chiarito come il par. 1 dell'art. 10, nel proclamare il diritto alla riservatezza delle informazioni sulla salute, riaffermi il principio di cui all'art. 8 CEDU, ripreso anche dalla Convenzione n. 108 del 1981, la quale all'art. 6 – richiamato – annovera i dati relativi alla salute fra le categorie particolari di dati meritevoli di speciale protezione, come già evidenziato. Aggiunge, altresì, che alcune limitazioni al rispetto della privacy sono ammesse per una delle ragioni e alle condizioni dettate dall'art. 26, par. 1, ossia purché vengano previste dalla legge e costituiscano delle misure necessarie, in una società democratica, alla sicurezza pubblica, alla prevenzione delle infrazioni penali, alla protezione della salute pubblica o alla protezione dei diritti e libertà altrui[6].

Sempre nell'ambito del Consiglio d'Europa, il 13 febbraio 1997, il Comitato dei ministri adottò una raccomandazione relativa alla protezione dei dati sanitari[7]. Facendo

---

nell'ordinamento italiano, attraverso la legislazione in armonia con essa e l'operato della giurisprudenza, che ha fatto uso delle sue nozioni per interpretare le disposizioni di diritto interno.

[5] Art. 10 – *Private life and right to information*: «*1. Everyone has the right to respect for private life in relation to information about his or her health. 2. Everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed. 3. In exceptional cases, restrictions may be placed by law on the exercise of the rights contained in paragraph 2 in the interests of the patient*». Cfr. COCO, *op. cit.*, 437 ss., spec. 454 ss.; CHADWICK, LEVITT e SHICKLE (a cura di), *The Right to Know and the Right Not to Know: Genetic Privacy and Responsibility*, 2a ed., Cambridge University Press, 2014.

[6] «*The first paragraph establishes the right to privacy of information in the health field, thereby reaffirming the principle introduced in Article 8 of the European Convention on Human Rights and reiterated in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. It should be pointed out that, under Article 6 of the latter Convention, personal data concerning health constitute a special category of data and are as such subject to special rules. 64. However, certain restrictions to the respect of privacy are possible for one of the reasons and under the conditions provided for in under Article 26.1. For example, a judicial authority may order that a test be carried out in order to identify the author of a crime (exception based on the prevention of a crime) or to determine the filiation link (exception based on the protection of the rights of others)*». COUNCIL OF EUROPE, *Explanatory Report to the Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine*, Oviedo, 4.4.2017, in *www.coe.int*, 11, punti 63 e 64.

[7] È la Raccomandazione n. R(97), *www.coe.int.*

V. FINOCCHIARO, *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, in G.F. FERRARI (a cura di), *La legge sulla privacy dieci anni dopo*, Milano, EGEA, 2008, 217, che ne ricorda l'applicabilità in materia, pur trattandosi di fonti non cogenti. Dopo la presentazione del rapporto del 2015 (BOSSI MALAFOSSE, *Introductory Report for*

seguito a quella e alla raccomandazione sulla protezione dei dati personali raccolti e trattati a scopi assicurativi[8], il 26 ottobre 2016, è stata adottata anche una raccomandazione sul trattamento dei dati personali relativi alla salute a scopi assicurativi, inclusi i dati risultanti da test genetici[9].

Del tema si sono occupate anche le Nazioni Unite. Lo *Special Rapporteur on the Right to Privacy*[10] ha istituito la *Task Force on Privacy and the Protection of Health- Related Data* e ha guidato la preparazione della *Recommendation on the Protection and Use of Health-Related Data*, adottata il 6 novembre 2019[11].

Il trattamento dei dati relativi alla salute viene poi ad essere strettamente legato al funzionamento dei sistemi sanitari nazionali e di tale connessione si ha riscontro a livello internazionale. L'Organizzazione mondiale della Sanità, infatti, ha evidenziato come, potendo raggiungersi migliori risultati nell'ambito della salute pubblica mediante i sistemi informativi, sia fondamentale per avere un buon sistema informativo sanitario poter contare su processi organizzati di raccolta, condivisione, analisi e utilizzo di dati relativi alla salute nei processi decisionali[12].

---

updating Recommendation R (97) 5 of the Council of Europe on the Protection of medical Data, Strasburgo, 15 giugno 2015, consultabile in *www.coe.int*), la raccomandazione è stata aggiornata nel 2019. L'aggiornamento è avvenuto ad opera della Raccomandazione del Comitato dei ministri, CM/Rec(2019)2, reperibile in *www.edoc.coe.int*, la cui appendice ha sostituito il testo della raccomandazione del '97.

[8] *Recommendation Rec(2002)9 on the protection of personal data collected and processed for insurance purposes*, adottata dal Comitato dei ministri il 18 settembre 2002, consultabile in *www.coe.int*.

[9] *Recommendation CM/Rec(2016)8 of tCommittee of Ministers to the member States on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests*, in *www.coe.int*.

[10] Nel 2015 lo *Human Rights Council* dispose il primo mandato sulla privacy, con la Risoluzione 28/16, *The right to privacy in the digital age*, poi rinnovato con la Risoluzione del 22 marzo 2018. In relazione, nello specifico, al trattamento dei dati personali relativi alla salute, lo *Special Rapporteur* ha presentato un report sulla gestione della crisi pandemica (A/76/220) e un report sulle attività svolte nel 2019 (A/HRC/43/52). Tutti i testi sono consultabili in *www.undocs.org*.

[11] Il testo è consultabile in *www.ohchr.org*. Le basi giuridiche specifiche per il trattamento dei dati relativi alla salute elencate nella sezione 5, di cui al capitolo 2, di questa raccomandazione presentano diversi profili di somiglianza con le eccezioni al divieto di trattamento di cui al par. 2 dell'art. 9 del reg. Ue n. 679 del 2016, pur discostandosene per svariati aspetti. Oltre al consenso dell'interessato, posto in apertura dell'elenco, si considera legittimo, in particolare, il trattamento dei dati relativi alla salute effettuato «*for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*» (lett. *e*, sezione 5.1).

[12] «*A sound health information system depends upon organized processes for gathering, sharing, analysing and using health-related data for decision-making*». WORLD HEALTH ORGANIZATION, *Framework and Standards for Country Health Information Systems*, 2a ed., in *www.who.int*, 2012, 8. Cfr. WORLD HEALTH ORGANIZATION. REGIONAL OFFICE FOR EUROPE, *The protection of personal data in health information systems – principles and processes for public health*, *ivi*, 2021. «*A well-functioning national health information system (HIS) is a prerequisite for the provision of reliable and timely health-related information. This information is essential for: 1) policy development and evidence-informed decision-making; 2) proper health*

Alla tutela della salute sono dedicate norme pure nel Trattato sul funzionamento dell'Unione europea. Così, la tutela e il miglioramento della salute umana costituiscono, ai sensi dell'art. 6, lett. *a*, TFUE, uno dei settori in cui l'Unione «ha competenza per svolgere azioni intese a sostenere, coordinare o completare l'azione degli Stati membri» e, come sancito nel Titolo XIV, "Sanità pubblica", della Parte III del TFUE, "Politiche e azioni interne dell'Unione", dall'art. 168, par. 1, «nella definizione e nell'attuazione di tutte le politiche ed attività dell'Unione è garantito un livello elevato di protezione della salute umana»[13]. In base a tale

---

management and rational resource allocation; and 3) monitoring and evaluation of health systems and other related social services performance». ALWAN *et al*., *Strengthening national health information systems: challenges and response*, in *Eastern Mediterranean Health Journal*, 2016, vol. 22, n. 11, 840.

[13] L'art. 168 TFUE, *ex* art. 152 TCE, prosegue così: «L'azione dell'Unione, che completa le politiche nazionali, si indirizza al miglioramento della sanità pubblica, alla prevenzione delle malattie e affezioni e all'eliminazione delle fonti di pericolo per la salute fisica e mentale. Tale azione comprende la lotta contro i grandi flagelli, favorendo la ricerca sulle loro cause, la loro propagazione e la loro prevenzione, nonché l'informazione e l'educazione in materia sanitaria, nonché la sorveglianza, l'allarme e la lotta contro gravi minacce per la salute a carattere transfrontaliero. L'Unione completa l'azione degli Stati membri volta a ridurre gli effetti nocivi per la salute umana derivanti dall'uso di stupefacenti, comprese l'informazione e la prevenzione. 2. L'Unione incoraggia la cooperazione tra gli Stati membri nei settori di cui al presente articolo e, ove necessario, appoggia la loro azione. In particolare incoraggia la cooperazione tra gli Stati membri per migliorare la complementarietà dei loro servizi sanitari nelle regioni di frontiera. Gli Stati membri coordinano tra loro, in collegamento con la Commissione, le rispettive politiche ed i rispettivi programmi nei settori di cui al paragrafo 1. La Commissione può prendere, in stretto contatto con gli Stati membri, ogni iniziativa utile a promuovere detto coordinamento, in particolare iniziative finalizzate alla definizione di orientamenti e indicatori, all'organizzazione di scambi delle migliori pratiche e alla preparazione di elementi necessari per il controllo e la valutazione periodici. Il Parlamento europeo è pienamente informato.

3. L'Unione e gli Stati membri favoriscono la cooperazione con i paesi terzi e con le organizzazioni internazionali competenti in materia di sanità pubblica. 4. In deroga all'articolo 2, paragrafo 5, e all'articolo 6, lettera a), e in conformità dell'articolo 4, paragrafo 2, lettera k), il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria e previa consultazione del Comitato economico e sociale e del Comitato delle regioni, contribuiscono alla realizzazione degli obiettivi previsti dal presente articolo, adottando, per affrontare i problemi comuni di sicurezza: a) misure che fissino parametri elevati di qualità e sicurezza degli organi e sostanze di origine umana, del sangue e degli emoderivati; tali misure non ostano a che gli Stati membri mantengano o introducano misure protettive più rigorose; b) misure nei settori veterinario e fitosanitario il cui obiettivo primario sia la protezione della sanità pubblica; c) misure che fissino parametri elevati di qualità e sicurezza dei medicinali e dei dispositivi di impiego medico. 5. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria e previa consultazione del Comitato economico e sociale e del Comitato delle regioni, possono anche adottare misure di incentivazione per proteggere e migliorare la salute umana, in particolare per lottare contro i grandi flagelli che si propagano oltre frontiera, misure concernenti la sorveglianza, l'allarme e la lotta contro gravi minacce per la salute a carattere transfrontaliero, e misure il cui obiettivo diretto sia la protezione della sanità pubblica in relazione al tabacco e all'abuso di alcol, ad esclusione di qualsiasi armonizzazione delle disposizioni legislative e regolamentari degli Stati membri. 6. Il Consiglio, su proposta della Commissione, può altresì adottare raccomandazioni per i fini stabiliti dal presente articolo. 7. L'azione dell'Unione rispetta le responsabilità degli Stati membri per la definizione della loro politica sanitaria e per l'organizzazione e la fornitura di servizi sanitari e di assistenza medica. Le responsabilità degli Stati membri includono la gestione dei servizi sanitari e dell'assistenza medica e l'assegnazione delle risorse loro destinate. Le misure di cui al paragrafo 4, lettera a) non pregiudicano le disposizioni nazionali sulla donazione e l'impiego medico di organi e sangue». In arg. RINOLDI, *«In deroga…*

articolo, il Parlamento europeo e il Consiglio hanno adottato, abrogando il reg. Ue n. 282 del 2014, il reg. Ue 2021/522, istitutivo del programma UE per la salute (*EU4Health*) per il periodo 2021-2027[14].

Tale programma ha fra i suoi obiettivi generali – come si legge all'art. 3 – quello di «rafforzare i sistemi sanitari migliorandone la resilienza e sviluppando l'efficienza delle risorse, in particolare promuovendo l'attuazione delle migliori pratiche e promuovendo la condivisione dei dati» (lett. *d, ii*). Mentre, fra gli obiettivi specifici attraverso i quali si perseguono quelli generali, si annovera l'obiettivo di «rafforzare l'uso e il riutilizzo dei dati sanitari per la prestazione di assistenza sanitaria e per la ricerca e l'innovazione, promuovere la diffusione di strumenti e servizi digitali, nonché la trasformazione digitale dei sistemi sanitari, anche sostenendo la creazione di uno spazio europeo dei dati sanitari» (art. 4, lett. *f*)[15]. «Nella gestione e attuazione del programma – recita l'art. 18 – la Commissione e gli Stati membri garantiscono il rispetto di tutte le disposizioni di legge pertinenti relative alla protezione dei dati personali nonché, se del caso, l'introduzione di meccanismi volti a garantire la riservatezza e la sicurezza di tali dati»[16].

---

e in conformità»: prospettive dell'Unione europea della salute muovendo dall'art. 168 TFUE per andar ben oltre (verso un comparto sanitario federale continentale?), in *Corti supreme e salute*, 2022, fasc. 1, 273 ss. Cfr. ODDENINO, *Profili internazionali ed europei del diritto alla salute*, in R. FERRARA (a cura di), *Salute e sanità*, nel *Trattato di biodiritto* diretto da Rodotà e Zatti, Milano, Giuffrè, 2010, 65 ss.

[14] Regolamento (UE) 2021/522 del Parlamento europeo e del Consiglio, del 24 marzo 2021, *che istituisce un programma d'azione dell'Unione in materia di salute per il periodo 2021-2027 («programma UE per la salute») (EU4Health) e che abroga il regolamento (UE) n. 282/2014*.

[15] Ulteriori obiettivi specifici che includono l'utilizzo dei dati sono previsti alle lett. *b* e *h* dell'art. 4, rispettivamente: «rafforzare le capacità dell'Unione in materia di prevenzione, preparazione e risposta rapida in caso di gravi minacce per la salute a carattere transfrontaliero in conformità della pertinente legislazione dell'Unione e migliorare la gestione delle crisi sanitarie, in particolare attraverso il coordinamento, la fornitura e la mobilitazione di capacità di assistenza sanitaria di emergenza, sostenere la raccolta di dati, lo scambio di informazioni, la sorveglianza, il coordinamento delle prove di stress volontarie dei sistemi sanitari nazionali e l'elaborazione di norme per un'assistenza sanitaria di qualità a livello nazionale»; e «sostenere l'elaborazione, l'attuazione e l'applicazione e, ove necessario, la revisione della legislazione dell'Unione in materia di salute e sostenere la fornitura di dati validi, affidabili e comparabili di elevata qualità per consentire un processo decisionale e un monitoraggio delle decisioni basati su elementi concreti, e promuovere il ricorso a valutazioni dell'impatto sanitario delle altre politiche pertinenti dell'Unione».

[16] «Anche il citato regolamento, tuttavia, non può che muoversi nel quadro delle competenze attualmente vigenti incentrate, come si è ripetutamente sottolineato, sul ruolo degli Stati membri, dei quali può "soltanto" essere incentivata e promossa la "collaborazione e cooperazione"». MORANA, *Verso un diritto eu rounitario alle cure? La direttiva sull'assistenza transfrontaliera tra obiettivi ambiziosi e debolezze competenziali dell'Unione*, in *Corti supreme e salute*, 2022, fasc. 1, 238 s. Cfr. A. RIZZO, *La crisi pandemica e la nuova centralità delle politiche sanitarie europee alla luce della disciplina "EU4Health"*, in *Studi sull'integrazione europea*, 2021, 107 ss.

La protezione dei dati personali si va dunque ad intersecare con il diritto alla salute[17] che gli ordinamenti devono garantire ai singoli e alla collettività. Punto d'incontro e insieme frizione e convergenza dei diversi poli di interessi contrapposti viene ad essere la tecnologia e dall'Intelligenza Artificiale, per mezzo della quale maggiormente si compie il trattamento di dati relativi alla salute e si tende a una miglior tutela della salute stessa[18]. Oltre a una sanità più efficiente e in grado di offrire più servizi, la digitalizzazione nel settore sanitario è stata considerata elemento chiave nella gestione della crisi pandemica. Tali argomenti saranno trattati nel terzo capitolo dell'elaborato.

Del diritto alla salute esiste, infatti, una dimensione europea[19]. Accolto e tutelato nell'ordinamento interno, non si è affermato solo a livello nazionale – in Italia il riferimento è all'art. 32 Cost. –, ma anche sul piano sovranazionale. Con riguardo al

[17] Secondo la celebre definizione dell'OMS, «*health is a state of complete physical, mental, and social well-being and not merely the absence of disease or infirmity*». Tale definizione, che per V. DURANTE, *Dimensioni della salute: dalla definizione dell'OMS al diritto attuale*, in *Nuova giur. civ. comm.*, 2001, II, 132, è «diffusamente giudicata come ricca di implicazioni non facilmente circoscrivibili», rimanda a un'idea di salute che, lungi dal limitarsi all'aspetto corporeo dell'individuo, si estende fino a ricomprendere il benessere sociale della persona. Peraltro, l'endiadi, salute e benessere, costituisce anche l'oggetto di uno dei diciassette obiettivi per lo sviluppo sostenibile – il terzo – di cui alla c.d. Agenda 2030, il programma di azione per le persone, il pianeta e la prosperità, sottoscritto nel settembre 2015 dai governi dei 193 Paesi membri dell'ONU. V. PACINI e PIZZANELLI (a cura di), *L'obiettivo 3 dell'Agenda 2030: salute e benessere. Statistiche, politiche e diritto*, Napoli, Editoriale Scientifica, 2022. Informazioni al riguardo sono fornite anche in *sdgs.un.org*, e, per la prospettiva italiana, in *www.agenzia- coesione.gov.it*. Cfr. WILKINSON *et al*., *Cambiamento climatico, migrazioni e Agenda 2030 per lo sviluppo sostenibile*, in *Equilibri*, 2017, fasc. 1, p. 148 ss. Si aggiunga pure che salute e protezione dei dati personali incrociano la tutela dell'ambiente, prendendo in considerazione l'informazione ambientale. In arg. BRUTTI, *Le regole dell'informazione ambientale, tra pubblico e privato*, in *Dir. inf*., 2022, 617 ss.

[18] Si vedano i contributi raccolti in HERVEG (a cura di), *La protection des données médicales. Les défis du XXI^e siècle*, Limal, Anthemis, 2008, in particolare il capitolo introduttivo di WILSON, *The changing face of healthcare systems and new demands on medical data handling*, 13 ss.

[19] LEENEN, *The Rights of Patients in Europe*, in *European Journal of Health Law*, vol. 1, n. 1, 1994, 5 ss.; ROSCAM ABBING, *European Governance of Health Systems. It Takes Two to Tango: The Council of Europe and the European Union*, in *European Journal of Health Law*, vol. 25, n. 2, 2018, 121 ss. V. poi CUTTAIA, *La dimensione europea del diritto alla salute e i suoi riflessi sull'ordinamento italiano*, in ALPA (a cura di), *La responsabilità sanitaria. Commento alla l. 8 marzo 2017, n. 24*, 2a ed., Pisa, Pacini, 2022, 153 ss.; ID., *Il recupero della centralità del diritto alla salute. Prospettive di riforma del Servizio Sanitario Nazionale*, cit., 99 ss.; CAPPUCCINI, *La dimensione europea del diritto alla salute*, in ALPA (a cura di), *La responsabilità sanitaria. Commento alla L.8 marzo 2017, n. 24*, Pisa, Pacini, 2017, 55 ss. Anche per le successive considerazioni, sia concesso il rimando a S. CORSO, *Brevi riflessioni sulla dimensione europea del diritto alla salute*, in *www.rivistaresponsabilitamedica.it*, 3 ottobre 2018; POSTERARO, *La responsabilità del medico nelle prime applicazioni della legge Gelli-Bianco*, Roma, Dike, 2019, 15 ss. Cfr. IADICICCO, *Frontiere e confini del diritto alla salute*, in *Diritto e società*, 2019, 76, secondo cui «l'intervento dell'Unione a tutela della salute umana non può in alcun modo tradursi nel riconoscimento in capo agli individui del diritto ad ottenere determinate cure mediche, potendosi al più sostanziare in limitate forme di ingerenza nella definizione delle politiche sanitarie nazionali e nell'organizzazione dei servizi sanitari». V. anche DIURNI, *I diritti collettivi dei pazienti nel panorama europeo*, in *Riv. dir. priv*., 2017, 349 ss. In una prospettiva bioetica e biogiuridica, FANNI, *Human health and vulnerability in the era of the Anthropocene and of the transhumanism*, in *Ius et scientia*, 2019, vol. 5, n. 1, 11 ss.

perimetro europeo, a contribuire nel delineare il diritto alla salute, nel tempo, è stata una pluralità di fonti di carattere sovranazionale e non solo. Se la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali non menziona il diritto alla salute, pur offrendone una garanzia indiretta attraverso il riconoscimento di altri diritti[20], a contemplarlo espressamente è la Carta dei diritti fondamentali dell'Unione europea. L'art. 35 della Carta di Nizza, implicante un principio di eguaglianza sostanziale nella tutela della salute, sancisce, infatti, il diritto di accesso alla prevenzione sanitaria e di ottenimento di cure mediche, affidando alle legislazioni e alle prassi degli Stati il compito di stabilirne le condizioni, e, riferendosi all'Unione europea, ne ravviva l'impegno per garantire la protezione della salute umana a un "livello elevato"[21].

La Carta europea dei diritti del malato, inoltre, proclama quattordici "diritti dei pazienti": diritto a misure preventive, all'accesso, all'informazione, al consenso, alla libera scelta, alla privacy e alla confidenzialità, al rispetto del suo tempo, al rispetto di standard di qualità, alla sicurezza, alla innovazione, a evitare le sofferenze e il dolore non necessari, a un trattamento personalizzato, al reclamo, al risarcimento.

La Carta europea dei diritti del malato viene peraltro richiamata nel Parere del Comitato economico e sociale europeo sul tema "I diritti del paziente", del 15 gennaio 2008, in cui il Comitato stesso dichiara di accoglierne con favore e riconoscerne i diritti sanciti, in particolare osservando come tre di essi possano considerarsi 'orizzontali' o preliminari ad altri: il diritto all'informazione, il diritto al consenso libero e informato e il diritto alla dignità. In merito a quest'ultimo, il Comitato, al punto 3.4.1.1 del suo parere, afferma che «ciascun cittadino ha diritto non solo alla riservatezza delle informazioni riguardanti il suo stato di salute, la diagnosi formulata e le modalità di cura, ma anche al rispetto della sua intimità durante gli esami, le visite e le cure mediche e chirurgiche». Mentre, con riguardo all'informazione, per il Comitato «è auspicabile che i dati riguardanti lo stato di salute della

[20] Si pensi, ad esempio, al diritto alla vita, al divieto di tortura, al diritto a un equo processo, al diritto al rispetto della vita privata e familiare, al divieto di discriminazione. Nello spazio della CEDU, una protezione concreta al diritto alla salute è poi offerta dalla giurisprudenza della Corte europea dei diritti dell'uomo, come conseguenza della tutela di altri diritti. Così è stato per l'applicazione dell'art. 3 CEDU, per cui nessuno può essere sottoposto a tortura né a pene o trattamenti inumani o degradanti, in relazione alla salute dei detenuti. V., al riguardo, Corte EDU, 28.1.1994, n. 17549/90, *Hurtado c. Svizzera*; Corte EDU, 24.10.2006, n. 6253/03, *Vincent c. Francia*; Corte EDU, 7.2.2012, n. 2447/05, *Cara-Damiani c. Italia*, tutte consultabili all'indirizzo *www.hudoc.echr.coe.int*.

[21] Art. 35 Carta dei diritti fondamentali dell'Unione europea, *Protezione della salute*: «Ogni individuo ha il diritto di accedere alla prevenzione sanitaria e di ottenere cure mediche alle condizioni stabilite dalle legislazioni e prassi nazionali. Nella definizione e nell'attuazione di tutte le politiche ed attività dell'Unione è garantito un livello elevato di protezione della salute umana».

persona interessata, gli approcci diagnostici e terapeutici messi in campo e i relativi risultati siano resi disponibili in un'apposita "cartella sanitaria". Anche l'accesso a tale cartella direttamente da parte del paziente oppure, se quest'ultimo lo desidera, con l'intermediazione del medico di sua scelta, fa parte del processo di informazione e di emancipazione del paziente stesso. Gli sforzi intesi a garantire maggiori informazioni e trasparenza devono tuttavia essere regolati da un quadro giuridico adeguato, per far sì che la raccolta di dati medici non sia utilizzata per scopi diversi da quelli previsti. Per quanto concerne i dati in formato elettronico e, se del caso, anche quelli diffusi oltrefrontiera, è particolarmente importante esercitare un controllo molto accurato sul modo in cui vengono utilizzati»[22].

Con questi presupposti, si può intendere come l'intreccio fra il diritto alla salute e la protezione dei dati personali diventa stringente ma anche articolato, nell'unitarietà dei diritti della persona.

Il presente elaborato procederà, innanzitutto, all'analisi della categoria di quella particolare categoria di dati sensibili rappresentata dai dati sanitari. Dal Regolamento generale sulla protezione dei dati si passerà alla normativa nazionale, cercando di capire quali strumenti sono stati predisposti dal legislatore interno per completare la tutela delineata a livello eurounitario, e si tratterà – a chiusura del primo capitolo – delle categorie particolari di dati personali logicamente più vicine, ossia i dati genetici e quelli biometrici, proprio in quanto legate ai dati sulla salute delle persone.

Nel secondo capitolo si approfondirà la tematica del consenso dell'interessato al trattamento delle diverse categorie di dati, con un focus sui dati sanitari, e secondo la disciplina comunitaria ed italiana.

Esaminando le disposizioni in materia di trattamento dei dati sanitari, nel terzo ed ultimo capitolo, si evidenzierà la loro necessaria vocazione alla garanzia delle libertà e i diritti fondamentali della persona; infatti, tutta la disciplina sulla protezione dei dati personali, comprese le regole sul trattamento di dati sanitari, non ha come fine la mera tutela dei dati stessi, bensì la persona[23]

[22] È il punto 3.2.5 del parere.

[23] «Il regolamento Ue, quindi, non è a tutela soltanto della riservatezza: esso disciplina più ampiamente la dignità della persona umana; la riservatezza ne è un aspetto, a volte relativo, e di certo non la esaurisce». P. PERLINGIERI, Privacy *digitale e protezione dei dati personali tra persona e mercato*, cit., 484. V. anche F. PIRAINO, *Il contrasto sulla nozione di dato sensibile, sui presupposti e sulle modalità del trattamento*, in *Nuova giur. civ. comm*., 2017, I, 1236 s.; ID., *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, cit., 401 ss. Cfr. A. THIENE, *I diritti morali d'autore*, in *Riv. dir. civ*., 2018, 1553 ss.

CAPITOLO I

I DATI RELATIVI ALLA SALUTE

1. *Dati relativi alla salute. Definizione*

La definizione di dato relativo alla salute si può considerare uno degli elementi chiave nel sistema di protezione delle informazioni personali. La disciplina sul trattamento dei dati inerenti allo stato di salute delle persone, negli ordinamenti giuridici, si basa infatti su questa nozione. Definire puntualmente il concetto di "dati relativi alla salute" rappresenta infatti un punto di partenza di rilevante importanza, considerata la delicatezza delle informazioni sulla persona che essi costituiscono.

Sul piano internazionale, la Convenzione n. 108 del 1981 non ne dà una definizione, ma il Rapporto esplicativo del Consiglio d'Europa, in relazione all'espressione '*personal data concerning health*' di cui all'art. 6, affermava che «*It includes information concerning the past, present and future, physical or mental health of an individual. The information may refer to a person who is sick, healthy or deceased. This category of data alsocovers those relating to abuse of alcohol or the taking of drugs*»[24]. Il Rapporto esplicativo della Convenzione n. 108 aggiunge dei tasselli, affermando che: «*Information concerning health includes information concerning the past, present and future, physical or mental health of an individual, and which may refer to a person who is sick or healthy. Processing images of persons with thick glasses, a broken leg, burnt skin or any other visible characteristics related to a person's health can only be considered as processing sensitive data when the processing is based on the health information that can be extracted from the pictures*»[25]. Una definizione di dati relativi alla salute è contenuta nella Raccomandazione sulla protezione dei dati relativi alla salute del 27 marzo 2019, adottata dal Comitato dei ministri del Consiglio d'Europa, all'art. 3: «*"health-related data" means all personal data concerning the physical or mental health of an individual, including the provision of healtcare services, which reveals information about this individual's past, current and future*

[24] «*The meaning of the term "personal data concerning health" has been carefully studied by the Committee of Experts on Data Protection in connection with its work on medical data banks*». COUNCIL OF EUROPE, *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, cit., 9, punto 45. Secondo GUARDA, *I dati sanitari*, cit., 593, «il nucleo concettuale di questa particolare categoria di dati si ritrova già nella Convenzione di Strasburgo 108/1981».

[25] COUNCIL OF EUROPE, *Convention 108+. Convention for the protection of individuals with regard to the processing of personal data*. *Explanatory Report*, cit., 22, punto 60.

health»[26]. Tale definizione ha peraltro sostituito quella di '*medical data*' offerta dalla Raccomandazione del 1997, secondo cui «*the expression "medical data" refers to all personal data concerning the health of an individual. It refers also to data which have a clear and close link with health as well as to genetic data*»[27].

Anche la Raccomandazione sulla protezione e l'uso dei dati relativi alla salute adottata in seno alle Nazioni Unite il 6 novembre 2019 ne fornisce una definizione, alla sezione 3, per cui «*"health-related data" means all personal data concerning the physical or mental health of an individual, including the provision of healthcare services, which reveals information about this individual's past, current or future health. Genetic data is health related data in the understanding of this recommendation. Health-related data concerning but not limited to data resulting from testing, such as a prenatal diagnosis, preimplantation diagnostics, or from the identification of genetic characteristics, whether or not regarded as the health-related data of the mother, must be protected to the same level as other health-related data*»[28].

L'Organizzazione internazionale per la normazione[29] ne ha dato a sua volta una definizione nelle linee guida del 2016 per gli standard di sicurezza informatica e le pratiche di gestione della sicurezza nel settore della salute, secondo cui per dati relativi alla salute si intende *«any information which relates to the physical or mental health of an individual, or to the provision of health service to the individual, and which may include: (a) information about the registration of the individual for the provision of health services; (b) information about payments or eligibility for healthcare with respect to the individual; (c) a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; (d) any information about the individual collected in the course of the provision of health services to the individual; (e) information derived from the testing or examination of a body part or bodily substance; and (f) identification of a person (healthcare professional) as provider of healthcare to the individual*»[30].

---

[26] Raccomandazione del Comitato dei ministri, CM/Rec(2019)2, cit

[27] Raccomandazione del Comitato dei ministri, n. R(97)5, cit.

[28] *Recommendation on the Protection and Use of Health-Related Data*, cit.

[29] Trattasi della *International Organization for Standardization*, meglio conosciuta con l'abbreviazione "ISO

[30] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, *Health informatics — Information security management in health using ISO/IEC 27002*, ISO 27799:2016, in *www.iso.org*. V. BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit.*, *sub* art. 4(15), 220. Si evidenzia che, nel Progetto di parere sulla proposta di direttiva concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera del 2008, il Garante europeo della protezione dei dati, dichiarandosi «decisamente favorevole all'adozione di una definizione specifica per i termini "dati sanitari"» in quel contesto, e suggerendo la possibilità che altresì fosse utilizzata successivamente «nell'ambito di altri testi pertinenti nella legislazione comunitaria», riporta, a tal proposito, la menzionata definizione di cui alla norma ISO 27799

Possiamo notare, quindi, che dello stesso concetto sono state date, nel tempo, più definizioni in ambito internazionale. Alcuni elementi sono ricorrenti, altri invece le diversificano. È però comune a tutte il riferimento alla salute non solo fisica, ma anche mentale del soggetto; è ricorrente quello ai servizi resi per la salute dell'individuo; allo stesso modo deve intendersi la connotazione temporale della condizione personale – passata, presente, futura – della nozione.

Quanto al diritto comunitario, la Direttiva n. 46 del 1995 non definiva i dati relativi alla salute. Nel 2003, però, la Corte di giustizia ne ha dato un'interpretazione, in relazione al disposto dell'art. 8 par. 1 della Direttiva, nel celebre caso *Lindqvist*[31].

La vicenda da cui ebbe origine il procedimento dinanzi ai giudici di Lussemburgo riguardava la pubblicazione in rete di una serie di dati personali, anche sensibili, in assenza del consenso degli interessati.

La signora Lindqvist era, nel 1998, una catechista in una parrocchia svedese. Un giorno, mentre era a casa, con il suo computer, decise di costruire alcune pagine in Internet per permettere, ai parrocchiani che si preparavano alla cresima, di avere le informazioni di cui necessitavano. Venne poi creato, a sua richiesta, anche un collegamento ipertestuale fra il sito della Chiesa di Svezia e quelle sue pagine. In esse, tuttavia, aveva inserito dati riguardanti, oltre a lei stessa, anche i suoi colleghi della parrocchia, includendo nome e cognome e descrivendo, scherzosamente, mansioni e abitudini nel tempo libero. Talvolta riportò anche i recapiti telefonici o la situazione familiare delle persone o le più varie informazioni. In particolare, fra i vari dati che aveva immesso, vi era anche il fatto che una collega si trovava in congedo parziale per malattia, per via di una ferita al piede. Non appena venne a sapere che la cosa non era apprezzata da alcuni colleghi, le eliminò. Del resto, ella non solo non li aveva resi edotti della sua iniziativa, ma neppure aveva chiesto se vi avrebbero acconsentito e non aveva nemmeno dichiarato il fatto all'ente pubblico svedese preposto alla tutela dei dati trasmessi per via informatica.

In seguito, vedendosi condannata al pagamento di un'ammenda dal tribunale di primo grado locale – contestò la rilevanza penale della sua condotta, impugnando il provvedimento

---

(Progetto di parere del garante europeo della protezione dei dati (GEPD) sulla proposta di direttiva del Parlamento europeo e del Consiglio concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (2009/C 128/03), del 2 dicembre 2008, in www.eulex.europa.eu, par. 16 e 17).

[31] La sentenza resa dai giudici di Lussemburgo in relazione al caso *Lindqvist* ebbe anche rilievo con riguardo al rapporto fra libertà di espressione e privacy. V., sul punto, SICA, *La libertà di informazione tra diritto interno e prospettiva europea*, cit., 22; M.G. STANZIONE, *Libertà di espressione e diritto alla privacy nel dialogo delle corti. Il caso del diritto all'oblio*, in *Eur. e dir. priv*., 2020, 991 ss., spec. 1001 s.

dinanzi al giudice dell'appello. Quest'ultimo, nutrendo dubbi sull'interpretazione della Direttiva n. 46 del 1995, sospese il procedimento e, con ordinanza del 23 febbraio 2001, investì la Corte di giustizia – ai sensi dell'art. 234 CE, corrispondente all'odierno art. 267 TFUE – di alcune questioni pregiudiziali, tra cui, nello specifico, la seguente: «se l'informazione, su una pagina iniziale, che un collega di lavoro, di cui viene specificato il nome, si è ferito ad un piede e si trova in congedo parziale per malattia costituisca un dato personale relativo alla salute che, a norma dell'art. 8, n. 1, della direttiva, non può essere trattato».

Nel rispondere affermativamente a tale quesito, la Corte ha accolto una lettura estensiva e una nozione inclusiva dei dati relativi alla salute. «In considerazione dell'oggetto [della] direttiva, occorre dare all'espressione "dati relativi alla salute" utilizzata nell'art. 8, n. 1, un'interpretazione ampia tale da comprendere informazioni riguardanti tutti gli aspetti, tanto fisici quanto psichici, della salute di una persona».

Trattasi di un approccio[32] basato sullo scopo della Direttiva di garantire un livello elevato di protezione dei dati personali, come enunciato nel suo considerando 10[33]. L'osservazione non è resa esplicita nella sentenza, ma tale indirizzo, oltre a trovare un fondamento tra gli obiettivi della Direttiva stessa, è riscontrato da una giurisprudenza più risalente, che ha privilegiato la confidenzialità di questi dati personali[34]. Nel 1992 la Corte di giustizia ebbe modo di affermare, infatti, che «il diritto al rispetto della sfera privata e quello alla tutela del segreto medico, che ne è uno degli aspetti, costituiscono diritti fondamentali tutelati dall'ordinamento giuridico comunitario»[35].

Questa impostazione è corroborata dall'orientamento, relativo all'interpretazione dell'art. 8 CEDU, della Corte europea dei diritti dell'uomo, secondo cui «*the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the*

---

[32] BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit.*, *sub* art. 4(15), 221.

[33] Considerando 10 della Direttiva: «Le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto comunitario; […] pertanto il ravvicinamento di dette legislazioni non deve avere per effetto un indebolimento della tutela da esse assicurata ma deve anzi mirare a garantire un elevato grado di tutela nella Comunità».

[34] BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit.*, *sub* art. 4(15), 221

[35] Corte giust. UE, 8.4.1992, causa C-62/90, in *Riv. it. dir. pubbl. comunit.*, 1993, 151, punto 23. Cfr. GÓMEZ ÁLVAREZ, *La protección de los datos de carácter personal relativos a la salud en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, in *Derecho y Salud*, Vol. 27, Extraordinario XXVI Congreso, 2017, 238 ss., spec. 248 s

Convention (art. 8). Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general»[36].

La giurisprudenza eurounitaria successiva ha proseguito nel percorso tracciato dalla Corte di giustizia, per segnare i confini dell'espressione 'dati relativi alla salute', dandone un'interpretazione in senso negativo. Così è stato con il caso *Dionyssopoulou*, riguardante, fra l'altro, la questione se un riferimento a 'limitazioni personali' in un rapporto informativo del Consiglio dell'Unione europea circa uno dei suoi dipendenti potesse reputarsi come un dato sulla salute del dipendente stesso, in relazione alle disposizioni del reg. Ce n. 45 del 2001. Il Tribunale, in quella circostanza, statuì che questo tipo di informazione non costituisce dato relativo alla salute, non potendo considerarsi tale una qualsivoglia espressione che non disveli alcuna informazione sulle condizioni di salute o sanitarie della persona[37].

Questi assunti furono ribaditi nella pronuncia del Tribunale, del 3 dicembre 2015, per cui «dalla giurisprudenza risulta che all'espressione "dati relativi alla salute" occorre dare un'interpretazione ampia, tale da comprendere informazioni concernenti tutti gli aspetti, tanto fisici quanto psichici, della salute di una persona […]. Tuttavia, questa nozione non può essere ampliata sino a inglobare espressioni che non comportino la divulgazione di nessun dato relativo alla salute o alla condizione medica di una persona»[38].

Anche a livello nazionale i giudici cercarono elementi per tentare di definire questa categoria di dati personali.

Così, nella decisione della corte d'appello inglese del 28 giugno 2018, i giudici del Regno Unito si espressero sul punto, in relazione a un caso di c.d. *mixed data*. A seguito di un reclamo di un paziente verso il suo medico di base per aver ritardato l'inizio dei trattamenti contro un tumore alla vescica, il *General Medical Council* (GMC) fece svolgere un'indagine da un esperto incaricato, che redasse un rapporto. La relazione concludeva nel

[36] Corte EDU, 25.2.1997, n. 22009/93, *Z. c. Finlandia*, in *Diritti dell'uomo e libertà fondamentali*, 2006, 575, punto 95. V. anche Corte EDU, 27.8.1997, n. 20837/92, *M.S. c. Svezia*, *ivi*, 628, punto 41, e Corte EDU, 17.7.2008, n. 20511/03, *I. c. Finlandia*, in *www.hudoc.echr.coe.int*, punto 38.

[37] «*Il suffit de relever, à cet égard, que l'expression "contraintes personnelles" n'entraîne la divulgation d'aucune donnée relative à la santé ou à la condition médicale de la requérante et ne constitue nullement une donnée à caractère personnel au sens de l'article 1er, paragraphe 1, et de l'article 2 du règlement n° 45/2001*». Corte giust. UE (Tribunale), 31.5.2005, causa T-105/03 (*Dionyssopoulou*), in *www.curia.europa.eu*, punto 33.

[38] Corte giust. UE (Tribunale), 3.12.2015, causa T-343/13, in *Foro amm.*, 2015, 3039, punto 50.

senso che, nelle medesime circostanze, la maggior parte dei medici generici non avrebbe sospettato il cancro. Il paziente poi chiese una copia per intero della relazione e il GMC accolse la sua richiesta, come domanda di accesso. Sulla base della considerazione per cui nel suddetto rapporto erano contenuti dati personali non solo del paziente, ma anche del medico, quest'ultimo chiese ed ottenne un'ingiunzione per impedirne la divulgazione da parte del GMC. Tuttavia la pretesa non fu accolta sulla base delle specifiche caratteristiche dei dati contenuti nella relazione, notando che si trattava sì di dati sensibili del paziente, in particolare di dati inerenti alla sua salute, ma che erano anche dati connessi o in qualche maniera riguardanti pure il medico e su questo versante non potevano qualificarsi allo stesso modo come sensibili[39].

Pure la Cassazione ha nel tempo più volte affrontato il problema dei confini definitori di questa particolare categoria di dati personali.

Nella sentenza n. 18980 del 2013, relativa a un caso di pubblicazione, da parte di un'amministrazione comunale, nell'albo pretorio nonché sul sito internet istituzionale, dei dati personali di un proprio dipendente, assente "per malattia", ritenne che costituisse diffusione di un dato sensibile quella sull'assenza dal lavoro di un dipendente appunto per malattia, poiché questa informazione, pur non facendo riferimento a specifiche patologie, è comunque suscettibile di rivelare lo stato di salute dell'interessato[40].

Con la sentenza n. 10280 del 2015, invece, la Sezione terza della Cassazione reputò che il riferimento alla legge 25 febbraio 1992, n. 210, recante "Indennizzo a favore dei soggetti danneggiati da complicanze di tipo irreversibile a causa di vaccinazioni obbligatorie, trasfusioni e somministrazioni di emoderivati", pure contenuto nell'estratto conto quale causale del bonifico, non fosse da considerare un dato idoneo a rivelare lo stato di salute della persona, in quanto le provvidenze previste dalla legge sarebbero state erogate sia «a coloro che hanno patito un'infezione per effetto di trasfusione o vaccinazione», sia «ai prossimi congiunti di persone decedute a causa dell'infezione da trasfusione o vaccinazione»[41]. E aggiunse che «l'"idoneità" d'un dato sensibile a rivelare stati personali va

[39] UK Court of Appeal, *B v The General Medical Council*, 28 giugno 2018, England and Wales Court of Appeal (Civil Division), in *www.bailii.org*, punto 81. Il parere di Lady Justice Arden è concordante, v. punto 96.

[40] Cass., 8.8.2013, n.18980, in *CED Cassazione*, 2013.

[41] «I beneficiari della prima categoria sono ovviamente persone malate; i beneficiari appartenenti alla seconda categoria invece non lo sono. Pertanto l'informazione secondo cui taluno sia percettore di un "assegno ex L. n. 210 del 1992", da sola, è inidonea a rivelare lo stato di salute del percettore, giacché l'erogazione potrebbe avvenire tanto in via diretta, quanto in via - per così dire - di "reversibilità", ed in questo secondo caso l'elargizione dipende non da una malattia dell'*accipiens*, ma da una malattia del suo dante causa». Cass.,

valutata in base al contenuto oggettivo di esso, e non certo in base all'opinione od al pregiudizio che il pubblico possa concepire in merito».

Di segno opposto era stata la sentenza resa dalla Cassazione, Sezione prima, l'anno precedente. Con la sentenza n. 10947 del 2014, i giudici di legittimità ritennero infatti che il dato riguardante la l. n. 210/1992, comunicato dalla Regione all'istituto di credito e da questo inserito nell'estratto conto mensile inviato al correntista, fosse dato sensibile, relativo allo stato di salute. Perciò il trattamento dei dati effettuato da detti soggetti qualificati, senza aver adottato le tecniche di cifratura di cui all'art. 22, comma 6°, del Codice della privacy – articolo oggi abrogato dal d.lgs. n. 101/2018 – fu ritenuto illecito[42].

Intervennero dunque le Sezioni unite, con sentenza n. 30984 del 2017, giungendo a conclusioni aderenti a quest'ultimo orientamento. «I dati desumibili dal richiamo alla L. n. 210 del 1992 sono personali in quanto relativi ad una persona fisica identificata […] e sensibili perché aventi un contenuto idoneo a rivelare lo stato di salute della persona identificata […]. Deve, infine, essere precisato […] che la dizione "pagamento rateo arretrati bimestrali e posticipati L. n. 210 del 1992" contiene la rivelazione del dato personale sensibile riguardante la salute del ricorrente in quanto la periodicità della corresponsione, desumibile inequivocamente dal testo come sopra descritto, non può che riguardare il soggetto affetto dalle patologie cui l'indennità si riferisce e non i suoi familiari-eredi ai quali la legge riconosce un importo a titolo di *una tantum*»[43].

Il Garante europeo della protezione dei dati, nel Progetto di parere sulla proposta di direttiva concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera del 2008, riconosceva l'assenza di una definizione nella Direttiva del 1995 e sosteneva, richiamando il documento del Gruppo di lavoro "Articolo 29" del 2007, sul trattamento dei dati relativi alla salute nelle cartelle cliniche elettroniche[44], che «generalmente se ne dà un'interpretazione ampia, che spesso definisce i dati sanitari come

---

20.5.2015, n. 10280, cit. Sull'attività di trattamento di dati posta in essere dagli istituti di credito, cfr. FRAU, *Il trattamento dei dati personali nell'attività bancaria*, in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., 627 ss. In giurisprudenza v. anche Cass. (ord.), 13.1.2021, n. 368, in *DeJure*.

[42] Cass., 19.5.2014, n. 10947, in *Foro it.*, 2015, I, 121; in *Fam. e dir.*, 2016, 468 ss., con nota di ASTIGGIANO, *Illecito trattamento di dati supersensibili e risarcimento del danno*. V. A. RICCI, *Causali di pagamento e tutela della riservatezza. A proposito di un recente contrasto interpretativo*, in *Riv. dir. comm. e dir. gen. obbl.*, 2017, 619 ss.

[43] Cass., sez. un., 27.12.2017, n. 30984, cit. Commenta l'ordinanza di rimessione, Cass., 9.2.2017, n. 3455, spiegando la vicenda, il contrasto giurisprudenziale e le prospettive dottrinali F. PIRAINO, *Il contrasto sulla nozione di dato sensibile, sui presupposti e sulle modalità del trattamento*, cit., 1232 ss.

[44] Gruppo Articolo 29, *Documento di lavoro sul trattamento di dati personali relativi alla salute nelle cartelle cliniche elettroniche (EHR)*, cit., 7.

dati personali che hanno un legame esplicito e stretto con la descrizione dello stato di salute di una persona»[45].

Come evidenziato dal Gruppo di lavoro "Articolo 29", nel menzionato *advice paper* sulle categorie particolari di dati personali del 2011, questa categoria di dati, considerato anche il gran numero di informazioni che possono essere ad essa ricondotte, rappresenta una delle aree più complesse dei dati sensibili e in cui gli Stati membri mostrano una particolare mancanza di certezza del diritto[46]. Il vario modo di intendere questo tipo di dati a livello nazionale si traduceva in soluzioni normative differenti, che rendevano il quadro delle discipline negli ordinamenti europei frastagliato, quando non confuso[47].

Il reg. Ue n. 679 del 2016 è venuto quindi a porre rimedio a tale situazione, dettando una definizione. Ai sensi dell'art. 4, n. 15), si intendono per «"dati relativi alla salute": 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»[48]. Identiche a quelle del Regolamento del 2016 sono le definizioni dettate dall'art. 3, n. 19), reg. Ue n. 1725 del 2018 (c.d. EUDPR)[49], e dall'art. 3, n. 14), dir. Ue n. 680 del 2016 (c.d. LED), così come quella dell'art. 2, n. 21), reg. Ue n. 1939 del 2017[50].

La definizione data dal Regolamento 2016/679 è stata il frutto di una elaborazione e di un confronto anche a livello istituzionale. Di dati relativi alla salute, infatti, furono proposte differenti soluzioni definitorie. Nel testo della proposta di Regolamento della Commissione, secondo l'art. 4, n. 12), per dati relativi alla salute si intendeva «qualsiasi informazione attinente alla salute fisica o mentale di una persona o alla prestazione di servizi sanitari a detta persona»[51]. Con la Risoluzione del 12 marzo 2014, il Parlamento europeo intervenne sull'enunciato eliminando la parola 'informazione' e sostituendola con l'espressione 'dato

[45] Progetto di parere del garante europeo della protezione dei dati (GEPD) sulla proposta di direttiva del Parlamento europeo e del Consiglio concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (2009/C 128/03), cit., par. 15.

[46] Gruppo Articolo 29, *Advice paper on special categories of data ("sensitive data")*, cit., 10.

[47] Sulla prospettiva francese si v. DE LAMBERTRIE, *Qu'est-ce qu'une donnée de santé?*, in *Le droit des données de santé*, numero speciale di *Revue générale de droit medical*, 2004; ZORN-MACREZ, *Données de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, Nancy, 2010.

[48] C. PERLINGIERI, *eHealth and Data, op. cit.*, 128 ss.

[49] V. il considerando 5 del reg. Ue 2018/1725, cit.

[50] Regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, *relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea («EPPO»)*, modificato dal Regolamento delegato della Commissione n. 2153 del 2020.

[51] Proposta della Commissione di Regolamento del Parlamento europeo e del Consiglio *concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, COM(2012) 25 gennaio 2012

personale'[52]. Il Consiglio nel 2015 propose una definizione di dati relativi alla salute in parte diversa: «dati attinenti alla salute fisica o mentale di una persona, che rivelano informazioni relative al suo stato di salute»[53].

Il testo definitivo del Regolamento, infine, ha coniugato le formulazioni definitorie avanzate da tutte le istituzioni. La definizione dettata dall'art. 4 del Regolamento infatti è ampia. Il legislatore eurounitario ha voluto così includere un numero elevato di informazioni personali nella nozione di dato relativo alla salute, estendendone la disciplina a più casi possibili e allo stesso tempo recependo in questo modo gli indirizzi giurisprudenziali della Corte di giustizia e della Corte europea dei diritti dell'uomo[54].

Le possibilità applicativo della nozione sembrano poi amplificate da quanto enunciato al considerando 35. «Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio[55]; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un

---

[52] Risoluzione legislativa del Parlamento europeo del 12 marzo 2014 sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamentodei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

[53] Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) - Elaborazione di un orientamento generale, Fascicolo interistituzionale: 2012/0011 (COD), 11 giugno 2015, p. 79. Il testo è consultabile in *data.consilium.europa.eu*.

[54] BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit.*, *sub* art. 4(15), 222. Cfr. FARES, *The processing of personal data concerning health according to the EU Regulation*, in ID. (a cura di), *The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis*, Torino, Giappichelli, 2021, 17 ss., spec. 19 ss. Offre un approccio per chiarire come intendere il dato relativo alla salute, nelle sue 'zone grigie' di interpretazione, SCHÄFKE-ZELL, *Revisiting the definition of health data in the age of digitalized health care*, in *International Data Privacy Law*, vol. 12, n. 1, 2022, 33 ss.

[55] Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, *concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera*.

ospedale, un dispositivo medico o un test diagnostico in vitro»[56].

Nell'esemplificazione e nella riflessione su quali fossero qualificabili come dati relativi alla salute si era speso il Gruppo di lavoro "Articolo 29" nel 2015[57] che aveva individuato un primo gruppo di dati personali ascrivibili senza dubbio alcuno alla categoria dei dati relativi alla salute, ossia i dati inerenti allo stato di salute fisico o mentale di un interessato generati in un contesto professionale, medico. In questo gruppo, che chiamava 'dati medici' (*medical data*), includeva tutti i dati connessi ai contatti di esercenti le professioni sanitarie con individui e le loro diagnosi o i loro trattamenti sanitari e ogni informazione correlata su malattie, disabilità e storia clinica, oltre ai dati generati da dispositivi o applicazioni utilizzati in queste circostanze.

Il Gruppo di lavoro precisava però che i 'dati medici' non sono la sola tipologia di dati personali rientrante nel concetto di dati relativi alla salute. Esso si estende, infatti, ad altre informazioni.

Così è dato relativo alla salute il dato circa il fatto che una donna si sia rotta una gamba, come si era affermato nel caso *Lindqvist*, oppure il fatto che un individuo porti gli occhiali o le lenti a contatto. Altri esempi di dati relativi alla salute, forniti dal Gruppo di lavoro, sono le informazioni sulla capacità emotiva o intellettiva, come il quoziente intellettivo, le informazioni sulle abitudini di bere o fumare, quelle sulle allergie comunicate a soggetti privati, come le compagnie di voli aerei, o a enti pubblici, come le scuole, l'appartenenza a un gruppo di supporto per pazienti, come un gruppo di supporto a malati di cancro, o a gruppi diversi, anche privati, ma con obiettivi legati alla salute personale o il semplice fatto che qualcuno sia malato in un ambiente lavorativo. A questi si aggiungono, nel contesto amministrativo, i dati sulla condizione di salute comunicati a enti pubblici a fini fiscali o per agevolazioni. Anche i dati relativi all'acquisto di prodotti, dispositivi e servizi medici, possono considerarsi dati sulla salute, se da essi si può evincere uno stato di salute personale,

[56]Da questa descrizione, peraltro, si evince che il materiale biologico da cui vengono fatti derivare i dati sulla salute non è da considerare in sé un dato relativo alla salute e nemmeno un dato personale. BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit.*, *sub* art. 4(1), 112; IID., *ivi*, *sub* art. 4(15), 223. In relazione ai dati biometrici, secondo il Gruppo Articolo 29, *Parere 4/2007 sul concetto di dato personale*, cit., 9, «i campioni di tessuti umani (un campione di sangue) sono fonti da cui vengono estratti dati biometrici, ma non sono di per sé dati biometrici (le impronte digitali sono dati biometrici, non il dito)». Con un richiamo a tale documento, il concetto è ribadito sempre dal Gruppo Articolo 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, 27 aprile 2012, WP193, 4. V., a livello nazionale, quanto espresso dal Garante per la protezione dei dati personali, Provvedimento del 21 giugno 2007, *Campione biologico e dato personale genetico*, consultabile in *www.garanteprivacy.it*.

[57] Gruppo Articolo 29, *Annex – Health data in apps and devices*, in *www.ec.europa.eu*, 5 febbraio 2015.

e lo stesso vale per i dati sulla partecipazione ad alcuni test di *screening* selettivamente eseguiti, come può avvenire per l'Aids o altre malattie sessualmente trasmissibili o malattie rare.

Nel suddetto Progetto del 2008, il Garante europeo della protezione dei dati affermava che, oltre ai 'dati medici' (ad es. impegnative e prescrizioni del medico, referti medici, esami di laboratorio, radiografie, ecc.), si annoverano fra i dati sanitari anche 'dati finanziari' e 'dati amministrativi' concernenti la salute (ad es. documenti relativi ai ricoveri ospedalieri, numero di sicurezza sociale, calendario delle consultazioni mediche, fatture delle prestazioni di servizi di assistenza sanitaria, ecc.)[58].

Secondo quanto illustrava il Gruppo di lavoro "Articolo 29" nel 2015[59], non necessariamente poi il dato relativo alla salute deve connotarsi nel senso di una patologia. Possono infatti qualificarsi come tali anche le informazioni sulle analisi del sangue o delle urine, indipendentemente dal fatto che rientrino o meno nelle soglie del non patologico, o le informazioni raccolte in questionari online allo scopo di fornire consigli sulla salute, a prescindere da quello che effettivamente indica l'interessato.

Dati relativi alla salute possono essere anche i dati sulle condizioni di salute della persona generati da applicazioni o dispositivi, a prescindere dalla qualificazione di prodotti sanitari attribuita a detti dispositivi o applicazioni o dall'uso da parte di professionisti della sanità o meno, come, ad esempio, il dato originato da un dispositivo di misurazione del glucosio, che avverte se il livello di glucosio è troppo elevato e sollecita l'utente ad attivarsi. Ma ci possono essere anche dati, pur generati da applicazioni sullo stile di vita dell'individuo, che generalmente non si annoverano fra i dati sulla salute. Si tratta di informazioni grezze da cui non è possibile ricavare ragionevolmente alcuna conclusione sullo stato di salute dell'interessato. L'esempio portato dal Gruppo di lavoro era quello del numero di passi conteggiati da un'applicazione durante una camminata: questi dati, non

---

[58] Progetto di parere del garante europeo della protezione dei dati (GEPD) sulla proposta di direttiva del Parlamento europeo e del Consiglio concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (2009/C 128/03), cit., par. 15. Sembra peraltro opportuno un chiarimento terminologico. Le espressioni 'dati relativi alla salute' e 'dati sanitari' vengono utilizzate molto spesso come sinonimi e così anche nel presente lavoro. Ciononostante è bene tenere presente la diversa sfumatura semantica delle due espressioni: a rigore, stando al significato di queste parole, qualificando un dato come sanitario lo si accosta alla 'sanità' e al suo ambito, con riferimento specialmente al piano pubblico e amministrativo e alla dimensione organizzativa dei servizi per la salute degli individui e della collettività, mentre è solo parlando in termini di relazione con la salute che si riconosce specificamente l'informazione inerente alla persona, alla sua condizione, al suo vissuto e alla sua identità. Cfr. CAPILLI, *Diritto privato sanitario. Fondamenti*, Pisa, Pacini, 2022, 43 ss.

[59] Gruppo Articolo 29, *Annex – Health data in apps and devices*, cit

combinandosi con altre informazioni sull'interessato e in assenza di un contesto medico specifico in cui utilizzarli, non vengono ad avere un impatto significativo sulla riservatezza del soggetto e non richiedono quindi la protezione prevista per i dati sensibili[60]. Sono dati relativi alla salute invece i dati sul rischio di sviluppare una malattia: si tratta, per il Gruppo di lavoro "Articolo 29", di informazioni inerenti alla potenziale condizione di salute futura di un individuo. Così vengono inclusi nella nozione di dati sulla salute le informazioni relative all'obesità, alla pressione sanguigna, alle predisposizioni ereditarie o genetiche, l'eccessivo consumo di alcol, l'uso di droghe o qualsiasi altra informazione per cui esiste un rischio di malattia scientificamente provato o comunemente percepito. Si includono anche i dati personali usati allo scopo di identificare un rischio di sviluppare una malattia, come quando si faccia ricorso a nuove correlazioni tra fattori e patologie, per esempio nel campo della ricerca.

Esistono poi dati non relativi alla salute che, se utilizzati in particolari maniere o se combinati con altri dati personali, finiscono per ricadere nell'ambito dei dati sanitari[61]. L'esempio, che forniva il Gruppo di lavoro "Articolo 29", era quello dell'analisi condotta sui *social media* per comprendere quando gli individui possono soffrire di depressione: anche se non si possono qualificare come dati relativi alla salute i messaggi 'tristi' inviati dagli utenti, una loro analisi sistematica per fini associati a diagnosi o prevenzione o di ricerca si può considerare trattamento di dati sulla salute. Lo stesso vale per i dati sullo stile di vita raccolti dalle applicazioni che si usano anche quotidianamente.

Inoltre, quando possono trarsi conclusioni circa la salute di una persona, indipendentemente dalla loro affidabilità, anche queste conclusioni devono reputarsi dati relativi alla salute[62].

La categoria dei dati sulla salute, inoltre, assume contorni molto più sfumati se considerata accanto a quelle di dati genetici e biometrici. Può essere anche molto difficile, se non impossibile talvolta, trovare un'esatta linea di confine tra queste informazioni, poiché le

---

[60] V. WEICHERT, *Die Verarbeitung von Wearable-Sensordaten bei Beschäftigten*, in *Neue Zeitschrift für Arbeitsrecht*, 2017, 565 ss. Cfr. DE FRANCESCHI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 4, reg. Ue n. 679/2016, 171.

[61] Cfr. MALGIERI e COMANDÉ, *Sensitive-by-distance: quasi-health data in the algorithmic era*, in *Information & Communications Technology Law*, vol. 26, n. 3, 2017, 229 ss.

[62] Ma, *ivi*, 172: «Onde non ampliare in misura eccessiva l'ambito di tutela, è necessario fare riferimento alle circostanze del caso concreto. È ad esempio rilevante se vengano trasmesse, direttamente o indirettamente, informazioni in merito alla salute dell'interessato. Non può ad esempio qualificarsi come dato sanitario l'informazione in merito al fatto che l'interessato abbia stipulato un'assicurazione sanitaria, così come la fotografia contenuta nel passaporto di un portatore di occhiali da vista».

loro nozioni – come si vedrà in seguito– tendono a sovrapporsi. In ogni caso, tali incertezze liminari non sembrano avere carattere problematico[63], almeno all'interno del sistema del diritto eurounitario[64].

Dobbiamo infine sempre tenere presente che l'area di informazioni che rientrano nella definizione di dati relativi alla salute è suscettibile di modificazioni, principalmente ad opera dell'evoluzione scientifica e tecnologica, specialmente in aumento. In altri termini, ciò che oggi si può ben ritenere non sussumibile nella fattispecie 'dato relativo alla salute', in futuro, per i nuovi significati che ogni segno può assumere, potrebbe essere, invece, incluso nella categoria.

1.1. *Sensibilità del dato relativo alla salute*

I dati relativi alla salute sono da sempre considerati dati sensibili. L'affermazione trova riscontro nella tradizionale regolamentazione circa la tenuta dei registri sanitari e delle cartelle cliniche da parte del personale medico[65].

Le informazioni sulla salute della persona rivestono un ruolo centrale nel rapporto fra medico e paziente[66], che nel tempo è stato costruito in termini di fiducia e riserbo, abbandonando le impostazioni paternalistiche, retaggio dei secoli passati, per approdare all'edificazione dell'alleanza terapeutica.

In tutto ciò, il linguaggio tecnico proprio della protezione dei dati personali deve cedere il passo alle parole della relazione di cura, in omaggio al rispetto della dignità della persona.

La considerazione dell'identità del paziente, delle sue inclinazioni personali e della sua storia resta tra i fondamenti del suo rapporto con il medico, le funzioni del cui sapere, messo al servizio della persona, si prestano a una costante rilettura, che «consente di delineare un modello di condotta sempre lucidamente governato, sullo sfondo, dal rispetto dei valori della dignità, dell'integrità e dell'identità del malato»[67].

La sensibilità dei dati relativi alla salute si fonda sulla comune percezione che essi

[63] BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit.*, *sub* art. 4(15), 222.

[64] La cosa potrebbe essere invece anche molto diversa nel diritto interno, posto che agli Stati membri l'art. 9, par. 4, del Regolamento assegna un rilevante margine di discrezionalità per disciplinare il trattamento di questi dati.

[65] «*Data concerning the health of natural persons ('health data') have traditionally been regarded as sensitive. This is reflected in long-standing rules to protect the confidentiality of the medical records that doctors keep on their patients – rules that predate the emergence of modern data protection laws*». *Ivi*, 218.

[66] GUARDA, *I dati sanitari*, cit., 591.

[67] PUCELLA, *Autodeterminazione e responsabilità nella relazione di cura*, Milano, Giuffrè, 2010, 84.

rivelino tratti della persona tra i più riservati e intimi e sul timore che il loro disvelamento abbia per conseguenza la discriminazione[68]. Il dato relativo alla salute, come uno dei più fragili frammenti dell'identità personale, è un elemento la cui assenza di controllo da parte dell'individuo e la cui conoscenza da parte di terzi determinano una specifica vulnerabilità di ogni persona.

Ma non tutti i dati personali qualificabili come 'sensibili' sono appunto sensibili allo stesso modo. La giurisprudenza italiana, sia nella prospettiva del giudice ordinario che in quella del giudice amministrativo, abbia ricavato un sottoinsieme di dati sensibili individuando la categoria dei dati '*supersensibili*' o sensibilissimi, in cui rientrano le informazioni sull'orientamento e la vita sessuale e quelle relative alla salute. E proprio all'interno di tale categoria di dati devono operarsi ulteriori distinzioni. Non tutti i dati personali sulla salute hanno infatti lo stesso grado di sensibilità. [69].

Atteso che a diverse tipologie di trattamento di dati possono corrispondere rischi diversi, lo stesso trattamento di dati sanitari, al variare del tipo di informazione relativa alla salute, può non determinare uno stesso rischio per i diritti e le libertà della persona.

Per comprendere meglio si devono prendere in considerazione trattamenti di un medesimo tipo, dal momento che, se il trattamento di dati personali preso a paragone è di per sé diverso, porterà con sé peculiarità anche sul piano dei rischi. Così un trattamento di dati effettuato per mezzo di meri supporti cartacei non presenterà i rischi propri del trattamento svolto con l'impiego degli strumenti informatici. Allo stesso modo, un trattamento posto in essere dal medico curante avrà caratteristiche differenti rispetto a quello realizzato dal datore di lavoro, anche in termini di rischio.

Consideriamo, ad esempio, il trattamento di dati sanitari consistente nella compilazione della cartella clinica. Se le informazioni che si inseriscono nella cartella clinica riguardano un caso di influenza, il trattamento di questi dati – pur sempre sensibili – avrà rischi diversi e minori rispetto all'ipotesi in cui oggetto del trattamento, cioè di quella compilazione, siano

---

[68] BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit.*, *sub* art. 4(15), 218.

[69] «*Other categories of data display major differences in the degree of sensitivity. For example, health data may range from information about a simple cold to stigmatizing information about illnesses or disabilities*». Gruppo Articolo 29, *Advice paper on special categories of data ("sensitive data")*, cit., 8. Sui diversi livelli di sensibilità, pur nella prospettiva italiana del Codice della privacy, anteriore all'entrata in vigore del Regolamento, cfr. CAGGIA, *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 407 ss. Ma v. già ZATTI, *Il diritto all'identità e l'«applicazione diretta» dell'art. 2 Cost.*, cit., 59.

informazioni inerenti a un paziente malato di Aids.

A fronte di informazioni sulla salute che appaiono del tutto innocue, come possono essere quelle su un episodio di raffreddore o su un'indigestione, esistono dati che invece portano con sé un insieme di considerazioni, valutazioni, correlazioni, raccontano cioè qualcosa di più che la sola condizione di salute della persona o si prestano a interpretazioni singolari anche relativamente al contesto sociale che possono raggiungere.

Alcuni dati relativi alla salute sono più sensibili di altri perché, per il tipo di informazione che veicolano, se trattati, possono divenire di serio rischio per le libertà e i diritti fondamentali della persona.

Il 'gradiente' di sensibilità dei dati sanitari sembra quindi muoversi su una linea che va oltre al mero diritto alla riservatezza della persona, sostanziandosi nel criterio del minor o maggior rischio per le libertà e i diritti inviolabili dell'individuo, coerentemente con la funzione antidiscriminatoria del divieto di trattamento dei dati sensibili.

Pensiamo all'informazione sull'infezione da HIV. A tal proposito, la raccomandazione adottata dal Comitato dei ministri del Consiglio d'Europa, il 24 ottobre 1989, richiedeva l'osservanza della più alta confidenzialità nei più svariati settori e, nello specifico, da parte delle autorità sanitarie in relazione alla segnalazione dei casi, al rapporto con gli esercenti le professioni sanitarie e alla notificazione al partner[70].

---

[70] È la Raccomandazione n. R(89)14 *on the Ethical Issues of HIV Infection in the Health Care and Social Settings*, che può consultarsi in *hrlibrary.umn.edu*. Per uno studio su diritti umani e sanità in relazione all'Aids, v. GOSTIN e LAZZARINI, *Human Rights and Public Health in the AIDS Pandemic*, Oxford University Press, 1997, i quali a più riprese evidenziano l'importanza della confidenzialità. Anche nella Risoluzione dell'Assemblea parlamentare del Consiglio d'Europa 1536(2007), *HIV/AIDS in Europe*, consultabile in *pace.coe.int*, è richiesta la confidenzialità per i pazienti affetti da HIV. I documenti in materia sono diversi. Ci si limita a ricordare in questa sede: dell'Assemblea generale delle Nazioni Unite, la *Declaration of Commitment on HIV/Aids*, adottata nella Sessione speciale su HIV/Aids nel 2001, in *www.unaids.org*, e la Risoluzione del 2 giugno 2006 (A/RES/60/262), *Political Declaration on HIV/AIDS*, in *digitallibrary.un.org*; di *Office of the United Nations High Commissioner for Human Rights and the Joint United Nations Programme on HIV/AIDS*, le *International Guidelines on HIV/AIDS and Human Rights*, nella versione consolidata del 2006, in *www.ohchr.org*; dell'Assemblea parlamentare del Consiglio d'Europa, in *pace.coe.int*, la Risoluzione 812(1983), *Acquired immune deficiency syndrome (AIDS)*, la Raccomandazione 1080(1988), *Coordinated European health policy to prevent the spread of AIDS in prisons*, la Raccomandazione 1116(1989), *Aids and human rights*, la Risoluzione 1399(2004) e la Raccomandazione 1675(2004), *European strategy for the promotion of sexual and reproductive health and rights*; le Comunicazioni della Commissione, in *eulex.europa.eu*, *sulla lotta contro l'HIV/AIDS nell'Unione europea e nei paesi vicini, 2006-2009*, COM(2005) 654 final, del 15 dicembre 2005, *2009 -2013*, COM(2009)569 final, del 26 ottobre 2009. È appena il caso di evidenziare come, al giorno d'oggi, l'informazione circa la sieropositività di una persona può essere dalla stessa svelata – e quindi veicolata – attraverso le applicazioni di incontri. Al riguardo v. GILES, *Digital disclosure: HIV status, mobile dating application design and legal responsibility*, in *Information & Communications Technology Law*, vol. 30, n. 1, 2021, 35 ss. Cfr. ID. *et al*., *Online safety and identity: navigating same-sex male*

La Corte europea dei diritti dell'uomo, richiamando anche tale raccomandazione, nella sentenza del 25 febbraio 1997 – resa nel caso *Z. c. Finlandia* – mise in luce la peculiare delicatezza del dato relativo all'infezione da HIV.

Dopo aver affermato, infatti, la portata essenziale della confidenzialità con riguardo ai dati relativi alla salute, nel rispetto dell'art. 8 CEDU, dichiarò che ciò è «*especially valid as regards protection of the confidentiality of information about a person's HIV infection. The disclosure of such data may dramatically affect his or her private and family life, as well as social and employment situation, by exposing him or her to opprobrium and the risk of ostracism*», sottolinenando «*the highly intimate and sensitive nature of information concerning a person's HIV status*»[71].

A tale rilievo aggiunse che la protezione dei dati personali, in relazione alle informazioni di tipo sanitario, è elemento cruciale non solo per garantire la riservatezza del paziente, ma anche per preservare la sua fiducia nella professione medica e nei servizi sanitari in generale. Perciò la diffusione dei dati su questa condizione di salute, proprio per via delle conseguenze negative che può avere nella vita della persona, «*may also discourage persons from seeking diagnosis or treatment and thus undermine any preventive efforts by the community to contain the pandemic*»[72].

In quel provvedimento la Corte giunse a configurare la violazione del diritto al rispetto della vita privata, sancito dall'art. 8 CEDU, per la pubblicazione nel testo di una pronuncia della Corte d'appello di Helsinki, dopo dieci anni, dei dati personali, compresa la sua precisa identità, e delle informazioni mediche relative ad un soggetto estraneo al processo e

---

social "dating" apps and networks, in *Information & Communications Technology Law*, vol. 31, n. 3, 2022, 269 ss.

[71] Corte EDU, 25.2.1997, n. 22009/93, *Z. c. Finlandia*, cit., punto 96. Il caso viene pure riportato da AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI, CORTE EUROPEA DEI DIRITTI DELL'UOMO E CONSIGLIO D'EUROPA (a cura di), *Manuale sul diritto europeo in materia di protezione dei dati*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea, 2018, 375. V. L. TOMASI, nel *Commentario breve alla Convenzione europea dei diritti dell'uomo Bartole De Sena Zagrebelsky*, 2012, *sub* art. 8, 316. Cfr. ANGIOLINI, *Health and Data Protection*, in IAMICELI, CAFAGGI e ANGIOLINI (a cura di), *Casebook Judicial Protection of Health as a Fundamental Right*, Roma, Scuola Superiore della Magistratura, 2022, 126 ss.; MAQUEO RAMÍREZ, MORENO GONZÁLEZ e RECIO GAYO, *Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario*, in *Revista de Derecho*, vol. 30, n. 1, 2017, 86 s.

[72] V. punto 96 della sentenza. Al punto 95 la Corte ribadiva che, senza l'adeguata protezione dei dati relativi alla salute, «*those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community*».

intenzionato a mantenerli riservati per un periodo più lungo[73].

Gli assunti espressi in quella pronuncia furono poi ribaditi dalla Corte con la sentenza del 17 luglio 2008, nel caso *I. c. Finlandia*. Le considerazioni sull'importanza della protezione dei dati relativi alla salute sono state reputate «*especially valid as regards protection of the confidentiality of information about a person's HIV infection, given the sensi tive issues surrounding this disease. The domestic law must afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention*»[74].

La particolarità di quel caso è che si trattava di una mancanza di accorgimenti a tutela della riservatezza dei propri dipendenti, da parte di una struttura sanitaria pubblica. Una donna lavorava come infermiera a tempo determinato in un ospedale e presso lo stesso si curava per la sua infezione da HIV. Nel 1992 iniziò a sospettare che i suoi colleghi fossero a conoscenza della sua patologia, dal momento che i dipendenti dell'ospedale avevano allora libero accesso al registro dei pazienti, in cui erano contenute informazioni sulle diagnosi e sui medici che eseguivano il trattamento. Nonostante il suo registro fosse stato in seguito modificato in modo da garantire un maggior riserbo su sua richiesta, nel 1995 il suo contratto di lavoro non venne rinnovato. Dopo il fallimento della sua richiesta di sapere i nominativi di chi aveva effettuato l'accesso al suo registro in ospedale, per via dell'impossibilità di risalire a queste identità da parte del sistema, che consentiva di vedere solo le ultime cinque consultazioni, nel 1998 la struttura modificò i propri registri permettendo la conoscibilità di ogni accesso agli stessi. Non trovando poi accoglimento, dinanzi all'autorità giudiziaria interna, la domanda di risarcimento del danno avanzata dalla donna verso l'autorità distrettuale sanitaria, principalmente perché si ritenne non dimostrato il nesso causale fra le carenze nelle norme di sicurezza per l'accesso e la divulgazione dell'informazione sulla sua condizione di salute, ella fece ricorso alla Corte europea dei

[73] Per un'analisi della giurisprudenza della Corte europea dei diritti dell'uomo, circa l'applica zione dell'art. 8 CEDU con riguardo al trattamento dei dati sanitari, v. FARES, *The processing of personal data concerning health according to the EU Regulation*, cit., 32 ss. e 37 ss. E' opportuno sottolineare come le informazioni sulla salute di un individuo possano intersecarsi ad altre categorie particolari di dati, come, ad esempio, quelli inerenti all'orientamento sessuale e alla vita sessuale. Cfr. Corte EDU, 8.9.2022, nn. 3153/16 e 27758/18, *Drelon c. Francia*, in *www.dirittoegiustizia.it*, 8 settembre 2022, con nota di MILIZIA, *Rifiutato come donatore di sangue per presunta omosessualità: la CEDU riconosce la lesione della privacy*, che ha accertato la violazione dell'art. 8 CEDU in occasione della raccolta e della conservazione dei dati personali riguardanti il ricorrente da parte dell'*Établissement français du sang*. Il soggetto era stato escluso dalla donazione di sangue sulla base del rifiuto a fornire informazioni sulla sua sessualità: da questo, infatti, per speculazioni e presunzioni, si erano ricavati dati su orientamento e vita sessuale dello stesso.

[74] Corte EDU, 17.7.2008, n. 20511/03, *I. c. Finlandia*, cit., punto 38. Cfr. L. TOMASI, *op. cit.*, 316, nonché ANGIOLINI, *Health and Data Protection*, cit., 126 ss.

diritti dell'uomo, lamentando la violazione dell'art. 8 CEDU.

Nell'accogliere la domanda della ricorrente, la Corte rilevò che, posto che richiedere la dimostrazione di quel nesso eziologico era estremamente gravoso per la paziente e la sua posizione di svantaggio in ordine all'onere della prova era dipesa dagli stessi deficit organizzativi della struttura, il semplice fatto che la normativa nazionale fornisse alla ricorrente la possibilità di chiedere il risarcimento dei danni causati da una presunta divulgazione illecita di dati personali non era sufficiente a tutelare la sua vita privata. In tale contesto, infatti, è necessaria una «*practical and effective protection*» per escludere qualsiasi possibilità di accesso non autorizzato, che non fu data in quel caso[75]. «*The need for sufficient guarantees is particularly important when processing highly intimate and sensitive data, as in the instant case, where, in addition, the applicant worked in the same hospital where she was treated*»[76].

Non si tratta di pronunce isolate, anzi, l'orientamento espresso da questi provvedimenti è stato ripreso anche da ulteriore giurisprudenza della Corte europea dei diritti dell'uomo, come, ad esempio, nella sentenza del 2 ottobre 2012, sul caso *Mitkus c. Lettonia,* e in quelle del 25 novembre 2008, relative ai casi *Armonienė c. Lituania* e *Biriuk c. Lituania*[77].

Anche il diritto interno conosce disposizioni speciali, per la tutela della riservatezza della persona affetta da questa patologia[78]. Nell'ordinamento italiano, per quanto attiene nel dettaglio all'informazione sulla sieropositività[79], il testo dei commi 1° e 2° dell'art. 5, l. n. 135 del 1990, recante "Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS", come modificati dall'art. 178, d.lgs. n. 196 del 2003[80] recita: «l'operatore sanitario e ogni altro soggetto che viene a conoscenza di un caso di AIDS, ovvero di un caso di infezione da HIV, anche non accompagnato da stato morboso, è tenuto a prestare la

[75] V. i punti 44-47 della sentenza.
[76] Punto 40 della sentenza
[77] Ci si riferisce rispettivamente a Corte EDU, 2.10.2012, n. 7259/03, *Mitkus c. Lettonia*; Corte EDU, 25.11.2008, n. 36919/02, *Armonienė c. Lituania;* Corte EDU, 25.11.2008, n. 23373/03, *Biriuk c. Lituania*,tutte consultabili in *www.hudoc.echr.coe.int*. È appena il caso di evidenziare come in tutte queste pronunce si faccia richiamo alla menzionata Raccomandazione n. R(89)14 del Consiglio d'Europa. Cfr. L. TOMASI, *op. cit*., 317.
[78] Richiamava la problematica anche RODOTÀ, *Tecnologie e diritti*, cit., 118. Cfr. LOSANO, *Dei diritti e dei doveri: anche nella tutela della privacy*, cit., V ss.
[79] V., anche per i riferimenti alla letteratura nordamericana, DI CIOMMO, *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e resp*., 2002, 121 ss., spec. 127 s.; ID., *La privacy sanitaria*, in PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003, 316 ss. Cfr. CASONATO, *Diritto alla riservatezza e trattamenti sanitari obbligatori: un'indagine comparata*, Università degli Studi di Trento, 1995, 225. In relazione a un caso concreto, CASONATO, Privacy *e AIDS. Il punto di vista giuridico*, in FUNGHI *et al*. (a cura di), *Medicina, bioetica e diritto. I problemi e la loro dimensione normativa*, 2a ed., Pisa, Edizioni ETS, 2013, 454 ss.
[80] L'articolo 178 è stato poi abrogato dall'art. 27, comma 1°, lett. *c*, n. 3), d.lgs. n. 101 del 2018.

necessaria assistenza e ad adottare ogni misura o accorgimento occorrente per la tutela dei diritti e delle libertà fondamentali dell'interessato, nonché della relativa dignità. Fatto salvo il vigente sistema di sorveglianza epidemiologica nazionale dei casi di AIDS conclamato e le garanzie ivi previste, la rilevazione statistica della infezione da HIV deve essere comunque effettuata con modalità che non consentano l'identificazione della persona. La disciplina per le rilevazioni epidemiologiche e statistiche è emanata con decreto del Ministro della salute, sentito il Garante per la protezione dei dati personali che dovrà prevedere modalità differenziate per i casi di AIDS e i casi di sieropositività»[81].

Ma il dato circa la sieropositività non è l'unico esempio di dato relativo alla salute che presenta un livello di sensibilità superiore. Esistono infatti anche altre informazioni di tipo sanitario che, se trattate, possono comportare un rischio serio per le libertà e i diritti fondamentali della persona. Così è, ad esempio, per il dato inerente all'interruzione della gravidanza, a episodi di violenza sessuale o di pedofilia, all'utilizzo di sostanze stupefacenti, di sostanze psicotrope e di alcool, a patologie psichiatriche.

Si tratta di informazioni che, pur appartenendo al novero dei dati relativi alla salute, in quanto idonee a rivelare elementi sulla condizione di salute della persona, non esauriscono il loro potenziale disvelativo nella sfera sanitaria dell'individuo e sue aree limitrofe, ma si estendono a molteplici connotazioni sull'esistenza del soggetto, coinvolgendo contemporaneamente più piani, da quello sociale ed economico, a quello filosofico o religioso, da quello sessuale a quello eventualmente giudiziario, e sostanziandosi anche in aspetti dai contorni talvolta stigmatizzanti[82].

L'assunto fu peraltro messo in luce anche dal Gruppo di lavoro "Articolo 29" nel 2007, pur nel più circoscritto contesto del trattamento di dati operato mediante le cartelle cliniche elettroniche[83].

A riprova di ciò, volgendo per un attimo lo sguardo all'esperienza italiana, si rammenta in questa sede la disposizione dell'art. 5, d.P.C.m. 29 settembre 2015, n. 178, recante il

[81] Ai sensi del comma 4° dell'art. 5, «la comunicazione di risultati di accertamenti diagnostici diretti o indiretti per infezione da HIV può essere data esclusivamente alla persona cui tali esami sono riferiti». Come chiarito poi dal Garante per la protezione dei dati personali, il referto sul test dell'HIV può essere inserito nel fascicolo sanitario elettronico solo dopo che il medico ha comunicato di persona all'interessato l'esito dell'esame. Cfr. la *newsletter* del 22 dicembre 2022, in *www.garanteprivacy.it*.

[82] BONSIGNORI, *AIDS e contagio sessuale: profili penali e civili*, nel *Trattato della responsabilità civile e penale in famiglia*, diretto da Cendon, vol. I, Padova, CEDAM, 2011, 905 ss

[83] «I diversi tipi di dati sulla salute non hanno lo stesso potenziale di arrecare pregiudizio». Gruppo Articolo 29, *Documento di lavoro sul trattamento di dati personali relativi alla salute nelle cartelle cliniche elettroniche (EHR)*, cit., 14.

"Regolamento in materia di fascicolo sanitario elettronico", rinviando per le ulteriori considerazioni sul fascicolo sanitario elettronico stesso a una parte successiva della trattazione. Tale norma, volendo apprestare una garanzia maggiore per le persone che vedano trattati mediante questo strumento informatico particolari dati relativi alla salute, contempla la necessità del «previo esplicito consenso dell'assistito» affinché questi siano resi visibili. Il riferimento è ai dati «disciplinati dalle disposizioni normative a tutela delle persone sieropositive, delle donne che si sottopongono a un'interruzione volontaria di gravidanza, delle vittime di atti di violenza sessuale o di pedofilia, delle persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, delle donne che decidono di partorire in anonimato, nonché i dati e i documenti riferiti ai servizi offerti dai consultori familiari»[84].

A tale riguardo, si deve ricordare che è pure l'insegnamento del giudice delle leggi a richiedere – a maggior ragione in questi casi – che sia garantita la più ampia tutela: la Corte costituzionale, con la sentenza n. 218 del 1994, dichiarò sì incostituzionale la mancanza di un obbligo a sottoporsi ai test di accertamento sul contagio da HIV per gli operatori sanitari, ma constatò anche che, nonostante tali esami dovessero considerarsi necessari a fini di interesse generale, dar corso alla loro esecuzione non avrebbe potuto prescindere dalla salvaguardia della «dignità della persona, che comprende anche il diritto alla riservatezza sul proprio stato di salute e al mantenimento della vita lavorativa e di relazione compatibile con tale stato»[85]. Ancora, la giurisprudenza della Corte europea dei diritti dell'uomo si è espressa in questo senso prendendo in considerazione altri dati relativi alla salute. Con particolare riguardo ai dati relativi alla salute mentale, merita di essere ricordata la sentenza del 27 febbraio 2018, resa nel caso *Mockutė c. Lituania*.

Affetta sin da giovane da disturbi paranoidi, una donna restava fortemente scossa nel 2002 dalla malattia del padre, cui era scoperto un cancro, e le veniva diagnosticato un disturbo post-traumatico da stress. L'anno seguente, mentre era al lavoro come legale negli uffici del Ministero dell'economia lituano, colta da un'acuta crisi di panico, si allontanava in stato

[84] S. CORSO, *Sanità digitale e riservatezza. Interpretazioni sul fascicolo sanitario elettronico*, in A. THIENE e S. CORSO (a cura di), *op. cit.*, 91 ss.

[85] Corte cost., 2.6.1994, n. 218, in *Il diritto della Regione*, 1995, 105 ss., con nota di M. MAGRI, *Corte Costituzionale ed "emergenza sociale": alla ricerca dei grandi principi*; in *Foro it*., 1995, I, 46 ss., con nota di IZZO, *Un difficile test per la Consulta: l'Aids, le leggi ed i giudici fiduciosi*; in *Riv. it. med. leg*., 1995, 241 ss., con nota di INTRONA, *Sieropositività HIV ed idoneità al lavoro*. V. LAMARQUE, *Privacy e salute*, in LOSANO (a cura di), *La legge italiana sulla* privacy. *Un bilancio dei primi cinque anni*, Roma- Bari, Laterza, 2001, 334. Per alcuni spunti relativi alla responsabilità da divulgazione di questi dati, v. G. GLIATTA, *Il diritto alla privacy in ambito medico: trattamento dei dati sensibili e fascicolo sanitario elettronico*, in *La resp. civ.*, 2010, 683, nt. 4.

confusionale e, avendo fatto ritorno nel proprio appartamento, usciva sul balcone e iniziava a gridare. Trasportata quindi, su richiesta dei parenti, all'ospedale psichiatrico di Vilnius, là restava forzatamente ricoverata per più di un mese e in quel periodo le veniva impedito di recarsi presso la sede del gruppo pseudo-religioso d'appartenenza, tentando gli psichiatri curanti di dissuaderla dal persistere nel suo credo sulla base di presunti effetti dannosi per il suo equilibrio psichico. Dopo alcuni giorni, si mandava in onda, su un canale a diffusione nazionale, un servizio su di lei, pur indicandola con uno pseudonimo, ma riportando altri elementi identificativi come il ruolo ricoperto al servizio dello Stato e la malattia del padre. Il servizio rivelava le sue condizioni di salute mentale, la sua adesione al gruppo religioso di Vilnius e la circostanza che, diversamente da altri adepti, sembrava non essere dedita a riti orgiastici e presentare un'iper-sessualizzazione. Le informazioni erano state ottenute dai giornalisti presso la struttura ospedaliera, intervistando il medico che aveva in cura la donna. Esperiti invano tutti gli strumenti di tutela interni, la donna ha proposto ricorso ai giudici di Strasburgo lamentando la violazione, da parte dell'ospedale psichiatrico, oltre che dell'art. 9, per averle impedito materialmente di esercitare il proprio culto nel periodo di degenza e per aver cercato di interferire nelle sue scelte di fede, anche dell'art. 8 CEDU per l'illecita comunicazione di dati relativi alla sua condizione di salute.

Nel riconoscere in questo caso la violazione del diritto al rispetto della vita privata, la Corte ha nuovamante ribadito l'importanza della riservatezza con riguardo alle informazioni inerenti alla salute della persona, oltreché a quelle sulla vita sessuale e sull'integrità morale, aggiungendo che «*information regarding a mental health related condition by its very nature constitutes highly sensitive personal data regardless of whether it is indicative of a particular medical diagnosis*»[86].

Si può quindi affermare che, all'interno della categoria dei dati relativi alla salute, esiste un gruppo più ristretto di dati sanitari il cui grado di sensibilità è estremamente elevato, avendo riguardo in particolar modo alla loro capacità di mettere a serio rischio le libertà e i diritti fondamentali della persona. Tale diverso livello di sensibilità giustifica una disciplina

[86] Corte EDU, 27.2.2018, n. 66490/09, *Mockutė c. Lituania*, punto 94, in *Riv. it. med. leg.*, 2018, 1060 ss., con nota di LAMANUZZI, *La Corte EDU condanna la Lituana per illecito trattamento dei dati sanitari e per violazione della libertà religiosa in danno di una paziente affetta da psicosi.* La Corte prosegue, al punto 95, affermando che «*the disclosure of medical data by medical institutions to a newspaper, to a prosecutor's office and to a patient's employer, and the collection of a patient's medical data by an institution responsible for monitoring the quality of medical care were also held to have constituted an interference with the right to respect for private life*». Cfr. ANGIOLINI, *Health and Data Protection*, cit., 126 ss.

a sé o quantomeno norme specifiche, che possano offrire una tutela adeguata all'individuo[87].

Non si esclude che il novero ristretto di questi dati relativi alla salute, più sensibili degli altri dati sanitari, possa nel tempo variare, ampliandosi, restringendosi o solo mutando le informazioni che lo compongono[88]. Se la scelta della riservatezza massima sia poi la soluzione migliore per combattere lo stigma legato a tali informazioni è discutibile, soprattutto se si considera che potrebbe avere un effetto maggiore e migliore, in questa lotta, raccontare le esperienze personali, quindi palesare il dato stesso, in modo che non venga più percepito come estraneo alla condizione di vita di molte persone[89]. La scelta per la privacy resta però la soluzione più certa e sicura per il singolo individuo, che non può essere costretto al disvelamento per il solo motivo di contribuire a combattere una percezione comune[90].

Esistono peraltro ulteriori profili, diversi dal contenuto dell'informazione in quanto tale, che possono rendere i dati sanitari particolarmente sensibili.

Uno di questi è la loro caratteristica peculiare di poter costituire o generare interazioni e legami con altri soggetti, diversi dall'interessato. I dati relativi alla salute, infatti, come i dati genetici, sono in grado di presentare natura strutturalmente condivisa, l'identità che disvelano è di tipo relazionale: una patologia di cui è affetto un soggetto può interessare, sotto molteplici aspetti, il suo nucleo familiare o altre persone. Così è, per esempio, nel caso di una patologia ereditaria o sessualmente trasmissibile.

La sensibilità del dato sarà dunque potenzialmente maggiore se questo si presenta a struttura condivisa, e sarà tanto maggiore quanto più ampio sarà il numero di soggetti con cui tale struttura avrà collegamenti. In questo caso è non solo e non tanto il contenuto

---

[87] Cfr. Gruppo Articolo 29, *Documento di lavoro sul trattamento di dati personali relativi alla salute nelle cartelle cliniche elettroniche (EHR)*, cit., 14.

[88] È concreta la possibilità che vengano ad esistere, in futuro, nuovi dati relativi alla salute che presentino una sensibilità maggiore o dati sanitari non nuovi che acquistino una nuova superiore sensibilità, rispetto al passato. Si consideri il caso del vaccino contro il c.d. vaiolo delle scimmie (*monkeypox*). MALGIERI, *"Vaccino per i gay" e dati supesensibili: quando la privacy può combattere lo stigma*, in *www.repubblica.it*, 10 agosto 2022.

[89] GELPI, *Rethinking supeconfidentiality in the age of disclosure: The ethical and social implications of privacy protections in mental health data*, in *Ethics, Medicine and Public Health*, 2017, vol. 3, n. 1, 116 ss. ».

[90] V. FEROLA, *op. cit.*, 414 ss. Mettono in rilievo tale aspetto, pur in relazione a un caso pratico inerente ai dati di tipo genetico, TORALDO DI FRANCIA, *Test genetici per malattia ad insorgenza tardiva. Il punto di vista bioetico*, in FUNGHI *et al.* (a cura di), *Medicina, bioetica e diritto. I problemi e la loro dimensione normativa*, 2a ed., Pisa, Edizioni ETS, 2013, 84 ss., e PICIOCCHI, *Test genetici per malattia ad insorgenza tardiva. Il punto di vista giuridico*, *ivi*, 91 ss., cui si rinvia anche per riferimenti bibliografici. Sulla relazionalità del dato personale, più in generale, ZENO-ZENCOVICH, *La "comunione" dei dati personali. Un contributo al sistema dei diritti della personalità*, in *Dir. inf.*, 2009, 5 ss.

dell'informazione a determinare il rischio più serio per le libertà e i diritti fondamentali della persona, quanto il fatto che il dato sia correlato ai diritti di più persone.

E' utile infine ricordare, tornando alla definizione di "dato relativo alla salute" che lo stesso può riguare un aspetto – pur di natura sanitaria – del passato, del presente o del futuro della persona. Da questa prospettiva si può cogliere come sia particolarmente vera per i dati relativi alla salute l'affermazione secondo cui i dati personali raccontino la storia della persona. Il dato sanitario, per la sua componente fisico-biologica, per quella amministrativa, per quella esistenziale, è in grado di narrare il vissuto dell'individuo non solo negli snodi più importanti e anche drammatici del tempo trascorso, ma anche nei segmenti più reconditi degli anni passati, per spingersi fino al futuro.

La particolare sensibilità del dato relativo alla salute si registra quindi anche per il suo singolare potenziale coinvolgimento di tutto l'arco della vita della persona.

2. *Il trattamento dei dati relativi alla salute*

A livello internazionale, la disciplina del trattamento dei dati relativi alla salute delineata nell'ambito del Consiglio d'Europa, ora dettagliatamente contemplata dalla citata Raccomandazione del Comitato dei ministri, CM/Rec(2019)2, non si discosta, in linea generale, dai principi di cui all'impianto normativo del reg. Ue n. 679 del 2016[91].

Ai sensi dell'art. 9, par. 1, del Regolamento, il trattamento dei dati relativi alla salute è vietato.

Come già visto, anche la Direttiva madre del 1995, all'art. 8, collocava i dati relativi alla salute fra i dati personali per il cui trattamento si imponeva il divieto agli Stati. Tra le deroghe allora previste, un ruolo determinante era giocato in ambito sanitario dal par. 3 dell'art. 8[92].

La loro classificazione non solo come dati sensibili, ma anche come supersensibili o sensibilissimi, è alla base, da un lato, delle rigide misure in ordine al loro trattamento e, dall'altro, di una considerazione particolare, che è in grado di tradursi normativamente in disposizioni speciali che regolino specificamente taluni aspetti del relativo trattamento[93]. La

[91] Cfr. HORDERN, *Data Protection Compliance in the Age of Digital Health*, in *European Journal of Health Law*, vol. 23, n. 3, 2016, 248 ss.

[92] «*Special measures are needed to protect health data, the processing of which is associated with serious privacy infringements, against abuse (e.g. the commercial use of patient data)*». Gruppo Articolo 29, *Advice paper on special categories of data ("sensitive data")*, cit., 10.

[93] «*The 'health law of privacy' finds its core of statutes in Art, 9, para 2, of GDPR*». FARES, *The processing of personal data concerning health according to the EU Regulation*, cit., 21. Sul tema si v. anche lo studio di

definizione in termini ampi della nozione di 'trattamento' determina l'estensione del divieto a un numero assai elevato di fattispecie concrete, ma esistono dei correttivi di carattere generale alla *vis* espansiva dell'applicabilità del Regolamento, che ridimensionano anche la portata del divieto di trattamento di dati relativi alla salute, proprio segnando un confine all'applicazione delle norme del GDPR.

Già si è detto della lett. *c* dell'art. 2, par. 2, venuta in rilievo anche nella sentenza *Lindqvist*.

Tuttavia, il vero e proprio meccanismo che argina l'incidenza del divieto sono le eccezioni dettate dall'art. 9, par. 2, del Regolamento[94]. Attraverso quelle deroghe, viene consentito uno dei tipi più rilevanti di trattamento di dati relativi alla salute, ossia il trattamento in ambito sanitario.

Oltre alle ipotesi riconducibili alla volontà della persona, ossia le eccezioni di cui alle lett. *a* ed *e*, giocano un ruolo di fondamentale importanza a tal fine le fattispecie enunciate alle lett. *c*, *g*, *h*, *i* e *j*.

Innanzitutto, l'eccezione di cui alla lett. *h*, che si sostanzia nella già citata 'finalità di cura', permette il trattamento dei dati relativi alla salute, qualora necessario, per l'erogazione dei servizi e delle prestazioni di natura medica e sanitaria, non solo sulla base del diritto eurounitario o nazionale, ma anche «conformemente al contratto con un professionista della sanità». Viene così coperto il panorama tanto del settore pubblico quanto di quello privato. La disposizione è integrata dalla previsione dell'art. 9, par. 3, secondo cui il trattamento per finalità di cura di dati sanitari, oltre alle altre categorie particolari di dati personali, deve avvenire soltanto ad opera o sotto la responsabilità di un professionista vincolato al segreto professionale o di un soggetto comunque tenuto all'obbligo di segretezza.

Il trattamento di dati relativi alla salute in ambito sanitario è parte essenziale del rapporto medico-paziente ed è indispensabile per l'individuazione e l'esecuzione del trattamento sanitario e per lo svolgimento della funzione di un sistema sanitario[95].

Ma il trattamento di dati relativi alla salute in ambito sanitario è permesso, sotto altri

---

TZANOU (a cura di), *Health Data Privacy under the GDPR. Big Data Challenges and Regulatory Responses*, Londra, Routledge, 2021. Cfr. C. PERLINGIERI, *eHealth and Data*, *op. cit.*, 130

[94] «L'informazione è dunque al centro delle organizzazioni sanitarie forse anche più della conoscenza. Le informazioni sanitarie sono cresciute in numero e complessità e sono divenute forse la prima preoccupazione delle strutture sanitarie». COMANDÉ, *Circolazione elettronica dei dati sanitari e regolazione settoriale: spunti ricostruttivi su «interferenze sistematiche»*, in RUSCELLO (a cura di), *Studi in onore di Davide Messinetti*, I, Napoli, Edizioni Scientifiche Italiane, 2008, 289.

[95] Cfr. GRECO, *Sanità e protezione dei dati personali*, in FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., 244 ss., spec. 249 ss.

aspetti, anche dalle altre ipotesi menzionate[96]. Così, con l'applicazione della lett. *c*, si consente il trattamento di dati sanitari che risulti necessario per un trattamento sanitario salvavita o richiesto in condizioni gravi di salute. Per la ricerca in ambito medico, la lett. *j* permette il necessario trattamento dei dati sulla salute[97].

L'importanza del trattamento dei dati sanitari, ma pure delle altre tipologie di dati sensibili, a scopi legati alla tutela della salute è sottolineata anche dal considerando 53 del Regolamento, per cui «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, compreso il trattamento di tali dati da parte della dirigenza e delle autorità sanitarie nazionali centrali a fini di controllo della qualità, informazione sulla gestione e supervisione nazionale e locale generale del sistema di assistenza sanitaria o sociale, nonché per garantire la continuità dell'assistenza sanitaria o sociale e dell'assistenza sanitaria transfrontaliera o per finalità di sicurezza sanitaria, controllo e allerta o 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

[96] «*Data processing and the use of sensitive personal data such as genome-based information are crucial for the advances of health research activities such as clinical research and translational research, for practicing whole genome sequencing, for research biobanking or the creation of research databases*». CHASSANG, *The impact of the EU general data protection regulation on scientific research*, in e*cancer*, 2017, n. 11, 709. Si aggiunga, come scrive CAYÓN-DE LAS CUEVAS, *Big data applied to biomedicine: in need for a research-friendly approach*, in FARES (a cura di), *The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis*, Torino, Giappichelli, 2021, 54, che «*big data does not represent the future of biomedicine but the present. Actually big data has already transformed biomediicine introducing a new era that implies a Copernican Revolution*».Si tenga anche presente come, nel quadro dei principi tracciato dal Regolamento, un trattamento ulteriore di dati personali a fini di ricerca non è considerato, conformemente all'art. 89, par. 1, incompatibile con le finalità iniziali, secondo l'art. 5, par. 1, lett. *b*. In arg. GUARDA, *Il regime giuridico dei dati della ricerca scientifica*, cit. Cfr. BECKER *et al*., *Secondary Use of Personal Health Data: When Is It "Further Processing" Under the GDPR, and What Are the Implications for Data Controllers?*, in *European Journal of Health Law*, in *brill.com*, 1° agosto 2022; HERVEG e ALTAVILLA, *Introducing Key Elements Regarding Access to Personal Data for Scientific Research in the Perspective of Developing Innovative Medicines*, in *European Journal of Health Law*, vol. 27, n. 3, 2020, 195 ss.; VERHENNEMAN *et al*., *How GDPR Enhances Transparency and Fosters Pseudonymisation in Academic Medical Research, ivi*, fasc. n. 1, 35 ss.; MOSTERT *et al*., *From Privacy to Data Protection in the eu: Implications for Big Data Health Research*, in *European Journal of Health Law*, vol. 25, n. 1, 2018, 43 ss

[97] La disposizione è coerente con quanto affermato al considerando 52 del Regolamento. In ogni caso, si ribadisce che, come disposto dal Regolamento, ciò deve avvenire sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale. Si osserva, a tal proposito, come il Consiglio di Stato francese abbia dichiarato illegittimo un decreto per l'assenza di garanzie sufficienti ad assicurare che l'accesso ai dati sanitari trattati non ecceda quanto strettamente necessario per l'esercizio del compito riconosciuto dalla legge. Conseil d'État, 25.11.2020, n. 428451, in *www.conseietat.fr.*

pubblico interesse nell'ambito della sanità pubblica»[98].

Va anche tenuto conto che il settore sanitario non è l'unico in cui avviene il trattamento di dati relativi alla salute. Esso infatti si svolge in numerosi ambiti, anche per scopi più strettamente legati al mondo dell'economia. Anche per questo l'esigenza di delineare attentamente le eccezioni al divieto di trattamento si impone con forza, soprattutto nella rapida evoluzione tecnologica che contraddistingue la società contemporanea[99].

Il Regolamento rinuncia poi a una vera e propria uniformazione delle discipline nazionali, lasciando alla discrezionalità degli Stati membri la possibilità di condizionare e anche limitare il trattamento dei dati relativi alla salute, così come quello dei dati genetici e biometrici, attraverso il mantenimento delle normative interne o l'introduzione di nuove regole, per certi versi seguendo una logica simile a quella armonizzante della direttiva.[100]

Ma, poiché i dati relativi alla salute sono un sottoinsieme di dati personali, per essi trovano applicazione anche le norme dettate per il trattamento dei dati personali, più in generale.

In particolare, le declinazioni dei diritti dell'interessato in relazione ai dati sanitari vengono ad assumere un tratto significativo nell'orizzonte normativo del trattamento di questa categoria particolare di dati, tenuto conto che, molte volte, la qualifica di 'interessato' viene a coincidere con quella di 'paziente', con riguardo a tale tipo di trattamenti[101].

---

[98] Prosegue: «Pertanto il presente regolamento dovrebbe prevedere condizioni armonizzate per il trattamento di categorie particolari di dati personali relativi alla salute in relazione a esigenze specifiche, in particolare qualora il trattamento di tali dati sia svolto da persone vincolate dal segreto professionale per talune finalità connesse alla salute. Il diritto dell'Unione o degli Stati membri dovrebbe prevedere misure specifiche e appropriate a protezione dei diritti fondamentali e dei dati personali delle persone fisiche. Gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre ulteriori condizioni, fra cui limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute, senza tuttavia ostacolare la libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi».

[99] Richiamando il '*mosaic of policies*' di WESTIN, *Computers, Health Records and Citizen Rights*, U.S. Dept. of Commerce, Washington DC, 1976, 269, come necessità per gestire le problematiche sollevate dal trattamento di dati sanitari, COMANDÉ, *Circolazione elettronica dei dati sanitari e regolazione settoriale: spunti ricostruttivi su «interferenze sistematiche»*, cit., 285, individua alcune aree in cui i dati sulla salute sono sempre maggiormente raccolti, usati e condivisi: «1. l'erogazione di servizi sanitari; 2. il pagamento delle prestazioni; 3. gli usi sociali dei dati sanitari per prevenire la diffusione di epidemie».

[100] la disposizione di riferimento in questo caso è il par. 4 dell'art. 9. una norma di diritto interno che richiedesse, in modo generalizzato, il consenso dell'individuo per il trattamento di dati sanitari risulterebbe compatibile con l'art. 9 del Regolamento, alla luce di quanto disposto dal suddetto par. 4.

[101] Sui 'diritti dell'interessato' sanciti nel Regolamento, *ex multis*, v. TUCCARI, *I diritti dell'interessato*, inG. MAGRI, MARTINELLI e THOBANI (a cura di), *Manuale di diritto privato delle nuove tecnologie*, Torino, Giappichelli, 2022, 151 ss.; CALISAI, *I diritti dell'interessato*, in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., 327 ss.; F. PIRAINO, *I "diritti dell'interessato" nel Regolamento generale sulla protezione dei dati personali*, in CATERINA (a cura di), *GDPR tra novità e discontinuità*, in *Giur. it.*, 2019, 2789 ss.; A. RICCI, *I diritti dell'interessato*, in FINOCCHIARO (a cura di),

Così l'informazione che il titolare del trattamento deve fornire all'interessato, quando i dati personali sono ottenuti, include, ai sensi dell'art. 13, par. 2, del Regolamento, tra l'altro, il periodo di conservazione dei dati o, se non è possibile, i criteri utilizzati per determinare tale periodo (lett. *a*). Tale previsione acquista importanza, nel trattamento dei dati sanitari, in relazione alle banche dati in uso in ambito medico e alle raccolte di dati a scopi di ricerca scientifica. Allo stesso modo, la disposizione di cui al par. 3 dell'art. 13, che prevede l'obbligo per il titolare del trattamento, nel caso in cui intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui sono stati raccolti, di fornire all'interessato, prima del trattamento ulteriore, le informazioni in merito a tale diversa finalità e ogni altra informazione pertinente, viene ad avere un peso specifico con riferimento ai dati relativi alla salute, soprattutto nei casi in cui vengano raccolti dati di pazienti per finalità di cura e poi si voglia utilizzarli per fini diversi, come può essere la ricerca, la statistica oppure ancora finalità istituzionali nel settore della sanità pubblica.

Nel caso in cui i dati personali non siano stati ottenuti presso l'interessato, l'informazione al medesimo è disciplinata dall'art. 14 del Regolamento, il quale al par. 5 deroga agli obblighi previsti dai paragrafi precedenti se e nella misura in cui «comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni» (lett. *b*). Anche questa previsione può trovare specifica applicazione per il trattamento di dati relativi alla salute, per esempio quando un trattamento coinvolga una coorte molto numerosa di pazienti.

Quanto al diritto di accesso, sancito all'art. 15, un esempio di esercizio di tale diritto in relazione ai dati sulla salute è dato dal considerando 63 del Regolamento stesso, quando si riferisce alle «cartelle mediche contenenti informazioni quali diagnosi, risultati di esami,

---

La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101, cit., 392 ss.; EAD., *I diritti dell'interessato*, in FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 179 ss. Per una prospettiva relativa al quadro normativo antecedente, MORMILE, *I diritti dell'interessato*, in PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, t. II, Milano, Giuffrè, 2006, 1199 ss.

pareri di medici curanti o eventuali terapie o interventi praticati».

Il diritto di rettifica, di cui all'art. 16, potrebbe esercitarsi invece per correggere inesattezze o per integrare le raccolte, laddove i dati trattati risultino incompleti, in ordine alle condizioni di salute del soggetto.

Il diritto di cancellare i dati personali trova invece rilevanti limitazioni nei trattamenti di dati sanitari. Secondo l'art. 17, par. 3, lett. *c*, infatti, il titolare del trattamento non è obbligato a cancellare i dati, se il loro trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'art. 9, par. 2, lett. *h* e *i*, e dell'art. 9, par. 3. Analogamente non sussiste l'obbligo, tra l'altro, qualora il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui il diritto di cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento (lett. *d*). Il rilievo di queste finalità[102] si può ritrovare all'art. 21, in relazione al diritto di opposizione. Così, se i dati personali sono trattati a fini di ricerca o a fini statistici, l'interessato, ai sensi del par. 6, per motivi connessi alla sua situazione particolare, ha sì il diritto di opporsi al trattamento di dati personali che lo riguarda, a meno che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico[103].

Ulteriori diritti dell'interessato, che possono venire in gioco in caso di trattamento dei dati relativi alla salute sono il diritto di limitazione di trattamento (art. 18) – che il paziente può esercitare per bloccare operazioni di trattamento di dati personali, ad esempio, da parte di un'azienda sanitaria – e il diritto alla portabilità dei dati (art. 20) – che diventa essenziale per il paziente che intraprenda un percorso di cure attraverso più strutture sanitarie[104].

---

[102] Cfr. CIPPITANI, *Finalità di ricerca scientifica ed eccezioni alla disciplina della protezione dei dati personali*, in *Ciberspazio e diritto*, 2019, 161 ss. Per uno studio sull'attuazione della Direttiva madre nei vari ordinamenti europei, con speciale riferimento ai profili legati al trattamento dei dati personali a fini di ricerca medico-scientifica, BEYLEVELD *et al.* (a cura di), *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*, Farnham, Ashgate, 2004.

[103] Sul bilanciamento operato con riguardo al diritto di opposizione, DI LORENZO, *Spunti di riflessione su taluni «diritti dell'interessato»*, in ZORZI GALGANO (a cura di), *op. cit.*, 251 ss.

[104] Si osserva peraltro che la garanzia di questo diritto, massimizzando le potenzialità circolatorie del dato personale, non è esente da profili di criticità sul versante della tutela della persona. Evidenzia i rischi e il possibile impatto negativo della portabilità dei dati personali sulla tutela della persona TROIANO, *Il diritto alla portabilità dei dati personali*, *ivi*, 195 ss., spec. 209 ss. In arg. BATTELLI e D'IPPOLITO, *Il diritto alla portabilità dei dati personali*, in TOSI (a cura di), *op. cit.*, 185 ss.; F. CATALANO, *Il diritto alla portabilità dei dati tra interessi individuali e prospettiva concorrenziale*, in *Eur. e dir. priv.*, 2019, 833 ss.; GIO.M. RICCIO e PEZZA, *Portabilità dei dati personali e interoperabilità*, in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., 397 ss.; SCORZA, *La portabilità dei dati tra privacy e regole del mercato*, in MANTELERO e POLETTI (a cura di), *op. cit.*, 307 ss. Con riguardo, nello specifico, ai

A questi diritti si aggiunge quello, *ex* art. 22, «di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona». L'incidenza di tale diritto (o divieto) si registra in particolar modo nelle applicazioni dell'intelligenza artificiale, che sempre più si aprono a nuovi sviluppi, anche con riguardo ai dati relativi alla salute[105].

Il Regolamento ammette poi la possibilità di restringere la sfera applicativa dei diritti dell'interessato, compresi quindi i diritti esercitabili nel contesto sanitario.

All'art. 23, par. 1, infatti, prevede che la portata degli obblighi e dei diritti di cui agli artt. da 12 a 22 e 34, nonché all'art. 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, possa essere limitata dal diritto eurounitario o dal diritto nazionale, sempreché questa limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare, tra l'altro, importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, anche in materia di sanità pubblica (lett. *e*).

Dalla disamina dei diritti dell'interessato, in relazione al trattamento dei dati sanitari, e dalle modalità del loro esercizio, emerge la funzione di garantire al soggetto cui le informazioni si riferiscono una sua partecipazione al controllo sul flusso dei dati stessi[106].

Con tutto ciò, il trattamento di dati relativi alla salute non può comunque dirsi ammesso in linea generale, semplicemente basandosi su un'applicazione delle eccezioni di cui all'art. 9, par. 2, ogniqualvolta il trattamento appaia utile, ma resta vietato in tutti quei casi in cui quelle eccezioni non possono applicarsi, seguendo come criterio esegetico di fondo quello dell'interpretazione restrittiva del par. 2 dell'art. 9.

Inoltre, attesa l'importanza quantitativa e qualitativa dei trattamenti di dati svolti mediante dispositivi medici, che, a decorrere dal 26 maggio 2020, è applicabile il Regolamento (UE) 2017/745, del Parlamento europeo e del Consiglio, del 5 aprile 2017,

---

dati relativi alla salute, TUZZOLINO, *La portabilità dei dati sanitari*, in A. THIENE e S. CORSO (a cura di), *op. cit.*, 59 ss.

[105] Gli approcci più nuovi della medicina non si limitano ai settori degli interventi, ma includono l'utilizzo dei *big data* e l'intelligenza artificiale in sanità. CIRILLO, *The Impact of e-Health on Privacy and Fundamental Rights: From Confidentiality to Data Protection Regulation*, in *European Journal of Privacy Law & Technologies*, 2019, fasc. 2.

[106] CIANCIMINO, *Protezione e controllo dei dati in àmbito sanitario e intelligenza artificiale. I dati relativi alla salute tra novità normative e innovazioni tecnologiche*, Napoli, Edizioni Scientifiche Italiane, 2020, 44 ss.; G. GAROFALO, *Trattamento e protezione dei dati personali: spunti rimediali in ambito sanitario*, in *Dir. fam. e pers.*, 2021, 1392 ss

relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio, il quale, come enunciato all'art. 1, par. 1, stabilisce le norme relative all'immissione sul mercato, la messa a disposizione sul mercato o la messa in servizio dei dispositivi medici per uso umano e degli accessori per tali dispositivi nell'Unione europea e si applica, inoltre, alle indagini cliniche relative a tali dispositivi medici e relativi accessori condotte nell'UE[107].

Il Regolamento sui dispositivi medici va, in ogni caso, coordinato con il Regolamento generale sulla protezione dei dati personali. Così l'art. 110, par. 1, del reg. Ue n. 745 del 2017, secondo cui gli Stati membri applicano la direttiva 95/46/CE al trattamento dei dati di carattere personale effettuato nel loro territorio a norma del Regolamento sui dispositivi medici, va letto ora in riferimento al reg. Ue n. 679 del 2016. Se non si è ritenuto ammissibile, almeno finora, un mercato di dati relativi alla salute, al contrario si è certamente ammesso – e regolato – il mercato di dispositivi medici. Ma il panorama potrebbe mutare, anche considerevolmente, dall'eventuale approvazione della proposta di Regolamento che istituisce lo spazio europeo dei dati sanitari.

[107] Tra le definizioni che fornisce all'art. 2, si ricordano: quella di 'dispositivo medico', al n. 1, ossia qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione, per una o più delle seguenti destinazioni d'uso mediche specifiche: diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie; diagnosi, monitoraggio, trattamento, attenuazione o compensazione di una lesione o di una disabilità; studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico; fornire informazioni attraverso l'esame in vitro di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati; e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere coadiuvata da tali mezzi (ma si considerano dispositivi medici anche i dispositivi per il controllo del concepimento o il supporto al concepimento e i prodotti specificamente destinati alla pulizia, disinfezione o sterilizzazione dei dispositivi di cui all'art. 1, par. 4, e di quelli di cui al primo comma di questo punto); quella di 'interoperabilità', al n. 26, cioè «la capacità di due o più dispositivi, compreso il software, dello stesso fabbricante o di fabbricanti diversi di: a) scambiare informazioni e utilizzare le informazioni scambiate ai fini della corretta esecuzione di una funzione specifica senza modifica del contenuto dei dati; e/o b) comunicare tra di loro; e/o c) funzionare congiuntamente come previsto»; e quella di 'dati clinici', al n. 48, vale a dire informazioni sulla sicurezza o sulle prestazioni ricavate dall'impiego di un dispositivo e che provengono: dalle indagini cliniche relative al dispositivo in questione; dalle indagini cliniche o da altri studi pubblicati nella letteratura scientifica relativi a un dispositivo di cui è dimostrabile l'equivalenza al dispositivo in questione; da relazioni pubblicate nella letteratura scientifica sottoposta a valutazione *inter pares* su altre esperienze cliniche relative al dispositivo in questione o a un dispositivo di cui è dimostrabile l'equivalenza al dispositivo in questione; da informazioni clinicamente rilevanti risultanti dalla sorveglianza post-commercializzazione, in particolare il *follow-up* clinico post-commercializzazione.

2.1. *Il trattamento dei dati relativi alla salute nell'ordinamento italiano*

Con l. 31 dicembre 1996, n. 675, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", com'è noto, fu data attuazione in Italia alla Direttiva n. 46 del 1995 sulla protezione dei dati personali.

La regola generale sui dati sensibili – tra cui si comprendevano i dati «idonei a rivelare lo stato di salute» – prevista all'art. 22 della l. n. 675/1996, era quella per cui il trattamento era ammesso «solo con il consenso scritto dell'interessato e previa autorizzazione del Garante»[108]. Tale impostazione, rigida e formalistica, non fu granché intaccata con i successivi interventi legislativi, il d.lgs. 11 maggio 1999, n. 135, e il d.lgs. 28 dicembre 2001, n. 467, che modificarono l'art. 22[109]. Se il trattamento di dati sensibili era posto in essere da soggetti pubblici, esso era consentito solo se autorizzato da espressa disposizione di legge nella quale fossero specificati i dati che potevano essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite (art. 22, comma 3°)[110].

Ai dati inerenti alla salute era specificamente dedicato l'art. 23, secondo cui il trattamento di tali dati poteva avvenire anche senza l'autorizzazione del Garante, se posto in essere dagli esercenti le professioni sanitarie e gli organismi sanitari pubblici, limitatamente ai dati e alle operazioni indispensabili per il perseguimento di finalità di tutela dell'incolumità fisica e della salute dell'interessato[111]. Nel caso in cui le stesse finalità

---

[108] Per una rassegna dei provvedimenti del Garante per la protezione dei dati personali resi nella vigenza di questa disciplina, si v. PERON, *Rassegna di giurisprudenza in materia di privacy (anche alla luce del* Codice della Privacy *che entrerà in vigore il 1° gennaio 2004)*, in *Resp. civ. e prev*., 2003, 1017 ss.

[109] Ma v. SICA, *La «riforma» della privacy ed il nuovo sistema di informativa e consenso: ben più di una modifica applicativa*, in *Corr. giur*., 2002, 537 ss.

[110] Numerose le opere di commento. *Ex multis*, BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, cit.; CUFFARO e RICCIUTO (a cura di), *La disciplina del trattamento dei dati personali*, Torino, Giappichelli, 1997; GIANNANTONIO, LOSANO e ZENO-ZENCOVICH (a cura di), *La tutela dei dati personali. Commentario alla l. 675/1996*, Padova, CEDAM, 1997; ALPA, *La disciplina dei dati personali. Note esegetiche sulla Legge 31 dicembre 1996, n. 675 e successive modifiche*, Roma, Seam, 1998; C.M. BIANCA e BUSNELLI (a cura di), *Tutela dei dati personali. Commentario alla l. 31 dicembre 1996, n. 675*, Padova, CEDAM, 1999; CLEMENTE (a cura di), *Privacy*, Padova, CEDAM, 1999; DOGLIOTTI, *Trattamento dei dati e tutela della persona*, in *Dir. fam. e pers*., 1999, 1289 ss. V. anche LOSANO (a cura di), *La legge italiana sulla* privacy. *Un bilancio dei primi cinque anni*, Roma-Bari, Laterza, 2001, e *ivi*, in particolare, MARCENÒ, *L'inserimento della legge sulla privacy nel sistema giuridico italiano*, 29 ss., e CARTABIA, *Le norme sulla privacy come osservatorio sulle tendenze attuali delle fonti del diritto*, 61 ss.; MANTELERO, *Il diritto alla riservatezza nella legge n. 675 del 1996: il nuovo che viene dal passato*, in *Riv. trim. dir. e proc. civ*., 2000, 973 ss.;

[111] Su quella norma v. MINARDI, in GIANNANTONIO, LOSANO e ZENO-ZENCOVICH (a cura di), *op. cit.*, 1997, *sub* art. 23, 207 ss.; POLETTI, in C.M. BIANCA e BUSNELLI (a cura di), *Tutela dei dati personali. Commentario alla l. 31 dicembre 1996, n. 675*, cit., *sub* art. 23, 560 ss.; C. SARZANA DI S. IPPOLITO, *La protezione dei dati personali nel campo sanitario: problemi giuridici e tecnologici*, in *Dir. inf.*, 1999, 29 ss., spec. 30 s.; TAGLIABRACCI, *Trattamento dei dati inerenti alla salute e privacy. Problemi applicativi e riflessioni medico-legali sulla legge 675/96*, in *Riv. it. med. leg*., 1999, 1087 ss.; DI CIOMMO, *La privacy*

riguardassero un terzo o la collettività, in mancanza del consenso dell'interessato, il trattamento poteva avvenire previa autorizzazione del Garante (comma 1°)[112]. Il disvelamento di queste informazioni all'interessato era possibile solo per il tramite di un medico designato dallo stesso o dal titolare (comma 2°). Le modalità con cui si prevedeva la prestazione del consenso, a fronte delle rigidità che si riscontravano nella pratica, videro un'apertura verso la semplificazione già con il d.lgs. 30 luglio 1999, n. 282[113]

La prima autorizzazione generale relativa al trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale fu del 27 novembre 1997. Era l'autorizzazione n. 2 del Garante, rilasciata dall'allora Presidente – il primo – Stefano Rodotà, alla quale fecero seguito di anno in anno le successive autorizzazioni[114].

E già allora buona parte delle problematiche inerenti all'impiego della tecnologia, nell'uso delle informazioni sulla salute in ambito sanitario, era da tempo nota[115].

Quella prima disciplina della protezione dei dati personali, presto invecchiata a fronte delle rapide evoluzioni della società, fu superata con la sistematizzazione della materia ad opera del Codice della privacy, il d.lgs. 30 giugno 2003, n. 196.

Il nuovo impianto normativo distingueva le regole applicabili al trattamento di dati sensibili da parte di soggetti pubblici da quelle applicabili invece al medesimo trattamento ad opera di privati ed enti pubblici economici.

Secondo le prime, dettate all'art. 20, era consentito il trattamento dei dati sensibili da parte di soggetti pubblici solo se autorizzato da espressa disposizione di legge, in cui si specificavano i tipi di dati trattabili e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite[116]. Qualora si fossero specificate solo le finalità, il trattamento

---

sanitaria, cit., 259 ss. Cfr. ZAMBRANO, *Dati sanitari e tutela della sfera privata*, in *Dir. inf*., 1999, 1 ss.; BATTAINI, *La tutela della privacy nelle strutture sanitarie*, in *Nuova rass.*, 1998, 609 ss.; GELLMANN, *Protection of medical data*, in AA.VV., *Società dell'informazione. Tutela della riservatezza*, Milano, Giuffrè, 1998, 79 ss.

[112] DOGLIOTTI, *op. cit*., 1293, osservava già l'opportunità di un'anonimizzazione. Per un caso di trattamento posto in essere da un ospedale universitario, v. il provvedimento del Garante per la protezione dei dati personali, del 24 maggio 1999, in *Nuova giur. civ. comm*., 1999, I, 829 ss., con nota di CATALLOZZI, *Dati sanitari e dati genetici: una frontiera aperta?*

[113] Cfr. GAMBERALE, *Il settore sanitario*, cit., 1506 ss.

[114] Il testo dell'autorizzazione n. 2 del 1997 e delle altre autorizzazioni generali è consultabile nel sito istituzionale dell'Autorità, *www.garanteprivacy.it*. Sulle autorizzazioni generali v. CATALLOZZI, *I provvedimenti del Garante per la protezione dei dati personali*, in *Nuova giur. civ. comm*., 1998, II, 441 ss.

[115] V. PICCININI GRAZIANI, *Diritto alla riservatezza, elaboratori e informazione sanitaria*, in *Giust. civ*., 1980, II, 243 ss., spec. 251 ss.

[116] FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, cit., 171 ss.; SANNA, in C.M. BIANCA e BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196, Codice della privacy*, cit., *sub* art. 20, 501 ss.; v. MAIETTA, in SICA e P. STANZIONE

consentito era limitato secondo il disposto del comma 2°, mentre, se il trattamento non fosse stato previsto espressamente da una disposizione di legge i soggetti pubblici avrebbero potuto rivolgersi al Garante per l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per la conseguente autorizzazione. I soggetti pubblici, ai sensi dell'art. 22, potevano trattare solo i dati sensibili indispensabili per svolgere attività istituzionali, che non potevano adempiersi, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

Per le seconde, invece, delineate dall'art. 26, si ribadiva la regola del consenso scritto dell'interessato e della previa autorizzazione del Garante[117]. Non mancavano comunque deroghe, tra cui, in particolare, quella che ammetteva il trattamento di dati sensibili a prescindere dal consenso dell'interessato, ma previa autorizzazione del Garante, qualora fosse necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo (comma 4°, lett. *b*).

In ogni caso, era categoricamente vietata la diffusione dei dati idonei a rivelare lo stato di salute.

Il regime del trattamento dei dati relativi alla salute da parte di esercenti le professioni sanitarie e di organismi sanitari pubblici era dettato dal Titolo V, "Trattamento di dati personali in ambito sanitario", della Parte II del Codice della privacy, ossia dagli artt. 75 ss.[118] In particolare, l'art. 76 richiedeva il consenso dell'interessato, a meno che il trattamento non riguardasse dati e operazioni indispensabili per perseguire una finalità di

---

(a cura di), *op. cit.*, *sub* artt. 11 ss., spec. 80 ss., secondo cui l'articolo in esame delinea una "tutela preventiva rafforzata". Sul diverso regime applicabile al trattamento operato in ambito pubblico, CARDARELLI, *I trattamenti in ambito pubblico: i soggetti ed i rapporti tra le fonti*, in CARDARELLI, SICA e ZENO-ZENCOVICH (a cura di), *op. cit.*, 203 ss. Cfr. DE TURA, *Le regole ulteriori per i soggetti pubblici*, in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, cit., 163 ss

[117] PELLECCHIA, in C.M. BIANCA e BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196, Codice della privacy*, cit., *sub* art. 26, 616 ss.; EAD., *Scelte contrattuali e informazioni personali*, Torino, Giappichelli, 2005, 47 s.; GIU.M. RICCIO, in SICA e P. STANZIONE (a cura di), *op. cit.*, *sub* artt. 23 ss., 89 ss., spec. 113 ss. Offre una ricostruzione cronologica del dato normativo GAMBERALE, *Il trattamento dei dati sensibili*, in PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, cit., 1071 ss. Cfr. MELONI, *Il trattamento dei dati da parte di soggetti privati: la disciplina del consenso*, in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, cit., 197 ss., spec. 215 ss.

[118] GIO.M. RICCIO, Privacy *e dati sanitari*, in CARDARELLI, SICA e ZENO- ZENCOVICH (a cura di), *op. cit.*, 247 ss.; GAMBERALE, *Il settore sanitario*, cit., 1509 ss.; VICIANI, *Brevi osservazioni sul trattamento dei dati inerenti la salute e la vita sessuale in ambito sanitario*, in *Riv. crit. dir. priv.*, 2007, 315 ss. Cfr. CAGGIA, *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, cit., 405 ss.; MASCHIO, *Il trattamento dei dati sanitari. Regole generali e particolari trattamenti per finalità di rilevante interesse pubblico*, in SANTANIELLO (a cura di), *op. cit.*, 485 ss.; ACCIAI, *I trattamenti in ambito sanitario*, in ID. (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Santarcangelo di Romagna, Maggioli, 2004, 486 ss.

tutela della salute o dell'incolumità fisica di un terzo o della collettività, nel qual caso era però necessaria l'autorizzazione del Garante[119].

Preso atto del peculiare ruolo svolto da questa tipologia di dati sensibili, il cui trattamento, da un lato, aveva presentato da sempre rischi notevoli e, dall'altro, risultava essenziale per lo svolgimento di determinate attività e il raggiungimento di obiettivi di rilievo pubblico[120], la nuova disciplina segnava comunque un passaggio dalla rigidità e dal formalismo del passato a regole che aprivano a una flessibilità, in vista della funzione svolta dal trattamento stesso[121], mantenendo però un certo rigore intorno al consenso[122]. Peraltro, la consapevolezza della più elevata esigenza di riserbo con riguardo alle informazioni sullo stato di salute della persona e del fondamentale ruolo giocato dal consenso si ritrovava nelle argomentazioni della giurisprudenza. Così evidenziavano i giudici di legittimità che «il regime di protezione dei dati sensibili relativi alla salute (e alla vita sessuale) è […] ispirato alla massima riservatezza dei dati stessi ed alla generale illiceità del trattamento di essi senza il consenso dell'interessato», aggiungendo che «le eccezioni sono tassativamente predeterminate da norme legislative che ne procedimentalizzano puntualmente le modalità d'uso, specie se riguardanti dati sensibili non anonimi»[123].

L'ultima autorizzazione del Garante, al trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, prima dell'entrata in vigore del reg. Ue 2016/679, è stata la n. 2 del 2016[124].

---

[119] POLETTI, in C.M. BIANCA e BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196, Codice della privacy*, cit., *sub* art. 76, 1212 ss.; ZAMBRANO, in SICA e P. STANZIONE (a cura di), *op. cit.*, *sub* art. 76, 319 ss. Nel medesimo Titolo V si sono individuate modalità semplificate per informativa e consenso, le finalità di rilevante interesse pubblico, regole sulle prescrizioni mediche, sui dati genetici, sulle cartelle cliniche, sulle banche dati.

[120] ZENO-ZENCOVICH, *Dieci anni di legislazione sui dati personali: tentativo di un bilancio*, in G.F. FERRARI (a cura di), *op. cit.*, 40, osservava come fosse «sempre maggiore […] l'importanza [dei dati] relativi alla salute, non solo perché attinenti alla sfera più intima della persona ma anche perché essenziali nell'ambito dei rapporti di lavoro, in quelli assicurativi, nelle relazioni interpersonali».

[121] DI MASI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 75, d.lgs. 30 giugno 2003, n. 196, 1234 s. Cfr. POLETTI, in C.M. BIANCA E BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196, Codice della privacy*, cit., *sub* art. 75, 1195 ss.

[122] FINOCCHIARO, *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dati personali*, cit., 211 s.: «nonostante la previsione di modalità semplificate, il legislatore italiano [ha] optato per una linea di grande rigore formale nella tutela dei diritti dell'interessato, prevedendo agli art. 18, c. 4, 76 e 85 del Codice la regola del consenso per il trattamento di dati sanitari». V. EAD., *Privacy e protezione dati personali. Disciplina e strumenti operativi*, cit., 214.

[123] Cass., sez. un., 27.12.2017, n. 30984, cit., punto 7.1.

[124] Provvedimento del Garante per la protezione dei dati personali del 15 dicembre 2016, n. 524, "Autori zazione n. 2/2016 - Autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale".

L'avvento del Regolamento ha determinato lo slittamento della disciplina applicabile dal diritto nazionale al diritto eurounitario, pur senza sottrarre ogni spazio al diritto interno. Il quadro normativo relativo al trattamento dei dati sanitari si compone adesso di una parte di disposizioni del Regolamento – soprattutto principi – che valgono ugualmente per tutti gli Stati membri dell'Unione e di una parte di regole proprie della legislazione nazionale[125].

Per adeguare l'assetto del proprio ordinamento, il legislatore italiano è intervenuto sul Codice della privacy apportando numerose ed estese modifiche al testo normativo, mediante il d.lgs. 10 agosto 2018, n. 101[126].

Il d.lgs. n. 101/2018 ha inciso profondamente sulla struttura e sulle disposizioni del Codice della privacy, abrogando interi blocchi di articoli, sostituendone e modificandone altri, introducendone di nuovi, con una tecnica legislativa che non è andata esente da critiche[127]. Anche il *nomen* del d.lgs. n. 196/2003 è stato cambiato, recitando ora, in modo meno sintetico, "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE"[128].

L'abrogazione dell'art. 4 ha comportato l'eliminazione della definizione di *dati sensibili*,

---

Per un esame dei principali provvedimenti del Garante in materia di sanità, nella vigenza di quella disciplina, v. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, cit., 295 ss.

[125] V. COLAPIETRO, *The general principles of the EU Regulation 2016/679 as a legitimacy's parameter of Member States' national legislations on personal data in a multilevel system of sources of law*, in FARES (a cura di), *The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis*, Torino, Giappichelli, 2021, 3 ss..

[126] Entrato in vigore il 19 settembre 2019, reca appunto "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

[127] CUFFARO, *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, in *Corr. giur.*, 2018, 1183 s.,

[128] Sono proseguite le opere di commento al Codice della privacy, così come modificato dal d.lgs. n. 101/2018: D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, 995 ss.; PIZZETTI (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, Giappichelli, 2021; SCIAUDONE e CARAVÀ (a cura di), *Il codice della privacy. Commento al D.Lgs. 30 giugno 2003, n. 196 e al D.Lgs. 10 agosto 2018, n. 101 alla luce del Regolamento (UE) 2016/679 (GDPR)*, Pisa, Pacini, 2019; BOLOGNINI e PELINO, *Codice privacy: tutte le novità del d.lgs. 101/2018*, numero speciale di *Il civilista*, Milano, Giuffrè, 2018. Cfr. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, cit.; CASSANO *et al.* (a cura di), *op. cit*. V. anche LUCCHINI GUASTALLA, Privacy *e* data protection*: principi generali*, in TOSI (a cura di), *op. cit.*, 55 ss.

contenuta alla lett. *d*, essendo ora assorbita dalla valenza dell'espressione 'categorie particolari di dati personali' di cui all'art. 9 del Regolamento. Come già messo in luce, però, permangono l'utilità e l'utilizzo – nel discorso giuridico – dell'espressione 'dati sensibili', che continua a rimandare a un retroterra, intimo ed esistenziale, proprio della persona.

Il Titolo III della Parte I del d.lgs. n. 196 del 2003 è stato abrogato per intero, con tutti gli articoli che conteneva, compresi gli artt. 20 e 26.

Una parte molto rilevante delle nuove disposizioni, introdotte nel 2018, si trova agli artt. 2 *bis* ss., distribuiti ora, nel Titolo I, "Principi e disposizioni generali", della Parte I, fra quattro diversi capi, "Oggetto, finalità e Autorità di controllo", "Principi", "Disposizioni in materia di diritti dell'interessato" e "Disposizioni relative al titolare del trattamento e al responsabile del trattamento". Si tratta di un insieme corposo di articoli, che il latino numera fino all'art. 2 *septiesdecies*, e su cui il legislatore è già tornato più volte, con aggiunte, modifiche o abrogazioni[129]. Fra questi, un ruolo di estrema importanza per il trattamento di dati personali appartenenti alle particolari categorie, anche e soprattutto per il trattamento dei dati relativi alla salute, è svolto dagli artt. 2 *sexies* e 2 *septies*[130].

L'art. 2 *sexies* precisa le condizioni di ammissibilità dei trattamenti necessari per motivi di interesse pubblico rilevante ai sensi dell'art. 9, par. 2, lett. *g*, del Regolamento[131]. Essi sono ammessi, ai sensi del comma 1°, «qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato»[132].

---

[129] Così l'art. 2 *quinquiesdecies* è stato abrogato dall'art. 9, c. 1°, lett. *c*, d.l. 8 ottobre 2021 n. 139.

[130] C. PERLINGIERI, *eHealth and Data*, *op. cit.*, 130 s

[131] F. CORTESE, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 2 *sexies*, d.lgs. 30 giugno 2003, n. 196, 1044 ss.; QUIROZ VITALE, in SCIAUDONE e CARAVÀ (a cura di), *op. cit.*, *sub* art. 2 *sexies*, 73 ss. Come scrive PIZZETTI, *La Parte I del Codice novellato*, in ID. (a cura di), *op. cit.*, 110, «l'indicazione dei casi di rilevante interesse pubblico in presenza dei quali possono essere posti in essere trattamenti di categorie particolari di dati, spetta dunque inevitabilmente, per la parte che li riguarda, agli Stati. Si tratta, forse, della competenza più delicata e più ricca di implicazioni, anche dal punto di vista del suo impatto sui diritti e i valori fondamentali delle persone, fra quelle attribuite ai legislatori nazionali nell'ambito del sistema regolatorio multilivello».

[132] Il comma 2° dell'art. 2 *sexies* fornisce invece un elenco di materie in cui è considerato rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri. Tra le numerosissime ipotesi di questo elenco, si evidenziano, per la stretta connessione con i dati sanitari, quelle di cui alle lett. *t*, *u*, *v*, *z*, *aa* e *cc*. Rispettivamente: «attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano»; «compiti del servizio

Tale disposizione è stata modificata dall'art. 9, comma 1°, lett. *b*, n. 1, d.l. 8 ottobre 2021, n. 139 – c.d. Decreto capienze –, convertito con modificazioni dalla l. 3 dicembre 2021, n. 205, che ha eliminato la fonte regolamentare della previsione come ipotesi di ammissibilità dei trattamenti nell'ordinamento interno e ha aggiunto invece quella degli atti amministrativi generali[133].

La medesima lett. *b* dell'art. 9, comma 1°, d.l. n. 139/2021, al n. 2 – così come modificato dalla citata legge di conversione n. 205/2021 – ha introdotto poi il comma 1 *bis* dell'art. 2 *sexies* del Codice della privacy, comma specificamente dedicato al trattamento di dati relativi alla salute: «I dati personali relativi alla salute, privi di elementi identificativi diretti, sono trattati, nel rispetto delle finalità istituzionali di ciascuno, dal Ministero della salute, dall'Istituto superiore di sanità, dall'Agenzia nazionale per i servizi sanitari regionali, dall'Agenzia italiana del farmaco, dall'Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle malattie della povertà e, relativamente ai propri assistiti, dalle regioni anche mediante l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Servizio sanitario nazionale, ivi incluso il *Fascicolo sanitario elettronico* (FSE), aventi finalità compatibili con quelle sottese al trattamento, con le modalità e per le finalità fissate con decreto del Ministro della salute, ai sensi del comma 1, previo parere del Garante, nel rispetto di quanto previsto dal Regolamento, dal presente codice, dal codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e dalle linee guida dell'Agenzia per l'Italia digitale in materia di interoperabilità».

---

sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica»; «programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale»; «vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria»; «tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili»; «trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan)».

[133] Riportando il chiarimento del Garante, di cui alla nota del 27 novembre 2018, F. CORTESE, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 2 *sexies*, d.lgs. 30 giugno 2003, n. 196, 1046, evidenzia come anche la prospettiva antecedente alle modifiche citate potesse aprire alla fonte di tipo amministrativo.

.

La nuova disposizione individua una serie di soggetti istituzionali consentendo per costoro, nel rispetto delle proprie finalità, il trattamento di dati personali relativi alla salute, che siano 'privi di elementi identificativi diretti'. Con tale espressione il legislatore esclude dall'area della norma i dati personali riguardanti una persona identificabile direttamente – e a maggior ragione devono intendersi esclusi quelli riguardanti una persona fisica identificata – includendo invece i dati relativi a una persona che possa identificarsi in via indiretta. Il riferimento è sembrato essere almeno ai dati pseudonimizzati, cioè a quei dati trattati in modo da non poter più essere «attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile» (art. 4, n. 5, del Regolamento), tenuto presente che il regime di protezione dei dati personali delineato dal Regolamento stesso, secondo il considerando 26, non si applica ai dati resi anonimi[134].

Si può notare, immediatamente, la centralità – nel trattamento dei dati relativi alla salute, per varie finalità – del fascicolo sanitario elettronico[135].

L'art. 2 *septies*, invece, richiamato pure dal comma 3° dell'art. 2 *sexies*, si pone in attuazione del par. 4 dell'art. 9 del Regolamento, prevedendo, come condizione per am mettere il trattamento di dati relativi alla salute, genetici e biometrici – condizione ulteriore rispetto al ricorrere di una delle fattispecie di deroga al divieto elencate all'art. 9, par. 2, del Regolamento – la conformità alle *misure di garanzia* disposte dal Garante[136].

Particolare importanza ha il comma 5°, per cui le misure di garanzia sono adottate in relazione a ciascuna categoria di dati personali di cui al comma 1°, ossia dati relativi alla salute, dati genetici e dati biometrici, avendo riguardo alle specifiche finalità del trattamento. Lo stesso comma specifica cosa individuino le misure di garanzia, ossia: «le misure di

---

[134] S. CORSO, *Modifiche alla disciplina sul trattamento dei dati relativi alla salute*, in *www.rivistaresponsabilita medica.it*, 29 gennaio 2022

[135] C. PERLINGIERI, *eHealth and Data*, *op. cit.*, 132 s.

[136] ZANOVELLO, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 2 *septies*, d.lgs. n. 196 del 2003, 1051 ss.; EAD., *Misure di garanzia e rischio di* data breach *in ambito sanitario*, cit., 129 ss., spec. 150 ss.; CARAVÀ, in SCIAUDONE e CARAVÀ (a cura di), *op. cit.*, *sub* art. 2 *septies*, 85 ss. Cfr. FEROLA, *op. cit.*, 411 ss., spec. 424 ss. I commi 2° e 3° dell'art. 2 *septies* dettano norme di carattere procedurale con riguardo al provvedimento con cui il Garante adotta le misure di garanzia, mentre il comma 4° precisa, su un versante contenutistico, che le misure di garanzia, adottate nel rispetto dell'art. 9, par. 2, del Regolamento, riguardano anche le cautele da adottare, oltre che per contrassegni sui veicoli e accessi a zone a traffico limitato, anche relativamente a profili organizzativi e gestionali in ambito sanitario, modalità per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute nonché prescrizioni di medicinali. Tali aspetti erano precedentemente regolati dal Codice della privacy agli artt. 74, 83, 84 e 87 a 89, poi abrogati dal d.lgs. n. 101/2018.

sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione[137], le misure di minimizzazione, le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a garantire i diritti degli interessati».

In tal senso, le misure di garanzia vengono ad essere l'elemento chiave, per coniugare la limitata circolazione dei dati appartenenti alle categorie particolari e la sicurezza nel trattamento, nell'ottica del rispetto dei diritti dell'interessato.

Ma alle misure di garanzia è anche affidata, dal comma 6°, la possibilità di individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato, conformemente al disposto dell'art. 9, par. 4, del Regolamento, o «altre cautele specifiche».

La previsione è però limitata ai dati genetici. Non sembra ammissibile, quindi, che le misure di garanzia prevedano il consenso, pur come cautela ulteriore, quando si sia in presenza di un livello di rischio peculiare ed elevato, in relazione al trattamento di dati relativi alla salute[138].

Ricalcando il divieto contenuto al comma 5° dell'art. 26 del Codice della privacy, ora abrogato, l'art. 2 *septies*, comma 8°, vieta che tanto i dati relativi alla salute quanto i dati genetici e biometrici vengano diffusi. Dunque, il trattamento di dati relativi alla salute che possa definirsi come 'diffusione' resta perentoriamente vietato, a prescindere dal rispetto delle misure di garanzia[139].

Il d.lgs. n. 101/2018 ha così assegnato al Garante – attraverso l'adozione di specifiche misure di garanzia – il compito di completare le condizioni di ammissibilità del trattamento di dati relativi alla salute, genetici e biometrici[140].

---

[137] Questo è il termine che si legge nel testo normativo, laddove, probabilmente per un refuso, si sarebbe dovuto leggere "pseudonimizzazione".

[138] V. ZANOVELLO, in D'ORAZIO, FINOCCHIARO, POLLICINO, G. RESTA, (*op. cit.*, *sub* art. 2 *septies*, d.lgs. n. 196 del 2003, 1058), cui tale previsione risulta «per certi versi preoccupante». Per quanto attiene, invece, all'utilizzo dei dati biometrici, il comma 7°, ammettendolo, con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, richiede che avvenga in ogni caso nel rispetto delle misure di garanzia.

[139] La diffusione di questi dati, costituendo un illecito trattamento di dati personali, al pari della violazione delle misure di garanzia, sia soggetta, ai sensi dell'art. 166, comma 2°, del Codice della privacy, alla sanzione amministrativa pecuniaria più grave, di cui all'art. 83, par. 5, del Regolamento. ZANOVELLO, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 2 *septies*, d.lgs. n. 196 del 2003, 1062, in cui si ricorda anche la sanzione penale prevista dall'art. 167, comma 2°, del Codice della privacy.

[140] Si è di fronte a «un nuovo strumento regolatorio di competenza del Garante: quello costituito, appunto, dalla misure di garanzia che l'Autorità deve adottare». PIZZETTI, *La Parte I del Codice novellato*, cit., 117 s. A ciò si aggiunga la promozione delle regole deontologiche, da parte del Garante, ai sensi dell'art. 2 *quater* del Codice della privacy. Le disposizioni contenute nei codici di deontologia e di buona condotta, di cui agli

Inoltre, nella previsione di un periodo transitorio, con l'art. 21 ha affidato alla stessa Autorità, da una parte, l'individuazione e l'eventuale aggiornamento delle prescrizioni di cui alle autorizzazioni generali sul trattamento dei c.d. dati sensibili che fossero compatibili con la nuova normativa europea e con il decreto per l'adeguamento e, dall'altra, la verifica della conformità dei codici deontologici al Regolamento[141].

Dunque, individuate le prescrizioni contenute nelle autorizzazioni generali nn. 1, 3, 6, 8 e 9 del 2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 e deliberato l'avvio della consultazione pubblica[142], il Garante ha successivamente adottato il provvedimento che reca le prescrizioni relative alle situazioni di trattamento enunciate all'art. 21 d.lgs. n. 101/2018[143]. Tra queste non rientrano le prescrizioni di cui all'autorizzazione al trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, le quali si intende quindi abbiano cessato efficacia[144].

Oltre a quelle sul trattamento dei dati personali nei rapporti di lavoro, particolarmente importanti per i dati relativi alla salute sono le prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica[145], cioè quelle che erano contenute

---

allegati al Codice della privacy, ritenute compatibili dal Garante per la protezione dei dati personali, ai sensi dell'art. 20 d.lgs. n. 101/2018 hanno preso il nome di 'regole deontologiche' e sono state pubblicate nella Gazzetta Ufficiale della Repubblica italiana e poi, con decreto del Ministro della giustizia, riportate nell'allegato A del Codice della privacy. Così, a seguito del parere dell'Autorità garante del 29 novembre 2018, le "Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica" sono state pubblicate nella G.U. del 4 gennaio 2019, n. 3, e riportate nell'allegato A con decreto del Ministro della giustizia del 31 gennaio 2019; ugualmente è avvenuto per le "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica", le "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale", le "Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria" e le "Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica".

[141] Sempre in previsione del periodo transitorio, l'art. 22, comma 11°, d.lgs. n. 101/2018 ha stabilito che le disposizioni del Codice della privacy relative al trattamento di dati genetici, biometrici o relative alla salute oggetto di abrogazione, avrebbero continuato a trovare applicazione, in quanto compatibili con il reg. Ue n. 679/2016, sino all'adozione delle misure di garanzia di cui allo stesso art. 2 *septies*

[142] Provvedimento del Garante per la protezione dei dati personali del 13 dicembre 2018, n. 497, "Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice".

[143] Provvedimento del Garante per la protezione dei dati personali del 5 giugno 2019, n. 146, "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101".

[144] ZANOVELLO, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 2 *septies*, d.lgs. n. 196 del 2003, 1056

[145] Al punto 5.2, si precisa che le prescrizioni «concernono il trattamento di dati personali per finalità di ricerca medica, biomedica ed epidemiologica effettuati quando: il trattamento è necessario per la conduzione di studi effettuati con dati raccolti in precedenza a fini di cura della salute o per l'esecuzione di precedenti progetti di ricerca ovvero ricavati da campioni biologici prelevati in precedenza per finalità di tutela della salute o per

nell'autorizzazione generale n. 9/2016. In aggiunta al ruolo del consenso dell'interessato[146], emerge la rilevanza del principio di minimizzazione nelle modalità di trattamento e la misura della pseudonimizzazione come strumento per garantire sicurezza.

Al trattamento svolto a fini di ricerca scientifica o storica, oltreché di archiviazione nel pubblico interesse o statistici, ai sensi dell'art. 89 del Regolamento[147], è dedicato, nel Codice della privacy, il Titolo VII della Parte II[148].

Per quel che riguarda il trattamento di dati sensibili, si nota il persistere della cautela. Così l'art. 100, comma 1°, d.lgs. n. 196/2003, continua ad escluderli – come avveniva prima del d.lgs. n. 101/2018 – dai dati relativi ad attività di studio e di ricerca che, al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico, i soggetti pubblici, ivi comprese le università e gli enti di ricerca, possono con autonome determinazioni comunicare e diffondere, anche a privati e per via telematica, a laureati,

---

l'esecuzione di precedenti progetti di ricerca oppure il trattamento è necessario per la conduzione di studi effettuati con dati riferiti a persone che, in ragione della gravità del loro stato clinico, non sono in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso. In questi casi la ricerca deve essere effettuata sulla base di un progetto, oggetto di motivato parere favorevole del competente comitato etico a livello territoriale».

[146] Al consenso è dedicato il punto 5.3. Se la ricerca non è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea, «quando non è possibile acquisire il consenso degli interessati, i titolari del trattamento devono documentare, nel progetto di ricerca, la sussistenza delle ragioni, considerate del tutto particolari o eccezionali, per le quali informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca». Tra queste: 1. «i motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione»; 2. «i motivi di impossibilità organizzativa riconducibili alla circostanza che la mancata considerazione dei dati riferiti al numero stimato di interessati che non è possibile contattare per informarli, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati»; 3. «motivi di salute riconducibili alla gravità dello stato clinico in cui versa l'interessato a causa del quale questi è impossibilitato a comprendere le indicazioni rese nell'informativa e a prestare validamente il consenso». In quest'ultimo caso, si noti, andrà comprovata la necessità di trattare i dati della persona 'incapace', «avuto riguardo, in particolare, ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché all'attendibilità dei risultati conseguibili in relazione alle specifiche finalità dello studio. Con riferimento a tali motivi, deve essere acquisito il consenso delle persone indicate nell´art. 82, comma 2, lett. a), del Codice come modificato dal d.lgs. n. 101/2018».

[147] Sul tema v. UDA, *Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*, in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., 557 ss.

[148] Il d.lgs. n. 1010/2018 abbia modificato anche la rubrica della Parte II, recante ora "Disposizioni specifiche per i trattamenti necessari per adempiere ad un obbligo legale o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri nonché disposizioni per i trattamenti di cui al capo IX del regolamento". La nuova e più verbosa nomenclatura trova riscontro nell'art. 45 *bis*, unico articolo del novello Titolo 0.I, "Disposizioni sulla base giuridica", secondo cui le disposizioni contenute in questa parte sono stabilite in attuazione dell'art. 6, par. 2, nonché dell'art. 23, par. 1, del Regolamento. CAPORALE, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 45 *bis*, d.lgs. 30 giugno 2003, n. 196, 1174, parla di 'rinvio circolare', rispetto all'art. 2 *ter*.

dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi[149].

Direttamente rivolto al trattamento di dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, è l'art. 110[150].

Il consenso dell'interessato, come disposto dal comma 1°, non è necessario se «la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento». Altresì non è necessario «quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca». Si prevede che, in questi casi, il titolare del trattamento adotti misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato; oltre a ciò «il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento»[151].

Enunciando la norma i casi in cui non è necessario, il presupposto è che il consenso sia generalmente richiesto[152]. Come evidenziato in dottrina, il legislatore italiano si è limitato, qui, a "inoculare" nel tessuto normativo del d.lgs. n. 196/2003 il riferimento all'art. 9, par. 2,

[149] L'art. 107, invece, rubricato proprio "Trattamento di categorie particolari di dati personali", si limita a consentire che il consenso dell'interessato al trattamento di dati sensibili, qualora richiesto, possa essere prestato con modalità semplificate

[150] V. COMANDÉ, *Ricerca in sanità e data protection un puzzle... risolvibile*, in *Riv. it. med. leg*., 2019, 187 ss., il quale, tra l'altro, rileva – a p. 205 – come l'art. 7 delle "nuove" regole deontologiche sembri imporre il consenso quale unica base legittimante il trattamento dei dati sensibili, in contraddizione, almeno apparentemente, con l'art. 9 del Regolamento in combinato disposto con l'art. 89 del medesimo e con lo stesso art. 110 del Codice della privacy

[151] Si v., a tal proposito, il provvedimento del Garante per la protezione dei dati personali del 30 giugno 2022, n. 238, "Parere ai sensi dell'art. 110 del Codice e dell'art. 36 del Regolamento", in *www.dirittoegiustizia.it*, 11 agosto 2022, con annotazione di ALOVISIO, *Il parere dal Garante Privacy sulla realizzazione di una banca dati sanitaria per fini di ricerca*. Con tale provvedimento, l'Autorità ha espresso parere favorevole sulla realizzazione di una banca dati sanitaria per fini di ricerca, con trattamenti di dati anche di soggetti deceduti o non contattabili, prescrivendo di acquisire un consenso a fase progressive. Nel caso di specie, l'istanza di consultazione preventiva è stata presentata dall'Azienda ospedaliera universitaria integrata di Verona, come promotrice dello studio osservazionale interdipartimentale, prospettico, retrospettivo, non farmacologico denominato "DB Torax". Sul trattamento di dati personali a scopo di ricerca scientifica nell'ambito medico, la letteratura è ampia e assai variegata. *Ex plurimis*, oltre ai contributi già citati, AMRAM, *Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks*, in *Computer Law & Security Review*, vol. 37, 2020;;

[152] GUARDA, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 110, d.lgs. 30 giugno 2003, n. 196, 1370 ss., spec. 1374.

lett. *j*, del Regolamento[153], nonostante l'insieme delle disposizioni dettate in materia di finalità di ricerca avrebbe forse avuto bisogno di un ammodernamento più incisivo[154].

Meritano attenzione infine, per il rilievo che possono avere in relazione ai dati relativi alla salute, anche le disposizioni di cui all'art. 2 *terdecies* del Codice della privacy.

Come annunciato dal considerando 27 del Regolamento, esso non si applica ai dati personali delle persone decedute[155], ma «gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute». E nell'ordinamento italiano si occupa di tale trattamento, appunto, l'art. 2 *terdecies*.

Si tratta di una fattispecie che può svolgere un ruolo non trascurabile in riferimento ai dati sanitari, nella misura in cui la conoscenza delle condizioni di salute, in vita, del defunto sia non solo di interesse per la persona – non necessariamente un familiare – ma anche essenziale per la tutela della sua salute[156].

Così, ai sensi del comma 1°, i diritti di cui agli artt. da 15 a 22 del Regolamento riferiti ai dati personali inerenti a persone decedute possono esercitarsi da chi abbia un interesse proprio, o agisca a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione[157]. Pensiamo al diritto di accesso, sancito all'art. 15: è infatti molto importante avere, ad esempio, la possibilità di accedere ai dati sanitari di un parente defunto

[153]AURUCCI, *Protezione e libera circolazione dei dati personali nel contesto della ricerca medica in Italia. Risposte istituzionali ad un necessario nuovo bilanciamento*, in *Queste istituzioni*, 2022, fasc. 4, 174 ss., spec. 185 ss

[154] Il c.d. trattamento ulteriore è rimesso, dall'art. 110 *bis*, all'autorizzazione del Garante quando risulti problematico informare gli interessati. In ogni caso, al comma 4°, si precisa come il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, non costituisca trattamento ulteriore da parte di terzi

[155] È appena il caso di ricordare che la *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, proclamata solennemente da Parlamento europeo, Consiglio e Commissione europea, e firmata il 15 dicembre 2022, al punto 19 afferma che «ogni persona dovrebbe essere in grado di determinare la propria eredità digitale e decidere cosa succede, dopo la sua morte, ai propri account personali e alle informazioni che la riguardano».

[156] G. RESTA, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 2 *terdecies*, d.lgs. 30 giugno 2003, n. 196, 1115 ss., spec. 1119. Cfr. ID., *La successione nei rapporti digitali e la tutela post-mortale dei dati personali*, in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., 1361 ss.;

[157]Il comma 2° prosegue specificando che l'ammissibilità di questo esercizio può essere esclusa dalla legge oppure – ma solo con riguardo all'offerta diretta di *servizi della società dell'informazione* – dall'interessato, che lo abbia vietato per iscritto, comunicandolo al titolare del trattamento. Tale divieto: deve corrispondere a una volontà inequivoca, specifica, libera e informata; può essere parziale; è sempre revocabile o modificabile; non può arrecare pregiudizio all'esercizio, da parte di terzi, di diritti patrimoniali derivanti dalla morte dell'interessato e del diritto di difesa. Al di là dei profili che intersecano gli aspetti patrimoniali della successione, si può intendere come, anche in questo caso, le norme, che modellano la protezione dei dati personali, correlate all'evento della morte dell'interessato, si delineino informate al prevalente principio personalista e come declinazioni della dignità della persona.

o di una persona con cui si siano avuti rapporti sessuali, quando queste informazioni siano utili a fini terapeutici o di prevenzione o per ricostruire la propria condizione di salute, specialmente se si pensa alla natura 'condivisa' di tali dati. Si intuisce già la sfuggevolezza e, talvolta, l'indeterminatezza del confine fra dati relativi alla salute e dati genetici.

La protezione dei dati personali assume poi una rilevanza peculiare nel contesto della sanità pubblica[158]. In particolare, in questo ambito gioca un ruolo importante il trattamento dei dati sensibili, soprattutto quelli relativi alla salute[159].

L'intervento di adeguamento al Regolamento operato con il d.lgs. n. 101/2018 ha toccato, eccezion fatta per l'art. 93, tutte le disposizioni del Titolo V della parte II del Codice della privacy[160].

L'art. 75, d.lgs. n. 196 del 2003, ora recita: «Il trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere h) ed i), e 3 del regolamento, dell'articolo 2-septies del presente codice, nonché nel rispetto delle specifiche disposizioni di settore».

La nuova disposizione, nel sottinteso riferimento all'oggetto del trattamento costituito dai dati sensibili, fa rinvio ad altre norme, prime fra tutte quelle di cui all'art. 9 del Regolamento, soppiantando la precedente disposizione di carattere sostanzialmente declamatorio[161].

Ad essere richiamate sono quindi le eccezioni previste dal par. 2 dell'art. 9 che si traducono nella finalità di cura (lett. *h*) – con l'ulteriore precisazione normativa di cui al par. 3 – e nei motivi di interesse pubblico nel settore della sanità pubblica (lett. *i*).

Il trattamento di dati relativi alla salute – ma anche di dati personali appartenenti ad altre categorie particolari – quando avvenga per gli scopi menzionati, ricorrendo le necessità che

---

[158] Il tema è di importanza trasversale per il mondo delle professioni sanitarie e non, ed è stato affrontato anche attraverso studi dal taglio pratico. V., *ex multis*, MULÀ, *La tutela della privacy in ambito sanitario*, Santarcangelo di Romagna, Maggioli, 2018; CARRO *et al*., *La privacy nella sanità*, Milano, Giuffrè, 2017; POLITO *et al.* (a cura di), *Sicurezza e privacy in ambito sanitario*, Roma, Edisef, 2012; R. TOMMASI, *La difesa della privacy nella sanità*, Santarcangelo di Romagna, Maggioli, 2007

[159] MONTISCI, *Trattamento dei dati personali ed attività sanitaria*, in DE BELVIS (a cura di), *op. cit.*, 111 ss. Offre un inquadramento generale DURST, *Il trattamento di categorie particolari di dati in ambito sanitario*, in PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, cit., 65 ss.

[160]Molti degli articoli che componevano questo titolo sono stati abrogati: artt. 76, 81, 83, 84, 85, 86, 87, 88, 89, 90, 91 e 94. Cfr. GRECO, *Sanità e protezione dei dati personali*, cit., 263 ss

[161] V. POLETTI, in C.M. BIANCA e BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196, Codice della privacy*, Padova, CEDAM, 2007, *sub* art. 75, 1195 ss. Cfr. CECAMORE, in SCIAUDONE e CARAVÀ (a cura di), *op. cit*., *sub* art. 75, 277 ss.

sono alla base di dette deroghe, prescinde dal consenso dell'interessato.

Deve inoltre essere conforme alle misure di garanzia, *ex* art. 2 *septies* del Codice della privacy, e rispettare anche le 'specifiche disposizioni di settore'. Con tale formula l'art. 75 fa rinvio ad altre norme, anche di livello non primario, tracciate sempre con riguardo al trattamento di dati personali per finalità di tutela della salute. In questo caso, il riferimento può essere, ad esempio, alla disciplina del trattamento dei dati operato mediante il fascicolo sanitario elettronico[162].

L'art. 75 non aggiunge dunque una vera e propria nuova disposizione in sé, ma ribadisce l'effetto di altre norme. Potrebbe avrere un carattere programmatico, poichè, non menzionando il consenso, sembrerebbe contenere l'idea di un suo formale superamento, almeno nell'area del trattamento dei dati in ambito sanitario[163].

Ma quanto dichiarato all'art. 75 non incide sulla portata applicativa dell'art. 9 del Regolamento. Così potrà aversi un trattamento di dati relativi alla salute o dati personali di altre particolari categorie, pure in ambito sanitario, che si regge su una delle eccezioni del par. 2, diversa da quelle di cui alle lett. *h* o *i*. Il trattamento di dati sulla salute in ambito sanitario si potrà svolgere, quindi, anche sulla base del consenso esplicito dell'interessato, non avendo l'ordinamento italiano disposto che l'interessato non possa revocare il divieto di cui al par. 1, ai sensi del par. 2, lett. *a*, o sulla base di altre deroghe, come ad esempio quella dettata dalla lett. *g*, cioè quando sia necessario per motivi di interesse pubblico rilevante. A tal proposito, l'art. 2 *sexies* del Codice della privacy, al citato nuovo comma 1 *bis*, esprime l'assunto per cui il trattamento di dati relativi alla salute, *ex* art. 9, par. 2, lett. *g*, del Regolamento, è quello effettuato anche attraverso il fascicolo sanitario elettronico, di cui si tratterà nei prossimi capitoli.

Qualora invece un trattamento di dati relativi alla salute o di altri dati sensibili, pure collocandosi nell'ambito sanitario, non sia sorretto da nessuna delle necessità di cui al par. 2 dell'art. 9 e nemmeno dall'ipotesi della lett. *d*, dovrà ricondursi al consenso dell'interessato, pena la violazione del divieto di cui al par. 1.

Il contenuto delle disposizioni 'superstiti' del Titolo V, preannunciato dall'art. 77 del Codice della privacy, è costituito dalle modalità particolari per informare l'interessato e

[162] Si v. il d.P.C.m., 29 settembre 2015, n. 178, recante il "Regolamento in materia di fascicolo sanitario elettronico".

[163] Ogni riferimento al consenso è stato espunto dalle disposizioni di questo Titolo, «per effetto della mutata *ratio* normativa». DI MASI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 75, d.lgs. 30 giugno 2003, n. 196, 1237

trattare i suoi dati[164].

Dinanzi alla mutata prospettiva nei confronti del consenso, acquista un ruolo più pregnante l'informazione al paziente[165].

Posto che gli elementi dell'informativa sono quelli dettati agli artt. 13 e 14 del Regolamento[166], l'art. 78 dispone che il medico di medicina generale, così come il pediatra di libera scelta, informi l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili detti elementi, conformemente al principio di trasparenza[167].

Vanno evidenziati, da parte sua, «analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato». E ciò, in particolare, nel caso di trattamenti effettuati: «a) per fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente; b) nell'ambito della teleassistenza o telemedicina; c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica; c-bis) ai fini dell'implementazione del *fascicolo sanitario elettronico* di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 di cembre 2012, n. 221; c-ter) ai fini dei sistemi di sorveglianza e dei registri di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221».

Si comprende da ciò, come si sia voluto tutelare l'interessato paziente, con precetti che garantiscano un raggiungimento di consapevolezza in ordine al trattamento dei dati che lo

---

[164] Il comma 2° dell'art. 77 si occupa del profilo soggettivo di applicazione. Sulle professioni sanitarie, RODRIGUEZ, *Le figure professionali*, in LENTI, PALERMO FABRIS e ZATTI (a cura di), *I diritti in medicina*, nel *Trattato di biodiritto*, diretto da Rodotà e Zatti, Milano, Giuffrè, 2011, 115 ss. Cfr. PIOGGIA, *Diritto sanitario e dei servizi sociali*, 3a ed., Torino, Giappichelli, 2020.

[165] DI MASI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 77, d.lgs. 30 giugno 2003, n. 196, 1244 ss.

[166] Sembra opportuno ricordare come, in dottrina, si sia sostenuta la configurabilità di una responsabilità contrattuale in caso di violazione degli obblighi informativi sanciti dal Regolamento e dal Codice della privacy, in quanto si tratterebbe dell'inadempimento di obbligazioni derivanti *ex lege*. F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, 389 s.

[167] DI MASI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 78, d.lgs. 30 giugno 2003, n. 196, 1255, osserva che «la lettura sistematica della disposizione evidenzia come il criterio ispiratore della particolarità delle modalità informative non abbia inciso sulla riduzione dei contenuti informativi, ma abbia inciso o sull'alleggerimento degli adempimenti informativi altrimenti necessari per più trattamenti di dati personali o sulla previsione di specifici oneri formali e comunicativi».

riguardano, specialmente quando il trattamento avvenga con gli strumenti informatici, come oggi accade maggiormente[168]. Da tale previsione si può peraltro ricavare ancora come l'attività di trattamento si presenti rischiosa particolarmente quando si realizzi attraverso la rete, come avviene appunto mediante fascicolo sanitario elettronico.

Le modalità descritte sono estese, dall'art. 79, alle strutture che erogano prestazioni sanitarie e socio-sanitarie, le quali, sulla base di adeguate misure organizzative, possono avvalersene «in modo omogeneo e coordinato in riferimento all'insieme dei trattamenti di dati personali effettuati nel complesso delle strutture facenti capo alle aziende sanitarie» per più trattamenti di dati[169].

L'informazione al paziente sul trattamento dei suoi dati personali deve precedere la prestazione medica, eccezion fatta per i casi di emergenza e tutela della salute e dell'incolumità fisica enunciati all'art. 82. La regola contribuisce alla conferma del fatto che nella prestazione sanitaria il trattamento dei dati relativi alla salute viene a costituire momento funzionale, per non dire coessenziale, alla sua esecuzione[170].

---

[168] La disciplina dell'informativa da parte del medico è completata dalle disposizioni secondo cui le informazioni possono essere fornite per il trattamento complessivo e riguardano anche il trattamento correlato.

[169] La proiezione della tutela propria della protezione dei dati personali nel contesto dell'organizzazione sanitaria e socio-sanitaria operata da questa norma può leggersi come un potenziamento della relazione di cura a favore del paziente. «Ciò perché l'idea di fondo è che occorra tradurre il principio personalistico alla base della Costituzione (art. 2) in indicazioni organizzative di portata strutturali, capaci di attuare concretamente i diritti sociali e fondamentali riconosciuti a livello nazionale e sovranazionale e di mettere al centro delle organizzazioni pubbliche e private che erogano servizi sanitari e socio-sanitari l'obiettivo del pieno sviluppo della persona». DI MASI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 79, d.lgs. 30 giugno 2003, n. 196, 1264. Cfr. PIOGGIA, *Diritto sanitario e dei servizi sociali*, 3a ed., Torino, Giappichelli, 2020. Della facoltà di fornire un'unica informativa per una pluralità di trattamenti di dati effettuati, a fini amministrativi e in tempi diversi, rispetto a dati raccolti presso l'interessato e presso terzi, possono avvalersi anche i soggetti di cui all'art. 80, ossia i competenti servizi o strutture di altri soggetti pubblici, diversi da quelli di cui all'art. 79, operanti in ambito sanitario o della protezione e sicurezza sociale.

[170] FINOCCHIARO, *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, cit., 213 ss. Con riguardo, invece, al trattamento effettuato per la prescrizione di medicinali, l'art. 89 *bis* dispone che si adottino 'cautele particolari' in relazione alle misure di garanzia del Garante, anche al di là della finalità di cura.

2.2 La cartella clinica

Alla modalità di trattamento di dati sulla salute che storicamente più ha contraddistinto i sistemi sanitari, cioè il trattamento operato per mezzo della cartella clinica, è dedicato l'art. 92[171].

Il d.lgs. n. 101 del 2018 non ha inciso molto sul testo di questo articolo. Dopo aver disposto, al comma 1°, che opportuni accorgimenti sono adottati per garantire la comprensibilità dei dati e per distinguere quelli relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri, al comma 2° regola l'esercizio del diritto di accesso, prevedendo che la richiesta, da parte di soggetti diversi dall'interessato, di presa visione o rilascio di copia possa trovare accoglimento solo in caso di necessità documentata di esercitare o difendere un diritto in sede giudiziaria, ai sensi dell'art. 9, par. 2, lett. *f*, del Regolamento, di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale, oppure di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale.

La privacy del paziente si è dovuta misurare quindi con le esigenze, di carattere pubblico, di trasparenza nell'operato della pubblica amministrazione e di tutela dei diritti. In tal senso va letta la garanzia del diritto di accesso[172]. A un approccio che avrebbe visto nel rapporto fra questi diritti un conflitto risolvibile sulla base di una scala gerarchica astrattamente definita, è apparso preferibile – e certamente conforme ai principi dell'ordinamento – procedere attraverso il bilanciamento, tenendo conto delle specificità del caso concreto e delle circostanze in cui vengono esercitati tali diritti[173].

Il criterio stabilito dal legislatore nel garantire il diritto di accesso[174], a fronte del diritto alla riservatezza, è quello del 'pari rango' della situazione giuridica che si intende far

[171] BARILÀ e CAPUTO, *Problemi applicativi della legge sulla privacy: il caso delle cartelle cliniche,* in *Pol dir*., 1998, 275 ss.

[172] Su diritto di accesso e privacy, si v., *ex plurimis*, M.A. SANDULLI, voce «Accesso alle notizie e ai documenti amministrativi», cit., 1 ss. Cfr. CIMINI, *Accesso ai documenti amministrativi e riservatezza: il legislatore alla ricerca di nuovi equilibri,* in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *Il codice del trattamento dei dati personali,* cit., 325 ss.

[173] SARTORETTI, *La cartella clinica tra diritto all'informazione e diritto alla privacy*, cit., 591

[174] BAICE, *La cartella clinica tra diritto di riservatezza e diritto di accesso*, in *La resp. civ.*, 2008, 169 ss.

valere[175]. Riprendendo quindi lo schema tracciato dagli artt. 24, l. n. 241 del 1990, e 60 del Codice della privacy, l'art. 92 prevede che il diritto di accesso alla cartella clinica sia riconosciuto a chi lo richiede avendo la necessità di tutelare una 'situazione giuridicamente rilevante', che sia almeno di *pari rango* rispetto ai diritti dell'interessato o consistente "in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile", o la necessità di "far valere o difendere un diritto in sede giudiziaria" che abbia le medesime caratteristiche[176].

Interseca il trattamento dei dati relativi alla salute operato per mezzo della cartella clinica l'ulteriore complessa questione – che ci si limita a ricordare soltanto – che attiene invece al rapporto fra la tutela della riservatezza dell'identità delle madri che al momento del parto si sono avvalse del diritto di non essere nominate e l'accesso alla documentazione da parte degli interessati. La volontà della madre di rimanere anonima è garantita infatti dall'ordinamento dello stato civile, nel dettaglio, dall'art. 30, comma 1°, d.P.R. 3 novembre 2000, n. 396, ove è sancito che «la dichiarazione di nascita è resa [...] rispettando l'eventuale volontà della madre di non essere nominata». Alla norma rinviano le scarne disposizioni di cui all'art. 93 del Codice della privacy. Ancora una volta il legislatore è chiamato a misurarsi

[175] V. FARES, *The processing of personal data concerning health according to the EU Regulation*, cit., 37, che riscontra l'applicazione del c.d. «pari passu *rank criterion used in many national laws, including the Italian one*», nella giurisprudenza sovranazionale.

[176] Al riguardo, il Garante per la protezione dei dati personali, nella pronuncia del 9 luglio 2003 [doc web n. 29832], ha affermato che, in caso di richiesta di un terzo di conoscere dati sulla salute o la vita sessuale, oppure di accedere a documenti che li contengono, quali la cartella clinica, il «destinatario della richiesta, nel valutare il "rango" del diritto di un terzo che può giustificare l'accesso o la comunicazione, deve utilizzare come parametro di raffronto non il "diritto di azione e difesa" che pure è costituzionalmente garantito (e che merita in generale protezione a prescindere dall'"importanza" del diritto sostanziale che si vuole difendere), quanto questo diritto sottostante che il terzo intende far valere sulla base del materiale documentale che chiede di conoscere. Ciò chiarito, tale sottostante diritto […] può essere ritenuto di "pari rango" rispetto a quello dell'interessato – giustificando quindi l'accesso o la comunicazione di dati che l'interessato stesso intende spesso mantenere altrimenti riservati – solo se fa parte della categoria dei diritti della personalità o è compreso tra altri diritti o libertà fondamentali ed inviolabili». Richiamando Cons. Stato n. 1882/2001, cit., ha proseguito considerando che «nella prevalenza dei casi riguardanti meri diritti di credito non sia possibile accogliere l'istanza di accesso o di comunicazione, e che si possa invece valutare, con cautela, caso per caso, l'effettiva necessità di consentire l'accesso ad una cartella clinica – prima della sua probabile acquisizione su iniziativa del giudice – in caso di controversia risarcitoria per danni ascritti all'attività professionale medica documentata nella cartella. Il riferimento normativo ai diritti della personalità e ad altri diritti e libertà fondamentali è collegato ad un "elenco aperto" di posizioni soggettive individuabile in chiave storico-evolutiva, e presuppone una valutazione in concreto, in modo da evitare per le amministrazioni, gli altri destinatari delle richieste e per il giudice stesso in caso di impugnazione, "il rischio di soluzioni precostituite poggianti su una astratta scala gerarchica dei diritti in contesa"». V. anche TESSARO, *Rapporto tra accesso e* privacy *nella Pubblica Amministrazione: problemi giuridici e applicativi*, in G.F. FERRARI (a cura di), *op. cit.*, 178. Cfr., sull'accesso ai documenti sanitari, BOLOGNINI, *Trasparenza dei dati e tutela della privacy*, in GELLI *et al.*, *Responsabilità, rischio e danno in sanità. La sicurezza delle cure dopo la pandemia COVID-19*, Milano, Giuffrè, 2022, 1103 ss.; MAROTTA, *Ordinamento sanitario e diritto di accesso: analisi della giurisprudenza amministrativa*, in *Corti supreme e salute*, 2021, fasc. 3, 587 ss.; VARANI, *Il diritto di accesso ai documenti amministrativi contenenti dati sanitari*, in *Foro amm. - TAR*, 2005, 929 ss.

con una scelta e con un bilanciamento, in questo caso fra il diritto all'anonimato materno e il diritto a conoscere le proprie origini[177].

Il rapporto fra l'impiego della cartella clinica e il trattamento dei dati personali che avviene per mezzo di esso attesta le molteplici declinazioni del diritto alla riservatezza in ambito sanitario. Il Garante per la protezione dei dati personali stesso è intervenuto numerose volte definendo i diritti dell'individuo con riferimento al trattamento dei dati che viene effettuato con la compilazione della cartella clinica[178].

---

[177] Il tema, in modo particolare, è stato affrontato in giurisprudenza, trasversalmente. V. Corte EDU, 25.9.2012, n. 33783/09, in *Giust. civ.*, 2013, I, 1597 ss., con nota di INGENITO, *Il diritto del figlio alla conoscenza delle origini e il diritto della madre al parto anonimo alla luce della recente giurisprudenza della Corte europea dei diritti dell'uomo*; Corte cost., 22.11.2013, n. 278, in *Corr. giur.*, 2014, 471 ss., con nota di AULETTA, *Sul diritto dell'adottato di conoscere la propria storia: un'occasione per ripensare alla disciplina della materia*; in *Nuova giur. civ. comm.*, 2014, I, 279 ss., con nota di MARCENÒ, *Quando da un dispositivo d'incostituzionalità possono derivare incertezze*, e con nota di LONG, *Adozione e segreti: costtuuzionalmente illegittima l'irreversibilità dell'anonimato del parto*; in *Fam. e dir.*, 2014, 11 ss., con nota di CARBONE, *Un passo avanti del diritto del figlio, abbandonato e adottato, di conoscere le sue origini rispetto all'anonimato materno*; in *Dir. fam. e pers.*, 2014, 13 ss., con nota di LISELLA, *Volontà della madre biologica di non essere nominata nella dichiarazione di nascita e diritto dell'adottato di conoscere le proprie origini*; Cass., sez. un., 25.1.2017, n. 1946, in *Fam. e dir.*, 2017, 740 ss., con nota di P. DI MARZIO, *Parto anonimo e diritto alla conoscenza delle origini*; in *Corr. giur.*, 2017, 618 ss., con nota di BUGETTI, *Sul difficile equilibrio tra anonimato materno e diritto alla conoscenza delle proprie origini: l'intervento delle Sezioni Unite*. In dottrina, fra tanti, CHECCHINI, *La giurisprudenza sul parto anonimo e il nuovo «istituto» dell'interpello*, in *Nuova giur. civ. comm.*, 2017, II, 1288 ss.; F. GIARDINA, *Interesse del minore: gli aspetti identitari*, in *Nuova giur. civ. comm.*, 2016, II, 159 ss.; GRANELLI, *Il c.d. "parto anonimo" ed il diritto del figlio alla conoscenza delle proprie origini: un caso emblematico di "dialogo" fra corti*, in *Jus civile*, 2016, 564 ss.; M.G. STANZIONE, *Identità del figlio e diritto di conoscere le proprie origini*, Torino, Giappichelli, 2015. Cfr. BOZZI, *Il diritto di conoscere le proprie origini*, in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., 1323 ss. V., anche per ulteriori riferimenti, ZANOVELLO, *Anonimato materno e diritto dell'adottato a conoscere le proprie origini: la parola al legislatore*, in *Studium iuris*, 2019, 1183 ss.

[178] L'attività del Garante in questa materia risale al tempo in cui vigeva ancora la l. n. 675 del 1996. Così il 12 ottobre 1999 ha chiarito che «i dati contenuti nelle cartelle cliniche non possono essere cancellati, ma è ammessa una loro rettifica o integrazione». Lo si è stabilito in un provvedimento con cui è stato dichiarato infondato il ricorso presentato da un cittadino che aveva chiesto ad una Asl la cancellazione di tutte le informazioni personali che lo riguardavano. «La richiesta, avanzata dal ricorrente, di provvedere alla cancellazione o, in subordine, al blocco dei dati, traeva origine dal fatto che le informazioni contenute nella propria cartella clinica sarebbero state confuse, non chiare e fondate su valutazioni estranee al campo medico e diagnostico e, comunque, non necessarie all'attività di salvaguardia dell'incolumità pubblica e del soggetto interessato». Il Garante non ha accolto la richiesta di cancellazione o di blocco dei dati della cartella clinica, perché il trattamento è avvenuto nel rispetto della legge e nell'ambito delle attività istituzionalmente affidate all'Azienda sanitaria locale. «L'Autorità ha precisato che è comunque consentito all'interessato di ottenere l'eventuale aggiornamento, rettifica, oppure, per motivi legittimi ed oggettivi, l'integrazione dei dati contenuti nella cartella sanitaria: ad esempio, attraverso l'inserimento di annotazioni sulle risultanze di accertamenti successivamente effettuati presso altri organismi sanitari accreditati». V. Comunicato stampa del 12 ottobre 1999, *Cartelle cliniche e cancellazione dati sensibili*, consultabile in *www.garanteprivacy.it*. affermato che, nel caso in cui la grafia con cui sia stata redatta una cartella clinica risulti incomprensibile per l'interessato, Con provvedimento del 30 settembre 2002 [doc web n. 1066144], *ivi*, invece, il Garante ha stabilito che il paziente ha il diritto di ottenere da parte della struttura sanitaria una trascrizione dattiloscritta o, comunque, comprensibile

Giova appena rammentare come, lungi dall'esaurirsi sul piano della privacy, il ruolo della cartella clinica si è potuto riscontrare in diversi ambiti dell'ordinamento giuridico e, in particolare, in relazione al sistema del diritto privato, in materia di responsabilità civile, nel dettaglio, della responsabilità medica[179].

Posto che la difettosa o incompleta tenuta della cartella clinica di per sé può costituire inadempimento in capo al sanitario, si è affermato come la lacunosità della cartella clinica sia circostanza di fatto che il giudice di merito può utilizzare per ritenere dimostrata l'esistenza di un nesso causale valido tra l'operato del medico e il danno patito dal paziente. Anche se non in modo automatico, ma solo quando l'esistenza del nesso eziologico tra condotta del medico e danno del paziente non possa essere accertata proprio a causa della incompletezza della cartella e il medico abbia, comunque, posto in essere una condotta astrattamente idonea a

---

delle informazioni contenute, che debbono essergli comunicate tramite un medico all'uopo designato, dal momento che la leggibilità dei dati richiesti è la prima condizione, necessaria ancorché non sufficiente, per la loro comprensione. I dati inseriti nella cartella clinica però devono essere corretti e rispondenti alla realtà e ciò vale per tutti i dati, non solamente per quelli di natura strettamente sanitaria. L'interessato ha infatti diritto di ottenere la rettifica pure dei dati relativi alle circostanze in cui si è verificato l'incidente che ha portato il paziente a ricoverarsi. V., al riguardo, il provvedimento del 19 maggio 2005 [doc. web n. 1151236], *ivi*. Nel caso di specie, il ricorrente aveva chiesto la rettifica di un dato personale relativo al proprio figlio minore contenuto nella cartella clinica redatta dalla struttura ospedaliera resistente a seguito di una visita di pronto soccorso. In occasione di quella visita, aveva dichiarato al medico di turno che il minore si era infortunato cadendo da una giostra e che il medico aveva invece annotato nella cartella clinica una frase diversa ("*APP: oggi riferita caduta accidentale*"). Perciò era stata chiesta la rettifica, per inserire l'indicazione delle esatte circostanze del sinistro. Con provvedimento del 13 luglio 2006 [doc web n. 1320728], *ivi*, si è chiarito poi che la conservazione delle cartelle cliniche è obbligatoria, «anche alla luce delle disposizioni in materia di archivi, delle indicazioni emergenti dalle direttive sinora impartite dal Ministero competente (cfr. circolare del Ministero della sanità 19 dicembre 1986, n. 61), nonché delle disposizioni di cui al d.m. 27 ottobre 2000, n. 380 ("Regolamento recante norme concernenti l'aggiornamento della disciplina del flusso informativo sui dimessi dagli istituti di ricovero pubblici e privati")». E tale obbligo di conservazione prevale sulla richiesta di cancellazione o trasformazione in forma anonima dei dati personali contenuti nella cartella clinica, quando il trattamento e la conservazione siano effettuati con l'osservanza della disciplina sancita dal Codice della privacy. Si può osservare, peraltro, che in quel caso la cartella clinica dei cui dati si chiedeva la cancellazione o la trasformazione in forma anonima era stata redatta in occasione di un ricovero avvenuto nel 1985 e risultava conservata sino al 2006, quando veniva presentato il ricorso.

[179] Pure del rilievo della cartella clinica e della relativa declinazione del principio dell'onere della prova si è occupata la storica Cass., sez. un., 11.1.2008, n. 577, in *Nuova giur. civ. comm.*, 2008, I, 612 ss., con nota di DE MATTEIS, *La responsabilità della struttura sanitaria per danno da emotrasfusione*; in *La resp. civ.*, 2008, 397 ss., con nota di CALVO, *Diritti del paziente,* onus probandi *e responsabilità della struttura sanitaria*; in *La resp. civ.*, 2008, 687 ss., con nota di DRAGONE, *Le S.U., "la vicinanza della prova" e il riparto dell'onere probatorio*; in *Giur. it.*, 2008, 1653 ss., con nota di CIATTI, *Crepuscolo della distinzione tra le obbligazioni di mezzi e le obbligazioni di risultato*; in *Giur. it.*, 2008, 2197 ss. con nota di CURSI, *Responsabilità della struttura sanitaria e riparto dell'onere probatorio*; in *Danno e resp.*, 2008, 788 ss., con nota di VINCIGUERRA, *Nuovi (ma provvisori?) assetti della responsabilità medica*; in *Danno e resp.*, 2008, 871 ss., con nota di NICOLUSSI, *Sezioni sempre più unite contro la distinzione fra obbligazioni di risultato e obbligazioni di mezzi. La responsabilità del medico*; in *La resp. civ.*, 2009, 221 ss., con nota di MIRIELLO, *Nuove e vecchie certezze sulla responsabilità medica*.

causare il danno[180].

Sull'uso della "tradizionale" cartella clinica ha ovviamente inciso, come è facilmente immaginabile, la digitalizzazione della sanità. Al cartaceo si è affiancato l'elettronico e medici e sanitari hanno cominciato a utilizzare l'*electronic health record* (EHR), la cartella clinica elettronica, che riporta le informazioni e i documenti inerenti allo specifico percorso di cura[181]. Dati relativi alla salute, unitamente a varie altre tipologie di dati, comuni o sensibili, hanno iniziato ad essere raccolti in formato digitale[182].

---

[180] Si v. Cass., 12.6.2015, n. 12218, in *DeJure*.

[181] La cartella clinica elettronica è definita dal Gruppo Articolo 29, *Documento di lavoro sul trattamento di dati personali relativi alla salute nelle cartelle cliniche elettroniche (EHR)*, cit., 4, come «documentazione medica completa o documentazione analoga sullo stato di salute fisico e mentale, passato e presente, di un individuo, in forma elettronica, e che consenta la pronta disponibilità di tali dati per cure mediche ed altri fini strettamente collegati», aggiungendo che risulta un mezzo adeguato per «migliorare la qualità delle cure fornendo informazioni più complete sul paziente; migliorare l'efficienza economica delle cure mediche evitando così un'ulteriore, rapida crescita del deficit del bilancio sanitario; fornire i dati necessari per un controllo della qualità, per le statistiche e per la pianificazione nel settore sanitario pubblico, provocando effetti positivi per il suo bilancio». La menzionata definizione è ripresa dalla Raccomandazione della Commissione, del 2 luglio 2008, sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche, punto 3, lettera c). V. AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI, CORTE EUROPEA DEI DIRITTI DELL'UOMO e CONSIGLIO D'EUROPA (a cura di), *Manuale sul diritto europeo in materia di protezione dei dati*, cit., 378 ss. Va detto, peraltro, che le definizioni di cartella clinica elettronica, fascicolo sanitario elettronico o di dossier sanitario presentano confini sfumati e non sempre è agevole distinguere in pratica gli strumenti digitali cui si riferiscono.

[182] Art. 47 *bis* d.l. 9 febbraio 2012, n. 5, "Semplificazione in materia di sanità digitale": «1. Nei limiti delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, nei piani di sanità nazionali e regionali si privilegia la gestione elettronica delle pratiche cliniche, attraverso l'utilizzo della cartella clinica elettronica, così come i sistemi di prenotazione elettronica per l'accesso alle strutture da parte dei cittadini con la finalità di ottenere vantaggi in termini di accessibilità e contenimento dei costi, senza nuovi o maggiori oneri per la finanza pubblica. 1-*bis*. A decorrere dal 1° gennaio 2013, la conservazione delle cartelle cliniche può essere effettuata, senza nuovi o maggiori oneri a carico della finanza pubblica, anche solo in forma digitale, nel rispetto di quanto previsto dal decreto legislativo 7 marzo 2005, n. 82, e dal decreto legislativo 30 giugno 2003, n. 196. 1-*ter*. Le disposizioni del presente articolo si applicano anche alle strutture sanitarie private accreditate». Sulle cartelle cliniche elettroniche la letteratura è pressoché sconfinata. *Ex multis*, GLENNIE, *Electronic Health Records: Where They Are Now and Where They Need to Be*, in MA (a cura di), *Clinical Costing Techniques and Analysis in Modern Healthcare Systems*, Hershey, IGI Global, 2019, 87 ss.; EVANS, *Electronic Health Records: Then, Now, and in the Future*, in *Yearbook of Medical Informatics*, 2016, *Special 25th Anniversary Edition*, 48 ss.; HOFFMAN, *Electronic Health Records and Medical Big Data. Law and policy*, Cambridge University Press, 2016; DE MINICO, *Electronic health record: political issues and privacy*, in *www.apertacontrada.it*, 18 dicembre 2015; TURK, *Electronic Health Records: How to Suture the Gap Between Privacy and Efficient Delivery of Healthcare*, in *Brooklyn Law review*, vol. 80, n. 3, 2015, 565 ss.; WANG, *Security and privacy of personal health record, electronic medical record and health information*, in *Problems and Perspectives in Management*, 2015, vol. 13, n. 4, 19 ss.; HARMAN *et al*., *Electronic Health Records: Privacy, Confidentiality, and Security*, in *Virtual Mentor. American Medical Association Journal of Ethics*, 2012, vol. 14, n. 9, 712 ss.; MIRON-SHATZ e ELWYN, *To serve and protect? Electronic health records pose challenges for privacy, autonomy and person-centered medicine*, in *The International Journal of Person Centered Medicine*, 2011, vol. 1, 405 ss. Più risalente ROSCAM ABBING, *Medical Confidentiality and Electronic Patient Files*, in *Medicine and Law*, vol. 19, n. 1, 2000, 107 ss. Cfr., anche per riferimenti

La raccolta dei dati personali del paziente è stata poi organizzata, sempre attraverso dispositivi informatici o digitali, mediante il fascicolo sanitario elettronico e il *dossier* sanitario. Trattasi di strumenti diversi, tanto per struttura quanto per funzione.

Mentre il fascicolo sanitario, infatti, è una sorta di banca dati generale dell'assistito, il dossier sanitario è una raccolta di dati sanitari svolta da un unico soggetto titolare del trattamento[183], come una struttura, e ad esso afferente, cioè potenzialmente inerente a più percorsi di cura del paziente presso lo stesso ente.

Tutti questi strumenti, che appaiono come innovazione ed evoluzione della 'vecchia' cartella clinica, non l'hanno però sostituita del tutto, poiché essa continua a rivestire un importante funzione documentale.

2.3 I chiarimenti del Garante per la protezione dei dati personali sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario

Con l'entrata in vigore del reg. Ue n. 679 del 2016 – e le modifiche apportate alle disposizioni del Codice della privacy da parte del d.lgs. n. 101 del 2018 – sono sorti dubbi interpretativi e applicativi in ordine alla normativa sul trattamento dei dati sanitari.

Così, con provvedimento del 7 marzo 2019, n. 55[184], il Garante per la protezione dei dati personali ha fornito chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario.

---

bibliografici, ARCHER *et al*., *Personal health records: a scoping review*, in *Journal of the American Medical Informatics Association*, 2011, vol. 18, n. 4, 515 ss. Ancora, sui profili probatori, R. CARLEO, *Cartella clinica elettronica e profili probatori nella responsabilità sanitaria*, in *Resp. med*., 2021, 99 ss. Si osserva pure che, alla protezione dei dati relativi alla salute negli *electronic health records*, è stato dedicato il Capo XII della citata *Recommendation on the Protection and Use of Health-Related Data*, del 6 novembre 2019, nell'ambito delle Nazioni Unite.

[183] A. THIENE, *Salute, riserbo e rimedio risarcitorio*, in *Riv. it. med. leg*., 2015, 1407 ss., spec. 1421

[184] Il provvedimento del Garante per la protezione dei dati personali del 7 marzo 2019, n. 55, cit., è stato adottato ai sensi degli artt. 57, par. 1, lett. *b* e *d*, del Regolamento e 154, comma 1°, lett. *g*, del d.lgs. n. 101/2018. È commentato da BUSCA, *Chiarimenti sull'applicazione della disciplina di protezione dei dati in ambito sanitario*, in *www.rivistaresponsabilitamedica.it*, 8 aprile 2019; ALOVISIO, *Primi chiarimenti del Garante privacy sul trattamento dei dati in ambito sanitario*, in *www.dirittoegiustizia.it*, 21 marzo 2019; D'AGOSTINO PANEBIANCO, *Il trattamento dei dati nel Sistema Sanitario Nazionale italiano alla luce del Provvedimento del Garante del 7 marzo 2019*, in *Ciberspazio e diritto*, 2019, 241 ss.; M. FOGLIA, *Patients and privacy: GDPR compliance for healthcare organizations*, in *European Journal of Privacy Law & Technologies*, 2020, Special Issue, 43 ss. V. anche CUTTAIA, *The impact of EU Regulation 2016/679 on the Italian health system*, in FARES (a cura di), *op. cit.*, 195 ss., spec. 200 s.; COLANGELO, *App mediche e protezione dei dati personali. Alcuni spunti giuridici tra Gdpr, codice privacy novellato e chiarimenti del Garante*, in *Autonomie locali e servizi sociali*, 2019, fasc. 2, 275 ss., spec. 278 s. Sia concesso di nuovo il rimando a S. CORSO, *Sul trattamento dei dati relativi alla salute in ambito sanitario: l'intervento del Garante per la protezione dei dati personali*, cit., 225 ss.

Tale provvedimento è stato adottato, in particolare, a seguito dell'esame, da parte dell'Autorità garante, delle segnalazioni e dei quesiti che hanno sollevato dubbi sull'interpretazione delle disposizioni, oggi differenti, riguardanti il trattamento dei dati sulla salute nel settore sanitario, nonché avendo ritenuto opportuno supportare i soggetti operanti in tale ambito nel processo di attuazione della disciplina e favorire un'interpretazione uniforme del nuovo assetto normativo, fornendo orientamenti utili per i cittadini e gli operatori del settore, specialmente con riferimento ai responsabili della protezione dei dati.

Dopo aver ricordato quanto disposto dall'art. 9 del Regolamento, il Garante si sofferma sulla deroga di cui alla lett. *h* del par. 2, che definisce – "finalità di cura", osservando che, diversamente dal passato, ora non è più indispensabile che il professionista sanitario, soggetto al segreto professionale[185], richieda il consenso del paziente per i trattamenti dei dati necessari alla prestazione sanitaria domandata dall'interessato, e ciò indipendentemente dal fatto che egli operi in qualità di libero professionista o all'interno di una struttura sanitaria pubblica o privata[186].

La liceità del trattamento delle categorie particolari di dati per le indicate finalità (lett. *h*), ove non sia riconosciuta sulla base del diritto dell'Unione o degli Stati membri, si fonda sul contratto con un professionista della sanità[187]. Ciò non significa, però, che il consenso di natura negoziale, per la conclusione del contratto, e il consenso dell'interessato al trattamento dei dati personali siano la stessa cosa[188]. Quindi, dobbiamo tener presente che si tratta di due consensi distinti.

In riferimento all'ambito oggettivo di applicabilità della fattispecie di cui alla lett. *h*, è posta in evidenza, nel provvedimento, la necessarietà per la cura della salute: gli eventuali trattamenti inerenti, solo in senso lato, alla cura, ma non strettamente necessari, richiedono perciò, pur se effettuati da professionisti della sanità, una distinta base giuridica da rintracciare, eventualmente, nel consenso dell'interessato o in un altro presupposto.

---

185 La previsione di cui alla lett. *h* si deve infatti coordinare, come anticipato, con quanto disposto dal par. 3 dell'art. 9. La tutela delle particolari categorie di dati personali è qui rimessa al segreto professionale o a un più generale obbligo di segretezza. In un'ottica analoga si poneva l'art. 8 della Direttiva. Cfr. LATTANZI, *Protecting health care data: from medical secrecy to personal data protection. Solution found?*, in HERVEG (a cura di), *op. cit.*, 21 ss.

186 Osservava FINOCCHIARO, *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, cit., 213, con riguardo alla disciplina previgente, che «l'interessato, in questo caso il paziente, esprime un consenso che non ha di fatto il potere di negare, se vuole essere curato. Non è dunque un consenso libero, dal momento che non si prospetta una reale alternativa, ma sostanzialmente obbligato».

187 Si v. GRANIERI, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, cit., 175 s.

188 BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, cit., 173 ss.

Il Garante procede poi ad elencare, a titolo esemplificativo, trattamenti in ambito sanitario che, non rientrando nelle altre ipotesi di deroga al divieto di cui all'art. 9, richiedono il consenso esplicito dell'interessato.

Tra questi ha individuato i trattamenti connessi all'impiego di App sulla salute, quelli effettuati da professionisti sanitari per finalità commerciali o elettorali[189] e anche i trattamenti operati con il fascicolo sanitario elettronico[190].

Riferendosi proprio al fascicolo sanitario elettronico, l'Autorità aggiungeva che, «in tali casi, l'acquisizione del consenso, quale condizione di liceità del trattamento, è richiesta dalle disposizioni di settore, precedenti all'applicazione del Regolamento, il cui rispetto è ora espressamente previsto dall'art. 75 del Codice», e proseguiva affermando, in un modo forse un po' arrischiato, che «un'eventuale opera di rimeditazione normativa in ordine all'eliminazione della necessità di acquisire il consenso dell'interessato all'alimentazione del Fascicolo, potrebbe essere ammissibile alla luce del nuovo quadro giuridico in materia di protezione dei dati», precisando subito dopo che, per i trattamenti effettuati attraverso il dossier sanitario, il consenso è richiesto dalle Linee guida emanate dal Garante stesso prima dell'applicazione del Regolamento[191], tuttavia, posto che il complessivo quadro giuridico è mutato, sarà l'Autorità ad individuare, all'interno della cornice di cui alle misure di garanzia *ex* art. 2 *septies*, d.lgs. n. 196/2003, i trattamenti che si possono effettuare prescindendo dal

---

189 Cfr. Provvedimento del Garante per la protezione dei dati personali del 6 marzo 2014, n. 107, **"**Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale", consultabile in *www.garanteprivacy.it.* Sul trattamento di dati personali a fini di marketing e nello specifico il consenso all'invio di e-mail promozionali, con riguardo alla disciplina antcedente all'entrata in vigore del d.lgs. n. 101/2018, v. Cass., 2.7.2018, n. 17278, in *Nuova giur. civ. comm.*, 2018, I, 1775 ss., con nota di ZANOVELLO, *Consenso libero e specifico alle e-mail promozionali*, pronuncia così massimata: «In tema di consenso al trattamento dei dati personali, la previsione dell'art. 23 del Codice della privacy (d. legis. n. 196 del 2003), nello stabilire che il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, consente al gestore di un sito Internet, il quale somministri un servizio fungibile, cui l'utente possa rinunciare senza gravoso sacrificio (nella specie servizio di newsletter su tematiche legate alla finanza, al fisco, al diritto e al lavoro), di condizionare la fornitura del servizio al trattamento dei dati per finalità pubblicitarie, sempre che il consenso sia singolarmente ed inequivocabilmente prestato in riferimento a tale effetto, il che comporta altresì la necessità, almeno, dell'indicazione dei settori merceologici o dei servizi cui i messaggi pubblicitari saranno riferiti». Cfr. T. ORRÙ, *«Nessuno può mettere il GDPR in un angolo». Breve storia comparata del consenso per il marketing nell'era globale*, in *Ciberspazio e diritto*, 2018, 41 ss.

190 S. CORSO, *Fascicolo sanitario elettronico ed ecosistema dati sanitari. I pareri critici del Garante per la protezione dei dati personali al Ministero della salute*, in *www.rivistaresponsabilitamedica.it*, 22-09- 2022.

191 Provvedimento del Garante per la protezione dei dati personali del 4 giugno 2015, n. 331, **"**Linee guida in materia di Dossier sanitario", in *www.garanteprivacy.it.*

consenso dell'interessato, ai sensi della lett. *h*[192].

Come si avrà modo di considerare più nel dettaglio, il panorama normativo sul fascicolo sanitario elettronico nel frattempo è cambiato, anche grazie a queste indicazioni fornite dal Garante.

Il provvedimento ha affrontato poi i profili attinenti all'informativa, alla posizione del responsabile della protezione dei dati e al registro delle attività di trattamento.

Così si è ribadito che il titolare del trattamento deve trasmettere all'interessato le informazioni sui principali elementi del trattamento stesso, alla luce del principio di trasparenza di cui all'art. 5, par. 1, lett. *a*, del Regolamento. Gli elementi da comunicare sono esplicitati agli artt. 13 e 14 del Regolamento, ma, in ogni caso, le informazioni devono essere rese in forma concisa, trasparente, intelligibile e facilmente accessibile, con linguaggio semplice e chiaro, mentre sarà il titolare a scegliere le modalità per l'informativa[193] più appropriate al caso di specie, tenendo conto di tutte le circostanze del trattamento e del contesto in cui viene effettuato, in virtù del principio di responsabilizzazione, o *accountability*, di cui all'art. 5 del Regolamento.

Relativamente all'attività posta in essere da titolari del trattamento, operanti in ambito sanitario, che effettuano più operazioni connotate da complessità particolare (ad esempio le aziende sanitarie), il Garante ha suggerito un criterio di progressività nel fornire le informazioni all'interessato[194].

---

[192] Il garante precisa inoltre che le disposizioni del Codice della privacy vanno comunque interpretate e applicate adeguatamente al Regolamento, com'è anche disposto dall'art. 22 del d.lgs. n. 101 del 2018, e la refertazione online il consenso dell'interessato è invece espressamente richiesto dalle disposizioni di settore relativamente alle modalità di consegna del referto. Art. 5, d.P.C.m. 8 agosto 2013, n. 71239: «1. Al fine di consentire all'interessato di esprimere scelte consapevoli in relazione al trattamento dei propri dati personali nell'utilizzo dei servizi di refertazione online, l'azienda sanitaria, in qualità di titolare del trattamento: a) fornisce all'interessato un'idonea informativa ai sensi dell'art. 13 del decreto legislativo 30 giugno 2003, n. 196, nonché sulle caratteristiche delle modalità digitali di consegna disponibili; b) acquisisce un autonomo e specifico consenso dell'interessato a trattare i suoi dati personali, anche sanitari, relativamente alle modalità digitali di consegna; c) consente la revoca in qualunque momento di tale consenso. 2. All'atto di richiesta del consenso o in ogni altro momento, l'interessato può indicare una farmacia presso cui ritirare il referto ai sensi del decreto del Ministro della salute 8 luglio 2011. Tale richiesta può essere modificata o revocata in ogni momento dall'interessato». V. FARCI, *Commento del d.p.c.m. 8 agosto 2013, n. 71239, sulla modalità di consegna dei referti medici tramite web*, in www.giustiziacivile.com, 5 marzo 2013.

[193] L'Autorità ha specificato che il contenuto dell'informativa non è stato stravolto dal Regolamento, ma va solo aggiornato e integrato con riferimento agli elementi di novità previsti dagli artt. 13 e 14.

[194] nei confronti della generalità dei pazienti afferenti a una struttura sanitaria potrebbero trasmettersi solo le informazioni appartenenti all'ordinaria attività di erogazione di prestazioni sanitarie, conformemente a quanto disposto dall'art. 79 del Codice della privacy, mentre gli elementi informativi relativi a particolari attività di trattamento potrebbero essere forniti in un secondo momento, solo ai pazienti interessati effettivamente da tali

Come elemento di novità, l'Autorità ha segnalato il dovere, da parte del titolare, di comunicare quello che sarà il periodo di conservazione dei dati, fornibile anche attraverso l'indicazione dei criteri utilizzati per determinarlo[195]. Quanto alle cartelle cliniche, esse, unitamente ai relativi referti, vanno conservate illimitatamente[196].

In ordine alla designazione del responsabile della protezione dei dati[197], il Garante ne ha chiarito l'obbligatorietà tanto per le strutture pubbliche che per quelle private. Tale designazione, infatti, è obbligatoria per le autorità o organismi pubblici, mentre per gli altri soggetti l'obbligo sussiste al ricorrere delle condizioni espresse dall'art. 37 del Regolamento[198].

Non vi è invece l'obbligo di designazione per il singolo professionista sanitario che operi in regime di libera professione a titolo individuale[199] e per le farmacie, le parafarmacie, le aziende ortopediche e sanitarie, nella misura in cui non effettuano trattamenti di dati personali su larga scala.

---

servizi e ulteriori trattamenti. Il Garante esemplifica indicando quali particolari attività di trattamento la fornitura di presidi sanitari, le modalità di consegna dei referti medici *online* e le finalità di ricerca.

[195] Qualora i tempi di conservazione di certi documenti sanitari non siano fissati da alcuna norma, egli dovrà comunque dare comunicazione di un periodo di tempo, individuandolo in modo che i dati vengano conservati, in una forma che permetta l'identificazione degli interessati, per un intervallo temporale che non superi quello necessario per conseguire le finalità del trattamento. Tale indirizzo è espressione dei principi di *accountability* e limitazione della conservazione.

[196] Cfr. Circolare del Ministero della Sanità del 19 dicembre 1986 n.900 2/AG454/260.

[197] Alle domande ricorrenti circa il responsabile della protezione dei dati, il Garante ha dato risposta con le schede informative del 15 dicembre 2017 [doc. web n. 7322110] e del 26 marzo 2018 [doc. web n. 8036793], in *www.garanteprivacy.it*, rispettivamente per l'ambito pubblico e per quello privato. Sull'inquadramento giuridico del DPO (*Data Protection Officer*), funzioni, prerogative e ruolo, AVITABILE, *Il* data protection officer, in FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 331 ss.; MARÌ, *El Delegado de Protección de Datos en el Reglamento General de Protección de Datos*, in MANTELERO e POLETTI (a cura di), *op. cit.*, 99 ss.; SOLINAS, *La nuova figura del responsabile della protezione dei dati*, in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., 879 ss. Cfr., nell'ambito della sanità, PEDRAZZI, *Il ruolo del responsabile della protezione dei dati (dpo) nel settore sanitario*, in *Riv. it. med. leg.*, 2019, 179 ss.

[198] Dunque, per le aziende sanitarie appartenenti al Servizio sanitario nazionale vige l'obbligo di designazione sia perché possono inquadrarsi nella nozione di organismo pubblico sia perché sussiste la condizione di cui alla lett. *c*, par. 1, dell'art. 37, essendo quello delle aziende menzionate un trattamento di dati relativi alla salute su larga scala, e così pure la designazione è obbligatoria per gli ospedali privati, le case di cura o le residenze sanitarie assistenziali dal momento che il trattamento dei dati relativi a pazienti svolto da queste strutture si può ricondurre, in linea generale, al concetto di larga scala (cfr. le "Linee guida sui responsabili della protezione dei dati" del Gruppo di lavoro articolo 29 per la protezione dei dati, adottate il 13 dicembre 2016 e poi il 5 aprile 2017 nella versione emendata (WP243 rev. 01)). Sul versante organizzativo, vengono rimesse alla responsabilità del titolare del trattamento «la possibilità e la fattibilità (art. 39 del Regolamento) di nominare un unico responsabile per più strutture sanitarie».

[199] Secondo il considerando 91 del Regolamento, «il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati».

In ambito sanitario, generalmente, vige sempre l'obbligo di tenuta del registro delle attività di trattamento[200], in quanto non è possibile derogarvi in presenza anche di uno solo degli elementi indicati dall'art. 30, par. 5, del Regolamento, ossia in caso di trattamento che presenta un rischio per i diritti e le libertà per l'interessato, trattamento non occasionale, trattamento che includa categorie particolari di dati di cui all'art. 9 o dati relativi a condanne penali e a reati[201]. Anche questa previsione è declinazione del principio di *accountability* e mira a garantire la gestione del rischio.

A distanza di due mesi dal provvedimento con cui il Garante ha fornito questi chiarimenti è stata pubblicata la Relazione del Garante sull'attività svolta nel 2018, unitamente al discorso del Presidente dell'Autorità. Una parte significativa del contenuto di quei documenti era dedicata al trattamento dei dati relativi alla salute. Come indicato nel discorso dell'allora Presidente Antonello Soro, nel settore sanitario gli attacchi erano incrementati raggiungendo il picco del 99% rispetto all'anno precedente, «con effetti tanto più gravi che in altri settori perché l'alterazione dei dati sanitari può determinare – come sottolineato anche rispetto al fascicolo sanitario elettronico – errori diagnostici o terapeutici. La carente sicurezza dei dati e dei sistemi che li ospitano può rappresentare, in altri termini, una causa di malasanità. […] Specularmente, la protezione dei dati è un fattore determinante di efficienza sanitaria, funzionale anche alla correttezza del processo analitico fondato su big data».[202] Massima l'attenzione prestata al trattamento di dati personali in relazione all'accertamento dell'infezione da HIV[203].

Tali considerazioni evidenziano ancora, da un lato, lo stretto rapporto fra il diritto alla salute e la protezione dei dati personali, specialmente quelli sanitari, e quasi una loro funzionalità reciproca e, dall'altro, la particolare – non sempre omogenea – sensibilità dei dati relativi alla

[200] Come recita il considerando 82, «per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti». Con il comunicato stampa dell'8 ottobre 2018 [doc. web n. 9047529], in *www.garanteprivacy.it*, il Garante per la protezione dei dati personali ha richiamato le istruzioni dallo stesso fornite sul registro delle attività di trattamento.

[201] Pertanto «non ricadono nelle ipotesi di esenzione dall'obbligo di tenuta del registro – ha affermato il Garante – i singoli professionisti sanitari che agiscano in libera professione, i medici di medicina generale/pediatri di libera scelta (MMG/PLS), gli ospedali privati, le case di cura, le RSA e le aziende sanitarie appartenenti al SSN, nonché le farmacie, le parafarmacie e le aziende ortopediche».

[202] SORO, *L'universo dei dati e la libertà della persona. Discorso del Presidente*, in *www.garanteprivacy.it*, 7 maggio 2019.

[203] S. CORSO, *Sul trattamento dei dati sanitari: l'attività del Garante per la protezione dei dati personali del 2018*, in *www.rivistaresponsabilitamedica.it*, 15 maggio 2019

salute.

Evidenziano inoltre lo sforzo di ricercare strumenti alternativi al consenso dell'interessato – che pure ricopre ancora una posizione di spessore – per la tutela della persona e l'orientamento di questa ricerca verso regole che rinforzino la sicurezza dei sistemi, soprattutto attraverso la responsabilizzazione del titolare del trattamento.

Successivamente a questi chiarimenti del Garante, il legislatore è più volte intervenuto – specie sulla disciplina del fascicolo sanitario elettronico – nella sua opera normativa di edificazione della sanità digitale, costretto o meno, attraverso passando attraverso il difficile periodo dell'emergenza sanitaria da Covid- 19.

3. *Dati genetici e biometrici*

La tematica relativa al trattamento di dati sanitari richiede di affrontare anche il tema dei dati genetici e biometrici, per la particolare vicinanza di queste tipologie di informazioni. Indagare i tratti salienti delle disposizioni sulla protezione di questi dati può esser utile per intendere come sia perseguito l'obiettivo di tutelare la persona e i suoi diritti e per cercare di comprendere i confini di ciascuna categoria.

Il riconoscimento normativo dei dati genetici e di quelli biometrici è stato graduale[204].

A livello internazionale, la Convenzione n. 108 non conteneva disposizioni specifiche in relazione a questi dati. La versione modernizzata del 2018 non li ha definiti, ma li ha inclusi fra le particolari categorie di dati, cui è riservato il più rigoroso regime dettato dall'art. 6. Una definizione di dati genetici e un'affermazione dettagliata su quelli biometrici sono offerte invece nel Rapporto esplicativo del Consiglio d'Europa a tale più giovane versione, secondo cui «*Genetic data are all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained.* […] *Processing of biometric data, that is data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of*

[204] Tale processo, come del resto può dirsi in relazione allo sviluppo della protezione dei dati personali, si è svolto, in primo luogo, per individuare il modo migliore per apprestare una tutela della persona. Cfr. PALMERINI, *Informazione genetica e tutela della persona. Implicazioni giuridiche delle analisi genetiche*, Pisa, ETS, 2004. Sulle tutele offerte dal diritto penale, PROVOLO, *L'identità genetica nella tutela penale della privacy e contro la discriminazione*, Padova University Press, 2018.

the individual, is also considered sensitive when it is precisely used to uniquely identify the data subject»[205]. Con riguardo specificamente ai dati genetici, nel testo della Convenzione n. 108 modernizzata si può cogliere l'influsso delle previsioni della Convenzione di Oviedo relative al genoma umano, in particolare il divieto di discriminazione *ex* art. 11 e le garanzie apprestate anche alla riservatezza, per i testgenetici predittivi, *ex* art. 12[206].

Svariati sono poi gli strumenti di *soft law* adottati da organizzazioni internazionali, riguardanti l'uso dei dati genetici. Ci si limita a ricordare qui la Dichiarazione internazionale sui dati genetici umani dell'Unesco, del 16 ottobre 2003, il cui art. 2 definisce i dati genetici umani come «informazioni sulle caratteristiche ereditarie degli individui ottenute dall'analisi degli acidi nucleici o da altre analisi scientifiche»[207].

Particolare importanza, nel panorama giurisprudenziale, riveste la sentenza della Corte europea dei diritti dell'uomo, resa dalla Grande Camera, il 4 dicembre 2008, nel caso *S. e Marper c. Regno Unito*. Ai sensi della sezione 64 del *Police and Criminal Evidence Act* del 1984, le impronte digitali, i profili di DNA e i campioni di cellule prelevati da una persona sospettata di un reato potevano essere conservati senza limiti di tempo, anche se il successivo procedimento penale si fosse concluso con l'assoluzione o il proscioglimento della persona. Nel caso sottoposto alla Corte, i ricorrenti avevano chiesto la distruzione delle loro impronte digitali e dei campioni cellulari – essendo stati accusati di reati, ma poi non condannati – tuttavia la polizia si rifiutò e pure le loro richieste di revisione giudiziaria furono respinte. Ritenute tali informazioni come riconducibili alla categoria di dati personali, la Corte, riconoscendo la violazione dell'art. 8 CEDU, concluse che il carattere generale ed indifferenziato con cui operava il meccanismo di conservazione, così come esso era stato applicato nel caso di specie ai ricorrenti, non garantiva un corretto bilanciamento dei concorrenti interessi pubblici e privati in gioco. Lo Stato aveva oltrepassato qualsiasi margine di apprezzamento accettabile in proposito: la conservazione dei dati personali oggetto della controversia costituiva un'ingerenza sproporzionata nel diritto al rispetto della vita privata e non poteva considerarsi necessaria in una società democratica[208].

---

[205] COUNCIL OF EUROPE, *Convention 108+. Convention for the protection of individuals with regard to the processing of personal data*. *Explanatory Report*, cit., 22, punti 57 e 58.

[206] BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit.*, *sub* art. 4(13), 199 s.

[207] La Dichiarazione internazionale sui dati genetici umani è stata preceduta dalla Dichiarazione universale sul genoma umano e i diritti umani, del 1997, e seguita dalla Dichiarazione universale sulla bioetica e i diritti umani, del 2005.

[208] Corte EDU, 4.12.2008, nn. 30562/04 e 30566/04, *S. e Marper c. Regno Unito*, in www.hudoc.echr.coe.int, in particolare i punti 68 e 125. V. L. TOMASI, *op. cit*., 318, nonché ANGIOLINI, *Health and Data Protection*,

La sensibilità dei dati genetici e biometrici, anche per i giudici di Strasburgo, richiede quindi una particolare attenzione, specialmente nel momento in cui se ne ammette il trattamento, che deve conformarsi alla tutela della persona. Nella stessa sentenza, peraltro, emerge il legame fra queste categorie di dati e le informazioni relative alla salute, il cui trattamento si afferma costituire una 'ingerenza particolarmente invasiva'[209].

Nell'ambito del diritto eurounitario, l'art. 21 della Carta di Nizza, nel vietare qualsiasi forma di discriminazione, include anche quella fondata sulle caratteristiche genetiche, riscontrando ulteriormente l'assunto per cui il contenuto di queste informazioni può essere alla base di atti discriminatori, ciò traducendosi nella concretizzazione del rischio per i diritti e le libertà fondamentali della persona che il divieto di trattamento delle particolari categorie di dati personali mira a prevenire.

La Direttiva madre non conteneva disposizioni espressamente inerenti ai dati genetici e biometrici e neppure la Direttiva n. 58 del 2002, relativa alla vita privata e alle comunicazioni elettroniche. Diversamente, il Regolamento (CE) n. 2252/2004 del Consiglio, del 13 dicembre 2004, *relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri*, conteneva già diverse previsioni sui dati biometrici[210].

Il Gruppo di lavoro "Articolo 29", che, in un primo momento, aveva riconosciuto il potenziale dei risultati degli studi sul DNA[211], adottò, nel 2004, un documento che costituì una base per le successive riflessioni in materia di dati genetici[212]. Nelle sue osservazioni - pur con le inesattezze dovute al limite dei progressi scientifici e tecnologici di allora[213] giunse a rilevare che l'informazione genetica è unica e distingue un individuo da un altro, potendo però rivelare dati ed avere implicazioni concernenti i membri della famiglia biologica dell'interessato, compresi quelli delle generazioni successive e precedenti; essa può caratterizzare un gruppo di persone, come i gruppi etnici, può rivelare la discendenza e i legami di parentela. Inoltre, i dati genetici potranno, in futuro, rivelare più informazioni ed

---

cit., 126 ss. Cfr. Corte EDU, 22.6.2017, n. 8806/12, *Aycaguer c. Francia*, in *Cass. pen.*, 2017, 3773; Corte EDU, 13.2.2020, n. 45245/15, *Gaughran c. Regno Unito*, in www.hudoc.echr.coe.int.

[209] «La Corte riconosce che il livello di intensità dell'ingerenza nel diritto dei ricorrenti al rispetto della loro vita privata può variare a seconda di ciascuna delle tre categorie di dati personali oggetto della conserva zione [ossia profili di DNA, campioni di cellule e impronte digitali]. Ad esempio, la conservazione di campioni di cellule è una ingerenza particolarmente invasiva dal momento che tali campioni contengono una grande quantità di informazioni genetiche, relative anche alla salute della persona interessata». Punto 120.

[210] Gruppo Articolo 29, *Opinion 6/2000 on the Human Genome and Privacy*, 13 luglio 2000, WP34.

[211] Gruppo Articolo 29, *Documento di lavoro sui dati genetici*, cit., 5.

[212] V. Gruppo Articolo 29, *Documento di lavoro sui dati genetici*, 17 marzo 2004, WP91

[213] BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit., sub* art. 4(13), 198

essere utilizzati da un numero crescente di organismi, a scopi diversi. A ciò aggiungeva che «l'umanità non deve però essere ridotta alle sue caratteristiche genetiche, alla sua cartografia genetica, che in ogni caso non costituiscono la spiegazione universale ultima della vita umana».

Il fine di quel documento era l'individuazione di una tutela legale particolare per la persona, relativa al trattamento dei dati genetici, attesa la specificità degli stessi. Riportandosi alla normativa vigente all'epoca e, nel dettaglio, al disposto dell'art. 8 della Direttiva n. 46 del 1995, il Gruppo di lavoro "Articolo 29" affermava che «i dati genetici possono, in certa misura, fornire un quadro dettagliato della condizione fisica di una persona e del suo stato di salute e potrebbero perciò essere considerati "dati relativi alla salute"»[214].

Ai dati relativi alla salute aveva fatto riferimento il Gruppo di lavoro stesso un anno prima, nel documento sulla biometria. Si affermò infatti che anche i dati biometrici potevano considerarsi 'di natura delicata', ai sensi dell'art. 8 della Direttiva, qualora si sostanziassero, ad esempio, in dati relativi alla salute[215]. Così pure le immagini digitali, che si possono considerare dati biometrici, sono riconducibili ai dati sulla salute, nella misura in cui da esse possano ricavarsi informazioni sullo stato di salute della persona[216].

Dati genetici e dati biometrici sono quindi confluiti, nella loro considerazione come dati che possono rivelare informazioni sulle condizioni di salute della persona, nelle ulteriori riflessioni compiute dal Gruppo di lavoro, nel parere del 2012, sugli sviluppi nelle tecnologie biometriche.

Innovando, rispetto alla Direttiva del '95, il reg. Ue n. 679 del 2016 definisce sia i dati genetici che quelli biometrici, all'art. 4, nn. 13 e 14[217]: i primi, come «i dati personali relativi

---

[214] V. Gruppo Articolo 29, *Documento di lavoro sulla biometria*, 1° agosto 2003, WP80, 10.

[215] Gruppo Articolo 29, *Opinion 02/2012 on facial recognition in online and mobile services*, 22 marzo 2012, WP192, 4.

[216] Gruppo Articolo 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, cit., *passim*, spec. 27 ss. È appena il caso di sottolineare come una definizione di dati biometrici fosse stata fornita dal Gruppo di lavoro "Articolo 29" già nel 2007, cui si accompagnava anche una esemplificazione: «Questi dati possono essere definiti proprietà biologiche, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche e/o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità. Esempi tipici di dati biometrici sono le impronte digitali, la struttura della retina, del volto, la voce, ma anche la forma della mano, gli elementi caratteristici delle vene o perfino alcune capacità profondamente radicate nella persona o altre caratteristiche comportamentali (la firma, la pressione esercitata sui tasti, il modo particolare di camminare o parlare, ecc...)». Gruppo Articolo 29, *Parere 4/2007 sul concetto di dato personale*, cit., 8 s.

[217] Queste definizioni sono le medesime utilizzate anche dalla dir. Ue 2016/680, art. 3, nn. 12 e 13, e dal reg. Ue 2018/1725, art. 3, nn. 17 e 18. Si v. anche la definizione di dati genetici resa dal Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, *che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI*, all'art. 2, lett. *j*, ossia: «tutti i

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 in questione»[218], e i secondi, come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»[219].

L'interpretazione della definizione di dati genetici – definizione suscettibile di obsolescenze in ragione degli sviluppi sempre più rapidi della tecnologia e delle sempre nuove acquisizioni della scienza – è resa più elastica da quanto espresso nel considerando 34 del Regolamento, secondo cui «è opportuno che per dati genetici si intendano i dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti».

Si deve evidenziare poi che i dati sul DNA possono qualificarsi sia come dati genetici che come dati biometrici, per via delle sovrapposizioni definitorie cui dà luogo il testo del Regolamento. Sono quindi dati personali appartenenti a categorie distinte, che hanno avuto

---

dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di un individuo che forniscono informazioni univoche sulla sua fisiologia o salute, ottenuti in particolare dall'analisi di un suo campione biologico». Una definizione di 'dati biometrici', identica a quella del reg. Ue n. 679/2016, è contenuta nella proposta della Commissione di Regolamento sull'intelligenza artificiale all'art. 3, n. 33

[218] Restano quindi esclusi dalla categoria dei dati genetici tutti quei dati sulle caratteristiche genetiche che, pur risultando da analisi di campioni biologici della persona fisica, non forniscono informazioni univoche sulla sua fisiologia o sulla sua salute

[219] La definizione di dati biometrici, come del resto anche quella di dati genetici, risulta abbastanza ampia e allo stesso tempo tecnica. Infatti, include i dati personali relativi sia alle caratteristiche fisiche, che a quelle fisiologiche e comportamentali, i quali tanto permettano quanto confermino l'identificazione univoca della persona fisica. La distinzione rileva, poiché consentire l'identificazione univoca di un individuo è l'attività di identificazione in senso stretto, mentre la conferma di una identificazione è un'attività diversa, ossia l'autenticazione o verificazione della persona. La definizione di dati biometrici resa dal Regolamento, oltre a qualificarli per la capacità di identificazione o autenticazione della persona fisica, li connota per il fatto di essere ottenuti da un *trattamento tecnico specifico*, ma senza specificare questo elemento. Tale nozione, in realtà, essendo parte della definizione stessa, risulta essenziale per comprendere quali dati personali ricadano in questa categoria di informazioni. Si osserva quindi come detto processo tecnico venga a comporsi di varie fasi, tra cui: a) l'acquisizione di una misura di riferimento di una o più caratteristiche fisiche, fisiologiche o comportamentali di una persona (spesso definita "arruolamento"); b) la creazione di una rappresentazione di tale misura in un modello; c) il collegamento di tale modello a un codice o a un oggetto utilizzato per identificare la persona (l'insieme di modello e codice/oggetto è spesso definito '*master template*'); d) la memorizzazione del *master template* in un database; e) l'acquisizione di nuove misurazioni (spesso definite '*live template*') delle stesse caratteristiche biologiche; f) l'abbinamento del *live template* al *master template*; g) l'applicazione di un algoritmo per generare un risultato dall'abbinamento. BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit.*, *sub* art. 4(14), 212

un processo di affermazione distinto, ma in un certo qual modo uniti tra loro per somiglianze, per lo più inerenti alla informazione che vengono a costituire e a ciò che possono veicolare, ciò che possono dire della persona. Somiglianze che condividono con i dati relativi alla salute, da cui derivano.

I dati genetici e i dati biometrici – questi ultimi, solo se intesi a identificare in modo univoco una persona fisica, cioè solo per l'identificazione in senso stretto e non anche per l'autenticazione – si annoverano, inoltre, fra le particolari categorie di dati personali il cui trattamento è vietato *ex* art. 9, par. 1, del Regolamento.

Per il trattamento di dati genetici, biometrici e relativi alla salute – inoltre – l'art. 9, par. 4, consente agli Stati membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni.

Le regole che valgono quindi per il trattamento dei dati relativi alla salute si applicano, in genere, anche al trattamento dei dati genetici e biometrici. Tuttavia, per la loro autonomia concettuale e le specificità, dati genetici e biometrici possono essere oggetto di regole particolari e di discipline speciali, rispetto a quella propria dei dati sanitari[220].

Così, nell'ordinamento italiano, l'art. 2 *septies* del Codice della privacy detta disposizioni sulle misure di garanzia, trasversalmente, per il trattamento di dati genetici, biometrici e relativi alla salute, ma solo per i dati genetici contempla la possibilità di introdurre il consenso del soggetto come ulteriore misura di protezione.

3.1 *Profili del trattamento di dati genetici*

Il trattamento dei dati genetici, laddove giustificato e ammesso da una delle ipotesi eccezionali di cui all'art. 9, par. 2, del Regolamento, nonché fondato su una delle basi giuridiche dell'art. 6, può essere posto in essere per diverse finalità e perseguire obiettivi differenti[221].

Il suo impiego può aversi innanzitutto in ambito medico. Dalle possibilità diagnostiche alle potenzialità della medicina predittiva, dalla individuazione di terapie specifiche o

[220] Come espresso dal considerando 35 del Regolamento, tra i dati sulla salute si annoverano «le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici».

[221] V., anche per i riferimenti ivi contenuti, SCAFFARDI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 9, reg. Ue n. 679/2016, *II. Il trattamento dei dati particolari: il dato genetico*, 249 ss. Cfr. MOLLO, *Il trattamento dei dati genetici tra libera circolazione e tutela della persona*, in *Jus civile*, 2022, 70 ss.; BOTTA, *La tutela dei dati genetici tra innovazione tecnologica e diritti fondamentali della persona*, in *De Iustitia*, 2021, fasc. 2, 56 ss.

personalizzate all'eventuale, futura, manipolazione del genoma umano per curare o prevenire malattie[222].

L'uso dei dati genetici è centrale, in particolare, con riguardo ai c.d. test genetici, che consentono di diagnosticare patologie, anche gravi[223]. Gli scenari che si dispiegano in questa direzione, come si può intendere, vanno al di là del piano meramente giuridico e investono i temi della bioetica, specialmente dovendo prendere in considerazione non solo la posizione del soggetto interessato, ma anche quella dei suoi familiari, che condividono con lui i tratti del patrimonio genetico[224], o di insiemi di individui. L'aspetto emerge, con particolare evidenza, per lo *screening* genetico di popolazioni, gruppi o soggetti in particolari condizioni e quello dei neonati.

Sempre inerente all'ambito medico, ma orientato alle finalità di ricerca, è il trattamento di dati genetici operato con la costituzione, l'implementazione e la conservazione di biobanche[225]. Nonostante il regime giuridico delle biobanche di ricerca sia tuttora di difficile inquadramento, posta l'assenza di precise norme vincolanti a livello sovranazionale e, in Italia, di una legge specifica, le disposizioni sulla protezione dei dati personali permettono di offrire una tutela delle libertà e dei diritti fondamentali della persona[226], nella complessità e doverosità del bilanciamento degli interessi contrapposti.

---

[222] IAGNEMMA, *L'editing genetico: una sfida (anche) normativa*, in *Riv. it. med. leg.*, 2019, 1309 ss., la quale pure sottolinea i rischi connessi all'*editing* genetico. Sull'*editing* genetico in particolare, si v. SLOKENBERGA *et al.*, *Governing, Protecting, and Regulating the Future of Genome Editing: The Significance of ELSPI Perspectives*, in *European Journal of Health Law*, vol. 29, n. 3-5, 2022, 327 ss., e i contributi raccolti nel medesimo numero monografico, *Genome Editing, Health Innovation and Regulation*.

[223] Si v. RODOTÀ, Privacy *e costruzione della sfera privata. Ipotesi e prospettive*, cit., 535, che rammenta la possibilità di diagnosi precoce di malattie come la corea di Huntington, che si sviluppa verso il quarantesimo anno dopo aver consentito al soggetto una vita del tutto normale). Con riferimento a un caso concreto, PICIOCCHI, *op. cit.*, 91 ss., e, per i profili etici, TORALDO DI FRANCIA, *op. cit.*, 84 ss. Cfr. SALARDI, *Test genetici tra determinismo e libertà*, Torino, Giappichelli, 2010. Per riflessioni sul ruolo dell'analisi del genoma nelle consulenze genetiche e sui rischi derivanti da un accesso ai dati genetici non regolamentato, cfr. M. PAGANELLI, *Diritti della personalità. L'individuo e il gruppo*, in LIPARI (a cura di), *Diritto privato europeo*, I, Padova, CEDAM, 1997, 152 ss.

[224] Moltissimi, al riguardo, gli studi. V., anche per riferimenti bibliografici, DOVE *et al*., *Familial genetic risks: how can we better navigate patient confidentiality and appropriate risk disclosure to relatives?*, in *Journal of Medical Ethics*, vol. 45, n. 8, 2019, 504 ss.

[225] RODOTÀ, Privacy *e costruzione della sfera privata. Ipotesi e prospettive*, cit., 535 s. Proprio qui, peraltro, la definizione di dati genetici offerta dal Regolamento può risultare manchevole. Essa non comprende l'aspetto 'condiviso' di queste informazioni, ossia il fatto che il dato genetico appartenga non solo alla persona cui si riferisce l'analisi da cui si ricava, ma anche al suo gruppo familiare. BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit.*, *sub* art. 4(13), 203. Sul rischio di ricadute discriminatorie legate alle indagini genetiche, cfr. PETRONE, *Trattamento di dati genetici e tutela della persona*, in *Fam. e dir*., 2007, 853 ss. Ma v. già NELKIN, *Informazione genetica: bioetica e legge*, in *Riv. crit. dir. priv*., 1994,

[226] MAESTRI, *Il feticcio della privacy nella sanità. Cura del paziente e biobanking genetico prima e dopo l'entrata in vigore del GDPR*, in A. THIENE e S. CORSO (a cura di), *op. cit.*, 23 ss.

Differente, ma non meno importante, è l'impiego del trattamento dei dati genetici nel campo delle indagini penali, della lotta alla criminalità e della prevenzione. Le operazioni di trattamento, in questi casi, non solo di raccolta e conservazione, possono confluire o scaturire dalla predisposizione di banche dati contenenti i profili genetici di condannati o, talvolta, di sospettati[227].

Ma possono esserci anche altri scopi per cui vengono trattati dati genetici. Esso può svolgere, infatti, un ruolo rilevante anche nell'ambito lavorativo, assicurativo o di accertamento della paternità[228].

Attese le plurime finalità che possono riguardare il trattamento di dati genetici, gioca un ruolo fondamentale, nella tutela della persona, il rispetto dei principi di cui all'art. 5 del Regolamento, in particolare quelli di cui alle lett. *b*, *c* ed *e*.

Così, in virtù del principio di limitazione della finalità (lett. *b*), i dati genetici vanno non solo raccolti per finalità determinate, esplicite e legittime, ma anche successivamente trattati in un modo che non sia incompatibile con quelle finalità, tenendo presente peraltro che un trattamento ulteriore non si considera incompatibile se avviene, tra l'altro, a fini di ricerca scientifica. È questo il c.d. uso secondario dei dati genetici, che specialmente si riscontra nella ricerca scientifica, soprattutto biomedica[229].

Per il principio di minimizzazione dei dati (lett. *c*), i dati genetici saranno adeguati, pertinenti e limitati a ciò che è necessario rispetto alle finalità per cui sono trattati, mentre, per quello di limitazione della conservazione (lett. *e*), qualora dovessero essere conservati per un tempo superiore a quello che consente il conseguimento delle finalità, il trattamento deve

---

[227] SCAFFARDI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 9, reg. Uen. 679/2016, *II. Il trattamento dei dati particolari: il dato genetico*, 252 s. Cfr. EAD. (a cura di), *La Banca dati italiana del DNA. Limiti e prospettive della genetica forense*, Bologna, 2019; EAD., *L'impiego processuale del DNA fra giustizia genetica e garanzie costituzionali: quali sfide per il diritto (e per la Costituzione)*, in *BioLaw Journal - Rivista di BioDiritto*, *Special issue* 2, 2019, 503 ss.; EAD., *Dati genetici e biometrici: nuove frontiere per le attività investigative*, in EAD. (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, Torino, Giappichelli, 2018, 37 ss.; EAD., *Giustizia genetica e tutela della persona. Uno studio comparato sull'uso (e abuso) delle Banche dati del DNA a fini giudiziari*, Padova, CEDAM, 2017. V. anche FELICIONI, *Il trattamento dei dati genetici tra efficacia investigativa e tutela della riservatezza*, in ADINOLFI e SIMONCINI (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, Edizioni Scientifiche Italiane, 2022, 625 ss.; PICOTTI, *Trattamento dei dati genetici, violazioni della* privacy *e tutela dei diritti fondamentali nel processo penale*, in *Dir. inf.*, 2003, 689 ss..

[228] DE FRANCESCHI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 4, reg. Ue n. 679/2016, 169

[229] DI TANO, *Protezione dei dati personali e ricerca scientifica: un rapporto controverso ma necessario*, in *BioLaw Journal - Rivista di BioDiritto*, 2022, 71 ss., spec. 82 ss.; LATTANZI, *Ricerca genetica e protezione dei dati personali*, cit., 319 ss

avvenire esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, in conformità all'art. 89, par. 1, del Regolamento, sempre attuando le misure tecniche e organizzative adeguate richieste a tutela dei diritti e delle libertà dell'interessato.

La peculiare delicatezza dei dati genetici è presa in considerazione dal legislatore italiano all'art. 2 *septies* del Codice della privacy, laddove, al comma 6°, prevede – come anticipato – che le misure di garanzia adottate dal garante possano, in caso di particolare ed elevato livello di rischio, individuare il consenso come ulteriore misura di protezione dei diritti dell'interessato. In questo, sembra ancora riconoscere al consenso un ruolo in chiave di tutela della persona, pur senza farlo assurgere, per ciò solo, a base giuridica del trattamento[230].

Il Garante per la protezione dei dati personali, con il menzionato provvedimento n. 146 del 2019, ha individuato le prescrizioni relative al trattamento dei dati genetici[231] di cui all'autorizzazione generale n. 8 del 2016[232] che risultano compatibili con le disposizioni del Regolamento e del d.lgs. n. 101/2018.

Dopo una prima parte di carattere definitorio, che riproduce fedelmente la formulazione del Regolamento in relazione alla definizione di 'dati genetici'[233], le prescrizioni

---

[230] FEROLA, *op. cit.*, 432 s.; ma, *contra*, SCAFFARDI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 9, reg. Ue n. 679/2016, *II. Il trattamento dei dati particolari: il dato genetico*, 260, secondo cui «con specifico riferimento ai dati genetici viene inoltre stabilito che il Garante possa prevedere il consenso dell'interessato quale ulteriore base giuridica di legittimità del trattamento». Cfr. ZANOVELLO, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 2 *septies*, d.lgs. n. 196 del 2003, 1058.

[231] V. SIRGIOVANNI, *Dal consenso dell'interessato alla "responsabilizzazione" del titolare del trattamento dei dati genetici*, in *Nuove leggi civ. comm.*, 2020, 1010 ss., spec. 1019 ss.

[232] Per i profili del trattamento di dati genetici in epoca antecedente al Regolamento, v. ANNECCA, *Il trattamento dei dati genetici*, in PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, cit., 1121 ss.; D'ANTONIO, *I dati genetici*, in CARDARELLI, SICA e ZENO-ZENCOVICH (a cura di), *op. cit.*, 337ss. Cfr., per analisi da differenti punti di vista, oltreché per riferimenti bibliografici, CASONATO, PICIOCCHI e VERONESI (a cura di), *I dati genetici nel biodiritto*, Padova, CEDAM, 2011; STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Padova, CEDAM, 2008.

[233] Di particolare importanza risulta la definizione – data dalla lett. *c* del punto 4.1 – di *test genetico*, di cui i test farmacogenetici, farmacogenomici e sulla variabilità individuale nonché lo screening genetico sono sottocategorie, per cui esso è «l'analisi a scopo clinico di uno specifico gene o del suo prodotto o funzione o di altre parti del Dna o di un cromosoma, volta a effettuare una diagnosi o a confermare un sospetto clinico in un individuo affetto (test diagnostico), oppure a individuare o escludere la presenza di una mutazione associata ad una malattia genetica che possa svilupparsi in un individuo non affetto (test presintomatico) o, ancora, a valutare la maggiore o minore suscettibilità di un individuo a sviluppare malattie multifattoriali (test predittivo o di suscettibilità)».

provvedono subito a dettare disposizioni circa la sicurezza del trattamento[234].

Le regole si pongono quindi in attuazione dei principi di minimizzazione dei dati e di integrità e riservatezza, di cui all'art. 5, lett. *c* e *f,* del Regolamento.

Alle prescrizioni sulle informazioni agli interessati e sulla consulenza genetica, fanno seguito quelle sul consenso. È previsto, infatti, che il consenso al trattamento dei dati genetici sia necessario per finalità di tutela della salute di un soggetto terzo[235], per lo svolgimento di test genetici nell'ambito delle investigazioni difensive o per l'esercizio di un diritto in sede giudiziaria, salvo che un'espressa disposizione di legge, o un provvedimento dell'autorità giudiziaria in conformità alla legge, disponga altrimenti, e per i trattamenti effettuati mediante test genetici, compreso lo screening, a fini di ricerca o di ricongiungimento familiare[236].

Particolare attenzione merita anche la prescrizione per cui il consenso al trattamento dei dati genetici può essere revocato dall'interessato e, in tal caso, i trattamenti devono cessare e i dati devono essere cancellati o resi anonimi, anche attraverso la distruzione del campione biologico prelevato.

---

[234] Si tratta di disposizioni in merito all'accesso ai locali, alla conservazione, l'utilizzo e il trasporto dei campioni biologici, al trasferimento dei dati con sistemi di messaggistica elettronica, alla consultazione dei dati trattati con strumenti elettronici e alla tenuta di elenchi, registri o banche di dati. In particolare, con riguardo a questi ultimi, si richiede che il trattamento avvenga con tecniche di cifratura o di pseudonimizzazione, cui si aggiungono, in chiusura, 'altre soluzioni' che, atteso il volume dei dati e dei campioni trattati, «li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità, in modo da ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato».

[235] Secondo quanto disposto dal punto 4.7, cui il 4.5 fa rinvio, «ferme restando le specifiche condizioni in ambito sanitario previste dall'art. 75 del Codice, il trattamento di dati genetici per finalità di tutela della salute di un soggetto terzo può essere effettuato se questi appartiene alla medesima linea genetica dell'interessato e con il consenso di quest'ultimo. Nel caso in cui il consenso dell'interessato non sia prestato o non possa essere prestato per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere, nonché per effettiva irreperibilità, il trattamento può essere effettuato limitatamente ai dati genetici disponibili qualora sia indispensabile per consentire al terzo di compiere una scelta riproduttiva consapevole o sia giustificato dalla necessità, per il terzo, di interventi di natura preventiva o terapeutica. Nel caso in cui l'interessato sia deceduto, il trattamento può comprendere anche dati genetici estrapolati dall'analisi dei campioni biologici della persona deceduta, sempre che sia indispensabile per consentire al terzo di compiere una scelta riproduttiva consapevole o sia giustificato dalla necessità, per il terzo, di interventi di natura preventiva o terapeutica (cons. 27, Regolamento UE 2016/679)».

[236] In quest'ultimo caso, si aggiunge – in linea con l'art. 10, par. 2, della Convenzione di Oviedo – che all'interessato venga chiesto di dichiarare se vuole conoscere o meno i risultati dell'esame o della ricerca, comprese eventuali notizie inattese che lo riguardano, qualora esse rappresentino per lui un beneficio concreto e diretto in termini di terapia o di prevenzione o di consapevolezza delle scelte riproduttive. A tale prescrizione fa eco quella di cui al punto 4.6, sulla comunicazione e la diffusione dei dati, per la quale «gli esiti di test e di screening genetici, nonché i risultati delle ricerche qualora comportino per l'interessato un beneficio concreto e diretto in termini di terapia, prevenzione o di consapevolezza delle scelte riproduttive, devono essere comunicati al medesimo interessato anche nel rispetto della sua dichiarazione di volontà di conoscere o meno tali eventi e, ove necessario, unitamente a un'appropriata consulenza genetica».

Il consenso dell'interessato è necessario, inoltre, in caso di trattamento di dati genetici per finalità di ricerca scientifica e statistica non previste dalla legge o da altro requisito specifico di cui all'art. 9 del Regolamento. Tale tipo di trattamento, secondo il punto 4.11, è consentito solo se volto alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico ed epidemiologico, anche nell'ambito della sperimentazione clinica o ricerca scientifica volta a sviluppare le tecniche di analisi genetica. Se la persona cui i dati genetici o i campioni biologici si riferiscono non può fornire il suo consenso per incapacità, il trattamento per finalità di ricerca scientifica, che non comporti un beneficio diretto per il medesimo interessato, può aversi – sempre tenendo in considerazione, ove possibile, l'opinione del minore o dell'incapace – al ricorrere di una serie di condizioni contemporaneamente, tra cui il fatto che la ricerca non comporti rischi significativi per la dignità, i diritti e le libertà fondamentali dell'interessato[237].

In attuazione del principio di limitazione della conservazione, è previsto poi che, in assenza del consenso dell'interessato, i campioni biologici prelevati e i dati genetici raccolti per scopi di tutela della salute possano essere conservati e utilizzati per finalità di ricerca scientifica o statistica, in caso di indagini statistiche o ricerche scientifiche previste dal diritto dell'Unione europea, dalla legge o, nei casi previsti dalla legge, da regolamento, o limitatamente al perseguimento di ulteriori scopi scientifici e statistici direttamente collegati con quelli per cui è stato acquisito, in origine, il consenso informato degli interessati.

Per quanto riguarda, dunque, il trattamento dei dati genetici, il consenso dell'interessato appare svolgere ancora una – pur limitata – funzione di protezione nei confronti dell'individuo, ma certamente l'attuale normativa è lontana dallo schema sotteso al vecchio impianto del Codice della privacy, che poggiarvala tutela della persona sul consenso [238].

---

[237] Le altre condizioni elencate al punto 4.11.2 sono: che la ricerca sia finalizzata al miglioramento della salute di altre persone appartenenti allo stesso gruppo d'età o che soffrono della stessa patologia o che si trovano nelle stesse condizioni e il programma di ricerca sia oggetto di motivato parere favorevole del competente comitato etico a livello territoriale; che il consenso al trattamento sia acquisito da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato; e che una ricerca di analoga finalità non possa essere realizzata mediante il trattamento di dati riferiti a persone che possono prestare il proprio consenso. Tale ultima condizione, in particolare, non solo appare quale ulteriore implementazione del principio di minimizzazione, ma ancora esprime la necessarietà del trattamento dei dati sensibili – genetici – in questo caso in quanto riferiti alla persona incapace.

[238] La peculiarità del dato genetico, che ha giustificato il rigore nelle scelte normative adottate, sta, almeno in parte, nella sua univoca riconducibilità al soggetto fisico, nella capacità predittiva circa la sua sorte – e quella delle sue condizioni di salute – e, in definitiva, nel delineare, in modo specifico, la sua identità. V. LA SPINA, *Complessità e identità personale*, Edizioni Scientifiche Italiane, Napoli, 2022; CORDIANO, *Identità della persona e disposizione del corpo. La tutela della salute nelle nuove scienze*, cit., 326 ss. Cfr. RODOTÀ,

Di quelle norme, oggi abrogate, ha fatto applicazione *ratione temporis* la Cassazione, con l'ordinanza n. 27325 del 2021. Il caso riguardava la cessione di una banca dati genetica, a seguito del fallimento della società che gestiva l'infrastruttura di ricerca e della sua acquisizione da parte di una società biotecnologica inglese. Sulla questione era intervenuto il Garante per la protezione dei dati personali, il quale, nelle more del completamento dell'istruttoria avviata a partire dall'istanza di alcuni dei partecipanti, aveva disposto il blocco del trattamento dei dati e dei campioni della biobanca stessa, per verificare la sussistenza di un legittimo presupposto del trattamento, verso la cessionaria[239]. Il Tribunale di Cagliari annullava tale provvedimento, in accoglimento del ricorso della società inglese, ritenendo valido il consenso espresso dagli interessati rispetto alla società fallita, in quanto la ricorrente avrebbe perseguito le medesime finalità di ricerca scientifica, e considerato anche che agli interessati non sarebbe stato precluso l'esercizio dei propri diritti, secondo le disposizioni del d.lgs. n. 196/2003[240].

Cassando la decisione del giudice *a quo*, la Suprema Corte è giunta alla conclusione per cui il trasferimento dei dati dal titolare originario ad un altro soggetto, pur essendo consentito, dà luogo alla cessazione del trattamento originario e non alla successione nello stesso, determinando, perciò, l'inizio di un altro trattamento ad opera del nuovo titolare, tenuto al rispetto della complessiva disciplina in tema di informativa e consenso e al relativo rinnovo. Ciò posto, in via generale, il consenso informato, in un caso come questo, di cessione di una banca dati genetica, resta imprescindibile, qualora non ricorrano le deroghe di cui agli artt. 13, comma 5°, 26, comma 4°, 110, comma 1°, del Codice della privacy[241]. Il riferimento

---

Tecnologie e diritti, cit., 118 ss. Con particolare riguardo alla posizione del minore, F. GIARDINA, *op. cit.*, 159 ss.

[239] Provvedimento del Garante per la protezione dei dati personali del 6 ottobre 2016, n. n. 389, "Provvedimento di blocco del trattamento dei dati personali contenuti in una biobanca", consultabile in *www.garanteprivacy.it.*

[240] Trib. Cagliari, 6.6.2017, n.1569, in *DeJure*.

[241] «La cessione di dati o banche dati è consentita dal d.lgs. n. 196 del 2003, art. 16; tuttavia la cessione dei dati ad un terzo, ed il conseguente mutamento soggettivo del titolare del trattamento, determina l'avvio di un nuovo trattamento, a sua volta soggetto alle disposizioni generali in tema di informativa e di consenso; in questo caso, il rinnovo dell'informativa e della raccolta del consenso può essere derogata, in misura più o meno ampia, solo ove ricorrano le specifiche condizioni previste dal codice della privacy; per quanto riguarda i "dati sensibili" e i "dati genetici", che costituiscono un sottoinsieme dei primi, la disciplina si connota di particolare rigore, temperato mediante il riconoscimento di poteri istruttori ed autorizzativi al Garante previsti dall'art. 13, comma 5, art. 26, comma 4, art. 110, comma 1, Codice della privacy, che non possono essere derogati, essendo volta ad assicurare lo svolgimento del trattamento ritenuto meritevole di tutela per le finalità perseguite, senza intaccare in maniera significativa i diritti degli interessati». Cass., 7.10.2021, n. 27325, in *Nuova giur. civ. comm*., 2022, I, 590 ss., con nota di CORTI, *La sorte (incerta) della ricerca sui campioni biologici umani all'indomani della decisione Shardna*; in *Dir. fam. e pers*., 2022, 26 ss., con nota di CIANCIMINO, *Circolazione "secondaria" di dati sanitari e biobanche. Nuovi paradigmi contrattuali e istanze personalistiche*. Cfr. CAREDDA, *Campioni*

normativo, nella pronuncia dei giudici di legittimità, è il testo del d.lgs. n. 196 del 2003, nella versione non modificata dal d.lgs. n. 101 del 2018. La Cassazione non indaga quale può essere una soluzione per casi analoghi futuri, limitandosi a ricostruire la cornice normativa vigente all'epoca e quindi applicabile al caso concreto[242]. Si è sottolineato, in particolare, come con questa pronuncia non si sia preso realmente in considerazione il contesto del trattamento dei dati, ossia la ricerca scientifica, attestandosi alla generale disciplina relativa al trattamento dei dati sensibili e disattendendo, in un certo qual modo, le aspettative sulle risposte interpretative alle questioni poste dall'assetto attuale[243].

Il provvedimento della Cassazione è ritornato quindi al modello del Codice della privacy, prima dell'entrata in vigore del Regolamento, confermando il ruolo allora svolto dal consenso dell'interessato, nel trattamento dei dati genetici e, più in generale, in quello dei dati sensibili.

3.2 *Profili del trattamento di dati biometrici*

Il ruolo della biometria, come misurazione numerica degli aspetti biologici, appare acquistare spazi, nella vita quotidiana, con l'evolversi della tecnologia e il suo diffondersi. Le misurazioni, in origine realizzate analogicamente, sono svolte via via sempre più mediante processi digitali, con modalità automatizzate o attraverso algoritmi[244].

Uno degli impieghi più rilevanti del trattamento di dati biometrici è quello che si ha, ormai da tempo, nella videosorveglianza. Tra le plurime finalità del videocontrollo, emerge la tutela della sicurezza. L'uso di videocamere e di nuovi strumenti, più sofisticati, ha destato preoccupazione nella misura in cui si è percepito un aumento del rischio di vedere violata la

---

biologici e big data*: l'evoluzione del consenso*, in *Dir. fam. e pers.*, 2022, 1061 ss., spec. 1085 ss.; GENOVESE, *Il trattamento dei dati personali su base consensuale. Ricognizioni giurisprudenziali di legittimità*, in D'AURIA (a cura di), *op. cit.*, 353 ss., spec. 369 ss.

[242]Il caso rappresentava, infatti, «*a fascinating point of reference to investigate how the interests of participants and freedom of research can be assessed in the Italian regulatory framework*». PENASA e M. TOMASI, *op. cit.*, 312.

[243] CORTI, *op. cit*., 597 s. Cfr. MARELLI e TESTA, *Scrutinizing the EU General Data Protection Regulation. How will new decentralized governance impact research?*, in *Science*, vol. 320, n. 6388, 498

[244] DE FRANCESCHI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 4, reg.Ue n. 679/2016, 169. Cfr. DUCATO, *I dati biometrici*, in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., 1285 ss. Con riguardo alle particolarità della firma grafometrica, v. A. CAVO, *La firma grafometrica e la protezione del dato biometrico nel quadro del Regolamento UE 2016/679*, in CUFFARO, D'ORAZIO e RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., 1414 ss.; EAD., *Firme grafometriche e trattamento dei dati biometrici alla luce del GDPR*, in MANTELERO e POLETTI (a cura di), *op. cit.*, 369 ss. Cfr. EAD., *Acquisizione del consenso informato in ambito diagnostico tramite firma biometrica e* data protection, in *Resp. civ. e prev*., 2019, 318 ss

propria riservatezza[245].

Anche in questo caso si è rivelata fondamentale la ponderazione del necessario bilanciamento dei diritti coinvolti. Gli orientamenti della Corte europea dei diritti dell'uomo hanno riconosciuto la tutela del rispetto della vita privata e familiare della persona anche verso l'utilizzo delle informazioni e delle immagini ottenute per mezzo di registrazioni e trattamenti svolti con videocamere, pur nel contemperamento di interessi opposti[246].

La Corte di giustizia ha contribuito, sul tema, a delineare la tutela della persona, nella sua opera di interpretazione. Così, nel caso *Ryneš*, oltre a sottolineare che «l'immagine di una persona registrata da una telecamera costituisce un dato personale ai sensi [dell'articolo 2, lettera a), della direttiva 95/46] se e in quanto essa consente di identificare la persona interessata», ha precisato che «una sorveglianza effettuata mediante una registrazione video delle persone […] immagazzinata in un dispositivo di registrazione continua, ossia in un disco duro, costituisce, conformemente all'articolo 3, paragrafo 1, della direttiva 95/46, un trattamento di dati personali automatizzato»[247].

Anche la Cassazione ha avuto modo di pronunciarsi in materia, affermando, con ri ferimento al quadro normativo italiano anteriore al Regolamento, che «l'installazione di un impianto di videosorveglianza all'interno di un esercizio commerciale, costituendo

---

[245] PIERUCCI, *Videosorveglianza e biometria*, in PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, cit., 1627 ss. Cfr. GIROTTO, *Il trattamento dei dati biometrici*, in CANESTRARI, FERRANDO, C.M. MAZZONI, RODOTÀ e ZATTI (a cura di), *Il governo del corpo*, nel *Trattato di biodiritto* diretto da Rodotà e Zatti, t. I, Milano, Giuffrè, 2011, 1237 ss. e lo studio di SMYTH, *Biometrics, Surveillance and the Law. Societies of Restricted Access, Discipline and Control*, Londra, Routledge, 2019. Si v. anche MANETTI e BORRELLO (a cura di), *Videosorveglianza e privacy*, Firenze, Pontecorboli editore, 2010; e, con un taglio più pratico, ALOVISIO (a cura di), *Videosorveglianza e GDPR. Profili di compliance nelle imprese e nelle pubbliche amministrazioni*, Milano, Giuffrè, 2021; ID. *et al.*, *Videosorveglianza e privacy*, Forlì, Experta, 2011. Rispetto all'uso nel processo penale, cfr. TORRE, *Nuove tecnologie e trattamento dei dati biometrici nel processo penale: il sistema automatico di riconoscimento delle immagini*, in ADINOLFI e SIMONCINI (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, Edizioni Scientifiche Italiane, 2022, 679 ss.

[246] V. Corte EDU, 28.1.2003, n. 44647/98, *Peck c. Regno Unito*, in *hudoc.echr.coe.int*, relativa a un caso di violazione dell'art. 8 CEDU, per la diffusione, in quotidiani e in televisione, delle immagini, tratte da un filmato di una telecamera a circuito chiuso, di un uomo che tentava il suicidio, senza sapere di essere ripreso; invece per Corte EDU, 5.10.2010, n. 420/07, *Köpke c. Germania*, in *Cass. pen*., 2011, 1972, ove la ricorrente era stata sospettata di furto sul luogo di lavoro e sottoposta di nascosto a videosorveglianza,
«nulla indicava che le autorità nazionali non avessero cercato un equo equilibrio, nell'ambito del loro margine di discrezionalità, fra il diritto della ricorrente al rispetto della propria vita privata di cui all'articolo 8 da una parte e, dall'altra, l'interesse del datore di lavoro alla protezione dei propri diritti di proprietà nonché l'interesse pubblico alla corretta amministrazione della giustizia». Pertanto, la domanda è stata dichiarata irricevibile. V. AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI, CORTE EUROPEA DEI DIRITTI DELL'UOMO e CONSIGLIO D'EUROPA (a cura di), *Manuale sul diritto europeo in materia di protezione dei dati*, cit., 270.

[247] Corte giust. UE, 11.12.2014, cit., punti 22 e 25.

trattamento di dati personali, deve formare oggetto di previa informativa, *ex* art. 13, d.lgs. n. 196 del 2003, resa ai soggetti interessati prima che facciano accesso nell'area videosorvegliata, mediante supporto da collocare perciò fuori del raggio d'azione delle telecamere che consentono la raccolta delle immagini delle persone e danno così inizio al trattamento stesso»[248].

Va tenuto ben presente, tuttavia, che non tutti i trattamenti di dati personali svolti tramite la videosorveglianza costituiscono trattamenti di dati biometrici, proprio perché, per dirsi tali, devono avere ad oggetto, secondo il Regolamento, dati ottenuti da un trattamento *tecnico specifico*[249].

Un compendio di indirizzi, generali e operativi, è stato offerto dal Comitato europeo per la protezione dei dati, con le Linee guida sul trattamento di dati personali attraverso dispositivi video, adottate nel 2020. Il Comitato ha osservato, tra l'altro, che «l'uso della videosorveglianza associata alla funzionalità del riconoscimento biometrico da parte di soggetti privati per proprie finalità (ad esempio, marketing, statistiche o persino sicurezza) richiederà, nella maggior parte dei casi, il consenso esplicito di tutti gli interessati (articolo 9, paragrafo 2, lettera a), ma potrebbe essere applicabile anche un'altra deroga idonea di cui all'articolo 9»; e, «quando il consenso è richiesto dall'articolo 9 del RGPD, il titolare del trattamento non deve condizionare l'accesso ai propri servizi all'accettazione del trattamento biometrico. In altre parole, in particolare quando il trattamento bio metrico è utilizzato a fini di autenticazione, il titolare del trattamento deve offrire una soluzione alternativa che non comporti il trattamento biometrico, senza imporre restrizioni o costi aggiuntivi all'interessato»[250].

La combinazione del trattamento di dati biometrici e dell'uso dell'intelligenza artificiale è stata oggetto, nel 2021, di una risoluzione del Parlamento europeo, che ha evidenziato il rischio di pregiudizi algoritmici nelle applicazioni e ha sostenuto la necessità della supervisione umana e di un chiaro quadro giuridico per prevenire le discriminazioni, soprattutto quando utilizzate dalla pubblica autorità, come dalle forze dell'ordine e di controllo delle frontiere[251].

---

[248] Cass., 5.7.2016, n. 13663, in *www.giustiziacivile.com*, 16 dicembre 2016, con nota di BRUNO, *L'informativa al trattamento dei dati personali negli esercizi commerciali sottoposti a videosorveglianza*.

[249] V. il considerando 51 del Regolamento.

[250] European Data Protection Board, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video. Versione 2.0,* cit., 20 e 22

[251] Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale, in *www.europarl.europa.eu*. In

Ai dati biometrici la proposta di Regolamento sull'intelligenza artificiale del 2021 dedica una specifica attenzione[252], prospettando alcune regole – come si può leggere nella relazione della Commissione che accompagna la proposta – «sulla protezione delle persone fisiche per quanto concerne il trattamento di dati personali, in particolare restrizioni sull'utilizzo di sistemi di IA per l'identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto»[253]. Si tratta di un uso che, «ritenuto particolarmente invasivo dei diritti e delle libertà delle persone interessate»[254], è vietato, in linea generale, dall'art. 5, par. 1, lett. *d*, della proposta e ammesso, in via eccezionale, solo in poche «situazioni elencate in modo esaustivo e definite rigorosamente, nelle quali l'uso è strettamente necessario per perseguire un interesse pubblico rilevante, la cui importanza

particolare, al punto 30, il Parlamento «sottolinea che l'uso dei dati biometrici è correlato in senso più ampio al principio di dignità umana, che è la base di tutti i diritti fondamentali garantiti dalla Carta; ritiene che l'utilizzo e la raccolta di dati biometrici per finalità di identificazione a distanza, ad esempio attraverso il riconoscimento facciale in luoghi pubblici, nonché i cancelli per il controllo automatizzato alle frontiere utilizzati per i controlli negli aeroporti, possano presentare rischi specifici per i diritti fondamentali, le cui implicazioni potrebbero variare notevolmente a seconda delle finalità, del contesto e dell'ambito di impiego; sottolinea, inoltre, la controversa validità scientifica della tecnologia di riconoscimento utilizzata, come le fotocamere che rilevano i movimenti degli occhi e le variazioni delle dimensioni della pupilla, nel contesto delle attività di contrasto; è del parere che l'uso dell'identificazione biometrica nel contesto delle attività di contrasto e giudiziarie dovrebbe sempre essere considerato ad "alto rischio" e pertanto soggetto a ulteriori requisiti, come previsto dalle raccomandazioni del gruppo di esperti di alto livello della Commissione sull'IA»; e, al punto 31, «esprime profonda preoccupazione per i progetti di ricerca finanziati nell'ambito di Orizzonte 2020 che diffondono l'intelligenza artificiale alle frontiere esterne, come il progetto iBorderCtrl, un "sistema intelligente di rilevamento delle menzogne" che permette di tracciare il profilo dei viaggiatori sulla base di un'intervista computerizzata effettuata con la webcam del passeggero prima del viaggio, e un'analisi basata sull'intelligenza artificiale di 38 microgesti, testata in Ungheria, Lettonia e Grecia; invita, pertanto, la Commissione, tramite strumenti legislativi e non legislativi e, ove necessario, mediante procedure d'infrazione, a introdurre il divieto di trattamento dei dati biometrici, comprese le immagini facciali, per finalità di applicazione della legge, tale da determinare sorveglianza di massa negli spazi accessibili al pubblico; invita, inoltre, la Commissione a interrompere il finanziamento della ricerca o diffusione della biometrica o di programmi che potrebbero portare alla sorveglianza di massa indiscriminata nei luoghi pubblici; sottolinea, in questo contesto, che andrebbe prestata particolare attenzione e dovrebbe essere applicato un quadro rigoroso all'utilizzo dei droni nelle operazioni di polizia».

[252] È la proposta della Commissione europea di Regolamento del Parlamento europeo e del Consiglio, *che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione*, del 21 aprile 2021, COM(2021) 206 final, c.d. *Artificial Intelligence Act*. Come annuncia al considerando 7, «la nozione di dati biometrici utilizzata nel presente regolamento è in linea e dovrebbe essere interpretata in modo coerente con la nozione di dati biometrici di cui all'articolo 4, punto 14), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, all'articolo 3, punto 18), del regolamento (UE) n. 2018/1725 del Parlamento europeo e del Consiglio e all'articolo 3, punto 13), della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio». La definizione di 'dati biometrici' di cui all'art. 3, n. 33, della proposta ricalca quella del Regolamento generale sulla protezione dei dati.

[253] Si v. pag. 7 del documento.

[254] Considerando 18 della proposta.

prevale sui rischi»[255].

In relazione alla disciplina dettata nell'ordinamento italiano, si ribadisce il ruolo delle misure di garanzia che è chiamato ad adottare il Garante. A ciò si aggiunge che, ai sensi dell'art. 2 *septies*, comma 7°, del Codice della privacy, nel rispetto dei principi in materia di protezione dei dati personali, con riferimento agli obblighi di cui all'articolo 32 del Regolamento, è ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, nel rispetto delle misure di garanzia[256].

In conclusione, va rilevato come il confine fra il trattamento dei dati biometrici e quello dei dati relativi alla salute, e ancor più, se si vuole, quello dei dati genetici, sia alquanto incerto. Dove finisca uno e inizi l'altro sembra sfumare, nella misura in cui tutte e tre queste categorie di dati personali si riferiscono all'elemento fisico o fisiologico della persona.

La "sovrapposzione concettuale" creata dalle formulazioni dell'art. 4 del Regolamento non pare però creare difficoltà nell'applicare le norme del Regolamento stesso[257]. Molto è lasciato quindi alle scelte dei legislatori nazionali, secondo il margine di discrezionalità loro conferito dall'art. 9, par. 4, nella costruzione di regimi coerenti, che siano in grado di tenere insieme e rispondere alle varie esigenze, realizzando l'opera del bilanciamento.

---

[255] Considerando 19 della proposta. Cfr. KINDT, *Biometric data processing: Is the legislator keeping up or just keeping up appearances?*, in GONZÁLEZ FUSTER, VAN BRAKEL e DE HERT (a cura di), *op. cit.*, 375 ss., spec. 396 ss.

[256] Il Garante mantiene in ogni caso anche l'essenziale funzione di controllo e sanzionatoria. Cfr. Provvedimento del Garante per la protezione dei dati personali del 10 febbraio 2022, n. 50, in *www.dirittodiinternet.it*, 20 maggio 2022, con annotazione di RUGGIERO PERRINO, *Monitoraggio biometrico: sanzione del Garante a Clearview*, con il quale l'Autorità ha irrogato una sanzione pecuniaria pari a venti milioni di euro a una società americana, per illecito trattamento di dati biometrici

[257] BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit.*, *sub* art. 4(14), 213

CAPITOLO II

IL CONSENSO DELL'INTERESSATO AL TRATTAMENTO DI DATI RELATIVI ALLA SALUTE

1. *Il diritto all'autodeterminazione informativa*

Il 15 dicembre 1983, nel celebre *Volkszählungsurteil*, la Corte costituzionale tedesca sancì il diritto all'autodeterminazione informativa[258].

L'autodeterminazione informativa, così come espressa dai giudici tedeschi, è il diritto fondamentale della persona di decidere autonomamente in merito alla divulgazione e all'utilizzo dei propri dati personali, derivante dal principio cardine della dignità e dalla garanzia del libero sviluppo della personalità, che richiede la protezione dell'individuo dalla raccolta, la conservazione, l'uso e la diffusione illimitati dei suoi dati personali .

Sin dal principio, questo diritto è stato riconosciuto in compromesso con le esigenze della comunità sociale. In quanto anch'esso espressione del generale diritto del cittadino alla libertà dallo Stato, può quindi subire restrizioni dalla pubblica autorità, ma ciò solamente nella misura in cui sia indispensabile per la tutela degli interessi pubblici e se previsto dalla legge, ossia nel rispetto della legalità[259] .

Il legislatore, nel tracciare i confini dell'autodeterminazione informativa, deve in ogni caso rispettare il principio di proporzionalità tra il mezzo (normativo) applicato e lo scopo perseguito e, al contempo, il principio di connessione fra la raccolta dei dati e la sua finalità, che dev'essere concreta e lecita [260]. Il portato della sentenza si è tradotto nei contenuti della normativa sulla privacy, costruita quindi, originariamente, in modo da offrire alla persona strumenti e tutele per determinarsi in base alle informazioni ricevute, per affermare, in altri termini, la libertà di ciascuno dal potere, pubblico o privato.

Tali affermazioni si sono trasmesse anche alla giurisprudenza di altri ordinamenti europei. Così, ad esempio, i giudici costituzionali spagnoli hanno fatto riferimento al

[258] BVerfG, 15.12.1983, in *Neue Juristische Wochenscrift*, 1984, 419.

[259] L'indeterminatezza dell'autodeterminazione informativa e la sua non misurabilità esatta nel bilanciamento con altri interessi risultano caratterizzanti – per non dire intrinseci a – questo diritto. «*Privacy law is not the product of logic*». WHITMAN, *op. cit.*, 1219.

[260] Oltre a questi, dalla pronuncia della Corte costituzionale tedesca possono trarsi, almeno indirettamente, altri principi, che tuttora si trovano nella legislazione in materia di protezione dei dati personali, come il principio di necessità oppure il principio di trasparenza, legato al diritto dell'interessato ad essere informato e a ottenere eventualmente la cancellazione dei dati che lo riguardano. SCHURR, *op. cit*., 977 ss. Cfr. ARZT, *op. cit*., 125 ss., spec. 129 ss.

concetto di autodeterminazione informativa, per la prima volta, con la sentenza n. 252, del 30 novembre 2000, mettendo a fuoco la nozione di libertà informatica, forse più nota con la classica espressione di *habeas data*.

Autodeterminazione, quindi, espressione della libertà. *Habeas corpus, habeas data*. Parole diverse ma simili, per contesti differenti, ma con la medesima vocazione[261].

Si è riconosciuto al singolo, per resistere al controllo del potere, il potere di controllo sulla circolazione dei propri dati. E l'esercizio di questo controllo è stato affidato, tradizionalmente, alla volontà del soggetto[262].

Ciò è vero, in modo particolare, nell'esperienza giuridica italiana, laddove la l. n. 675 del 1996, nel dare attuazione alla Direttiva madre del 1995, ha accolto il requisito del consenso, di cui agli artt. 7 e 8 della Direttiva, facendolo assurgere a regola e trasformando le altre basi giuridiche in deroghe [263].

L'autodeterminazione informativa compare nel primo provvedimento del Garante per la protezione dei dati personali del 28 maggio 1997, per qualificare il consenso dell'interessato come libero: esso può essere ritenuto effettivamente tale «solo se si presenta come manifestazione del diritto all'autodeterminazione informativa, e dunque, al riparo da qualsiasi pressione»[264].

Anche nell'ordinamento italiano, il diritto all'autodeterminazione informativa, evoluzione dinamica di una privacy statica, non è stato riconosciuto senza limiti e l'opera di

---

[261] RODOTÀ, *Il nuovo* habeas corpus*: la persona costituzionalizzata e la sua autodeterminazione*, in RODOTÀ e TALLACCHINI (a cura di), *Ambito e fonti del biodiritto*, nel *Trattato di biodiritto* diretto da Rodotà e Zatti, Milano, Giuffrè, 2010, 169 ss.;. Cfr. MAESTRI, *La persona digitale tra* habeas corpus *e* habeas data, in BILOTTA e RAIMONDI (a cura di), *Il soggetto di diritto storia ed evoluzione di un concetto nel diritto privato*, Napoli, Jovene, 2020, 277 ss.

[262] Cfr. BYGRAVE, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Alphen aan den Rijn, Kluwer Law International, 2002, 150 e 154; ID., *Data Privacy Law: An International Perspective*, cit., 158 ss.; BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit.*, *sub* art. 4. Si noti anche come la Carta dei diritti fondamentali dell'Unione europea, all'art. 8, par. 2, dispone che il trattamento dei dati personali deve avvenire, oltreché secondo il principio di lealtà e per finalità determinate,

[263] COMANDÉ, in GIANNANTONIO, LOSANO e ZENO-ZENCOVICH (a cura di), *op. cit.*, *sub* artt. 11 e 12, 101 s

[264] «E se – aggiunge l'Autorità garante – non viene condizionato all'accettazione di clausole che determinano un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto». Provvedimento del Garante per la protezione dei dati personali del 28 maggio 1997, in *Corr. giur*., 1997, 915 ss., con nota di ZENO-ZENCOVICH, *Il consenso informato" e la "autodeterminazione informativa" nella prima decisione del Garante*. In quella decisione, la riflessione sul consenso è preceduta da quella sull'informazione all'interessato, trattandosi, per poter spiegare il suo effetto, di consenso informato. Cfr. RODOTÀ, *Controllo e privacy della vita quotidiana. Dalla tutela della vita privata alla protezione dei dati personali*, in *Riv. crit. dir. priv*., 2019, 9 ss. Si è parlato anche di "rinascita del consenso". ID., *Tecnologie e diritti*, cit., 79 ss. V. MOREA, *Il consenso*, in FASANO (a cura di), *I vizi del consenso*, Torino, Giappichelli, 2013, 4 s.

bilanciamento, cui è chiamato l'interprete, è connaturata alla sua genesi[265].

Se l'impostazione della l. n. 675/1996 è stata, per certi versi, solo corretta con il d.lgs. n. 196 del 2003, la prospettiva è invece cambiata con l'entrata in vigore del reg. Ue n. 679 del 2016. Il consenso, da un punto di vista strettamente normativo, è ora solo una delle svariate basi giuridiche che legittimano il trattamento dei dati personali ed è solo una delle eccezioni al divieto di trattamento dei dati appartenenti alle categorie particolari. La residualità del consenso, nel sistema eurounitario, appare come diretta conseguenza della non assolutezza del diritto all'autodeterminazione informativa e come caratteristica funzionale alla circolazione dei dati personali, per lo sviluppo del mercato digitale[266].

Circoscrivere il diritto all'autodeterminazione informativa richiede però l'individuazione di dispositivi ulteriori rispetto al consenso dell'interessato, per evitare che la tutela della persona risulti sguarnita e che si apra a una graduale dissoluzione della privacy. Questi meccanismi, finalizzati alla protezione dei dati personali dovranno operare, come il consenso, preventivamente, non bastando istituti ad applicazione successiva e riparatoria, poiché la lesione del diritto significa già ineffettività – quando non negazione – della protezione dei dati personali stessa[267].

Quando tali dispositivi mirino ancora a permettere il controllo da parte della persona sulla circolazione dei propri dati, come ad esempio è per l'informativa, ossia l'attualizzazione del diritto dell'interessato all'informazione, possono essere intesi come strumenti di gestione del rischio, laddove però la valutazione circa i rischi e i benefici viene compiuta da chi assume il rischio e non dal titolare o dal responsabile del trattamento. Con una discreta conoscenza della tecnologia e rispetto ad operazioni di trattamento non troppo complesse, il

---

[265] FERONI, *I dati personali come oggetto di un diritto fondamentale*, in P. STANZIONE (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, Giappichelli, 2022. Così, ad esempio, si è ritenuto prevalente, in giurisprudenza, il diritto alla salute, rispetto alla riservatezza circa le informazioni riguardanti le persone. V. l'ordinanza, menzionata nel provvedimento del Garante per la protezione dei dati personali del 24 maggio 1999, cit., del Tribunale di Napoli, del 15 ottobre 1998. CATALLOZZI, *Dati sanitari e dati genetici: una frontiera aperta?*, cit

[266] R. MESSINETTI, *Circolazione dei dati personali e autonomia privata*, in ZORZI GALGANO (a cura di), *op. cit.*, Cfr. ERRIGO, *Sulle* nuove *libertà economiche. Criticità e prospettive del mercato digitale tra concorrenza, nuovi beni e autonomia negoziale*, in *Dir. cost*., 2023, fasc. 1

[267] In particolare, sulla distinzione fra riservatezza e protezione dei dati personali, MIRABELLI, *op. cit*., 317 s., osservava che, «anche se si accetta una nozione di diritto alla riservatezza che sia la più ampia possibile […] si deve riconoscere che la tutela che l'ordinamento offre alla riservatezza è una tutela repressiva e risarcitoria, successiva al verificarsi della lesione», mentre «l'interesse di cui si tratta richiede […] una tutela preventiva, diretta ad evitare la stessa possibilità di lesione». V. anche PUTIGNANI, *Consenso e disposizione della privacy*, cit.

soggetto è in grado di compiere consapevolmente la scelta[268]. In questo senso, la 'gestione' del rischio affidata all'individuo svolge la duplice funzione di tutelare la persona dall'ingerenza nella sua sfera, che si compie con il trattamento, e di consentire lo sfruttamento dei suoi dati.

Le evoluzioni e gli sviluppi non solo in ambito economico, ma anche nella società, e forse ancor più l'innovazione tecnologica portano la persona in un mercato in espansione: quello dei dati. L'autodeterminazione informativa è così chiamata, ora attraverso le disposizioni del Regolamento, a trovare declinazioni che rispondano ad esigenze nuove dell'economia, pur continuando a difendere la personalità dell'individuo[269].

1.1. *Autodeterminazione informativa in ambito sanitario*

L'autodeterminazione informativa nel contesto sanitario si connota specialmente per due aspetti: la sensibilità dei dati personali coinvolti e la qualifica prevalentemente pubblica dei soggetti che eseguono il trattamento e della loro funzione.

Partendo da tale constatazione, vediamo che proprio questo ambito sperimenta la tensione fra i valori e richieda un bilanciamento attento. Se si considera la peculiare sensibilità delle informazioni, emerge la necessità di una più elevata difesa della persona, mentre, considerando l'interesse pubblico perseguito, si evince l'esigenza del limite al diritto individuale. Linee di tutela che sembrano muoversi in direzioni opposte.

Quando si parla di autodeterminazione in ambito sanitario, tuttavia, non è a quella informativa che si fa usualmente riferimento, bensì all'autodeterminazione terapeutica o meglio, e più in generale, all'autodeterminazione della persona sul proprio corpo.

L'autodeterminazione accede, da questo piano, a un insieme di significati ampio e diversificato, una parte dei quali si rispecchia nei corrispondenti significati che stanno sul piano dell'autodeterminazione informativa e un'altra parte, la più cospicua, è invece ignota. Questo è probabilmente dovuto, da un lato, alla più breve e più recente storia dell'autodeterminazione informativa, in certo qual modo ancora poco conosciuta come poco conosciuta può essere l'innovazione della tecnologia, e, dall'altro, alle differenti potenzialità, sia concettuali che pratiche, ma anche evocative, dell'autodeterminazione

[268] MANTELERO, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 35, reg. Ue n. 679/2016

[269] C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, Giappichelli, 2021. Nel mercato, il profilo della protezione dei dati personali incrocia quello della protezione dei consumatori, specialmente con riguardo al funzionamento delle piattaforme digitali.

dell'individuo sul proprio corpo. L'insieme degli aspetti del potere o del controllo della persona sul corpo – portati all'attenzione del diritto, nei molteplici suoi rimandi e connessioni giuridici e metagiuridici – può descriversi e riassumersi nell'espressione 'governo del corpo'[270].

Nell'ordinamento italiano l'autodeterminazione[271], in questo senso, ma non solo, è considerata oggetto di un diritto fondamentale della persona, che trova il suo punto di sintesi con il diritto alla salute, nel consenso informato del paziente[272].

Il consenso informato al trattamento sanitario è elemento fondamentale del diritto all'autodeterminazione terapeutica della persona, annoverabile fra i diritti della personalità, e la sua violazione determina il diritto al risarcimento del danno[273].

La consensualità nella relazione di cura, affiancata dalla coniugazione del superamento dell'impostazione verticale e paternalistica del rapporto classico medico-paziente e della centralità della persona in medicina, ha trovato riconoscimento normativo con la legge 22 dicembre 2017, n. 219. Rubricata "Norme in materia di consenso informato e di disposizioni anticipate di trattamento", ha delineato una disciplina per la relazione di cura, dal momento attuale del dialogo fra medico e paziente a quello finale, in cui un'attualità di quel dialogo

[270] ZATTI, *Principi e forme del "governo del corpo"*, in CANESTRARI, FERRANDO, C.M. MAZZONI, RODOTÀ e ZATTI (a cura di), *Il governo del corpo*, nel *Trattato di biodiritto* diretto da Rodotà e Zatti, t. I, Milano, Giuffrè, 2011.

[271] È opportuno, in ogni caso, rammentare come il Codice civile abbia fornito, pur in termini alquanto angusti, un riconoscimento al diritto all'integrità fisica della persona e alla libertà di disporre di sé con l'art. 5, il quale, vietando gli atti di disposizione del proprio corpo «quando cagionino una diminuzione permanente della integrità fisica, o quando siano altrimenti contrari alla legge, all'ordine pubblico o al buon costume», implicitamente ammette gli atti che non rientrino in queste ipotesi. *Ex plurimis*, FARNETI, in CIAN (a cura di), *Commentario breve al Codice civile Cian Trabucchi*, 15a ed., 2022, *sub* art. 5 c.c.;

[272] «La circostanza che il consenso informato trova il suo fondamento negli artt. 2, 13 e 32 della Costituzione pone in risalto la sua funzione di sintesi di due diritti fondamentali della persona: quello all'autodeterminazione e quello alla salute, in quanto, se è vero che ogni individuo ha il diritto di essere curato, egli ha, altresì, il diritto di ricevere le opportune informazioni in ordine alla natura e ai possibili sviluppi del percorso terapeutico cui può essere sottoposto, nonché delle eventuali terapie alternative; informazioni che devono essere le più esaurienti possibili, proprio al fine di garantire la libera e consapevole scelta da parte del paziente e, quindi, la sua stessa libertà personale, conformemente all'art. 32, secondo comma, della Costituzione». Corte cost., 23.12.2008, n. 438, in *Giur. cost.*, 2008.

[273] «Il diritto al consenso informato del paziente, in quanto diritto irretrattabile della persona, va comunque e sempre rispettato dal sanitario, a meno che non ricorrano casi di urgenza, rinvenuti a seguito di un intervento concordato e programmato, per il quale sia stato richiesto ed ottenuto il consenso, e siano inoltre tali da porre in gravissimo pericolo la vita della persona [bene che riceve e si correda di una tutela primaria nella scala dei valori giuridici a fondamento dell'ordine giuridico e del vivere civile], ovvero che non si tratti di trattamento sanitario obbligatorio. Tale consenso è talmente inderogabile che non assume alcuna rilevanza, al fine di escluderlo, il fatto che l'intervento "absque pactis" sia stato effettuato in modo tecnicamente corretto, per la semplice ragione che, a causa del totale "deficit" di informazione, il paziente non è posto in condizione di assentire al trattamento, consumandosi nei suoi confronti, comunque, una lesione di quella dignità che connota l'esistenza nei momenti cruciali della sofferenza fisica e/o psichica». Cass., 15.4.2019, n. 10423, in *Danno e resp.*, 2019,.

può venire a mancare, per le condizioni di fragilità dell'individuo[274]. La legge non ha riempito un'area vuota di diritto, ma si è innestata su un terreno già abitato dal diritto vivente, nel fertile scambio di dottrina e giurisprudenza.

Il *consenso informato* [275]– espressione di cui si fa uso anche nella l. n. 219 del 2017 – è l'elemento che connota tanto l'autodeterminazione terapeutica quanto l'autodeterminazione informativa, ritrovando l'autodeterminazione, come comun denominatore, il profilo della volontà del soggetto.

All'interno del contesto sanitario, nel percorso di cura, l'autodeterminazione terapeutica supera e, per così dire, assorbe quella informativa. Infatti, nel momento in cui l'individuo esprime consapevolmente il proprio consenso al trattamento sanitario, non è necessario – come si ricava dall'art. 9 del Regolamento – che egli manifesti pure il consenso al trattamento dei suoi dati, perché questo avvenga .

Uno degli aspetti critici della disciplina italiana in materia, prima che entrasse in vigore e fosse applicabile il Regolamento, era proprio questo[276] . Dover richiedere il consenso del paziente al trattamento dei suoi dati sanitari per l'esecuzione della prestazione sanitaria apriva, in astratto, all'aporia del soggetto che avrebbe potuto domandare la prestazione medica, quindi acconsentendo al trattamento sanitario, e allo stesso tempo negare il consenso al trattamento dei dati relativi alla propria salute[277] . In concreto, per ottenere la prestazione

---

[274] Cfr. DI MASI, *La giuridificazione della relazione di cura e del fine vita. Riflessioni a margine della legge 22 dicembre 2017, n. 219,* in *Rivista di diritti comparati,* 2018.; ID., *La specialità della relazione di cura e la responsabilità medica. Un itinerario dal paternalismo al "consenso biografico"*, in M. FOGLIA (a cura di), *op. cit.*

[275] L''espressione fa eco all'inglese *informed consent*. È appena il caso di rammentare come il 'consenso informato' ritorni negli atti normativi del diritto eurounitario. Così, ad esempio, il Regolamento (UE) 2017/745, del Parlamento europeo e del Consiglio, del 5 aprile 2017, *relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio*, all'art. 2, n. 55), definisce il «consenso informato», ai fini di quella disciplina, come «l'espressione libera e volontaria di un soggetto della propria disponibilità a partecipare a una determinata indagine clinica, dopo essere stato informato di tutti gli aspetti dell'indagine clinica rilevanti per la sua decisione di partecipare oppure, nel caso dei minori e dei soggetti incapaci, l'autorizzazione o l'accordo dei rispettivi rappresentanti legalmente designati a includerli nell'indagine clinica». Norme dettagliate sul consenso informato all'indagine clinica sono poi date dagli artt. 63 ss., mentre l'art. 73 detta alcune prescrizioni in ordine alla protezione dei dati personali. Nell'ambito del diritto internazionale, cfr. NEGRI, *Consenso informato, diritti umani e biodiritto internazionale*, in *Biodiritto*, 2012, fasc. 2.

[276] «L'esame del travagliato *iter* che ha portato, nel nostro ordinamento, alla stesura del testo definitivo dell'art. 23 [l. n. 675/1996], fa emergere come uno dei profili più controversi, in materia di trattamento dei dati sanitari, sia rappresentato proprio dal consenso». ZAMBRANO, *Dati sanitari e tutela della sfera privata*, cit

[277] FINOCCHIARO, *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali,* cit. Si rileva, peraltro, come ancora il codice di deontologia medica, nella versione del 2014, richieda che il medico acquisisca il consenso informato del paziente per trattare i suoi dati personali: «Il medico acquisisce la titolarità del trattamento dei dati personali

medica, il paziente ovviamente acconsente anche al trattamento dei suoi dati sanitari e allora si coglie come il consenso possa dirsi del tutto apparente o necessitato[278] .

L'autodeterminazione informativa in ambito sanitario non è stata tuttavia cancellata ma va recuperata proprio nella dimensione della relazione di cura, sul piano del rapporto medico-paziente, non più gerarchizzato secondo gli schemi del passato, ma costruito sul dialogo e orientato all'alleanza terapeutica[279] . In questo orizzonte, la comunicazione da parte del professionista può includere anche l'informazione circa il trattamento dei dati sanitari del paziente e i suoi diritti. L'informativa, quindi, o meglio, l'informazione che il medico trasmette al paziente riveste un ruolo cruciale per permettere alla persona di autodeterminarsi in relazione all'uso dei propri dati personali [280], soprattutto quelli sensibili. Certo, questo non basta per garantire pienamente la protezione dei dati, servono, come si vedrà, ulteriori dispositivi.

Il consenso al trattamento dei dati personali non partecipa della medesima consensualità che è propria dell'autodeterminazione della persona verso le scelte che riguardano il proprio corpo, ma quanto maggiore è la sensibilità dell'informazione di cui si tratta tanto più la consensualità informativa si avvicina a quella del contesto terapeutico, poiché vi sarà una ponderazione anche in ordine al disvelamento del dato sensibile e alle sue conseguenze, in modo relativamente simile a quanto avviene per il trattamento sanitario cui si pensa di acconsentire. E quanto più si possa parlare di una consensualità informativa in questi termini, tanto più ineliminabile sembra, almeno assiologicamente, il consenso della persona al trattamento dei propri dati – i più sensibili – e tanto meno forti appaiono le cause che

previo consenso informato dell'assistito o del suo rappresentante legale ed è tenuto al rispetto della riservatezza, in particolare dei dati inerenti alla salute e alla vita sessuale. Il medico assicura la non identificabilità dei soggetti coinvolti nelle pubblicazioni o divulgazioni scientifiche di dati e studi clinici. Il medico non collabora alla costituzione, alla gestione o all'utilizzo di banche di dati relativi a persone assistite in assenza di garanzie sulla preliminare acquisizione del loro consenso informato e sulla tutela della riservatezza e della sicurezza dei dati stessi» (art. 11); «Il medico può trattare i dati sensibili idonei a rivelare lo stato di salute della persona solo con il consenso informato della stessa o del suo rappresentante legale e nelle specifiche condizioni previste dall'ordinamento» (art. 12).

[278] MINARDI, *op. cit*., 215; ZAMBRANO, *Dati sanitari e tutela della sfera privata*, cit.

[279] Cfr. GIO.M. RICCIO, Privacy *e dati sanitari*, cit.

[280]«L'informazione, allora, diventa pietra angolare della dignità personale e di quell'autodeterminazione informativa intesa quale possibilità di accedere alle informazioni che riguardano la propria persona, al fine di controllare la correttezza della loro acquisizione, correggere gli eventuali errori e sorvegliarne l'impiego nel corso del tempo». DI MASI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 77, d.lgs. 30 giugno 2003, n. 196. Secondo FINOCCHIARO, *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, cit., «più che il consenso al trattamento dei dati personali, dunque, è l'informativa a rappresentare lo strumento attraverso cui il diritto alla protezione dei dati personali dell'interessato si dovrebbe realizzare, anche nel settore sanitario».

legittimano il trattamento dei dati a prescindere dal consenso.

Alla luce del ruolo che continua a svolgere il consenso informato tanto sul piano del trattamento sanitario quanto su quello del trattamento dei dati personali e, nella specie, nell'ambito sanitario, sembra esserci un parallelismo, seppure imperfetto, fra autodeterminazione come governo del corpo e autodeterminazione come controllo delle proprie informazioni[281] . Governo del corpo fisico e governo del corpo digitale.

La protezione dei dati personali, derivazione della privacy, non va intesa quindi come limite ad altre situazioni giuridiche, come ostacolo all'esercizio di altri diritti o al perseguimento di diversi interessi, pubblici o privati, ma come diritto che integra la posizione del soggetto, aumentandone la tutela.

L'affermazione dell'autodeterminazione informativa in ambito sanitario, o forse la sua riaffermazione nell'accelerata evoluzione delle tecnologie e unitamente all'autodeterminazione terapeutica, può tradursi nel passaggio dal c.d. *patient empowerment* a un *patient and data subject empowerment* [282]. Con tutto ciò, riconoscendo la valenza generale dell'autodeterminazione della persona, senza ulteriori aggettivazioni o qualificazioni, espressione del più elevato principio – o valore – della dignità[283] .

2. *Il consenso dell'interessato nel reg. Ue 2016/679*

Il Regolamento generale sulla protezione dei dati definisce il "consenso dell'interessato" all'art. 4, n. 11, come «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano

[281]«Questo parallelismo dimostra come tanto l'autodeterminazione informativa quanto l'autodeterminazione terapeutica siano due aspetti essenziali della libertà e della dignità della persona oggi, entrambi meritevoli di una tutela tanto intensa quanto dinamica così da potersi adeguare alla rapidità propria dell'evoluzione tecnologica e scientifica, con cui questi diritti costantemente si rapportano. L'equilibrio tra i due è garanzia di qualità ed efficienza delle cure e del sistema sanitario cui il paziente si affida: tanto più in un contesto di progressiva digitalizzazione dei percorsi diagnostici e terapeutici». SORO, *Autodeterminazione terapeutica ed autodeterminazione informativa: i nuovi aspetti della dignità*, intervento al Convegno "La smaterializzazione dei documenti e il suo impatto sul sistema salute", in *www.garanteprivacy.it*, 6 maggio 2016.

[282] «*We can support the hypothesis of a transition from 'patient empowerment' to 'patient and data subject empowerment': an extension of the horizon that is useful to understand how the two core concepts go side- by-side in a logic of circular balancing of the personal rights*». FARES, *The processing of personal data concerning health according to the EU Regulation*, cit

[283] Si arrivò anche a parlare, nell'esperienza tedesca, di autodeterminazione biologica. «Questa ansia di aggettivare l'autodeterminazione, comprensibile nel momento in cui si voleva estenderne la rilevanza, rischia ora di farle perdere l'ormai raggiunta generalità, ed è bene che venga abbandonata». RODOTÀ, *Il diritto di avere diritti*, cit

oggetto di trattamento».

Già la Direttiva madre forniva una definizione di "consenso della persona interessata" all'art. 2, lett. *h*, ossia «qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento», discostandosi da quella nuova, come si può notare, per alcuni elementi, sul piano logico e sintattico.

La nuova definizione, raffrontata a quella della Direttiva, appare più dettagliata e più ricca di precisazioni, rappresentando l'evoluzione della riflessione sulla nozione[284].

Esistono anche altre norme che definiscono il 'consenso dell'interessato', in diversi atti normativi dell'Unione, ai fini degli stessi. Ciò è indice dell'espansione dell'interesse e dell'impatto dei dati personali nella società contemporanea, tanto per i soggetti del mercato quanto per le istituzioni.

In ogni caso, il riferimento, esplicito o implicito, rimane alla Direttiva madre o al reg. Ue n. 679 del 2016. Così, nel reg. Ce n. 45 del 2001, all'art. 2, lett. *h*, il consenso dell'interessato è definito in modo pressoché identico a come lo definiva la Direttiva del '95[285], mentre la Direttiva 2002/58/CE, all'art. 2, lett. *f*, prevede che il consenso, dell'utente o dell'abbonato, «corrisponde al consenso della persona interessata di cui alla direttiva 95/46/CE»[286]. Il reg. Ue n. 1725 del 2018, invece, lo definisce allo stesso modo del Regolamento generale sulla protezione dei dati personali[287]. Il reg. Ue n. 868 del 2022, il c.d. *Data Governance Act*[288], all'art. 2, n. 5, e il reg. Ue n. 1925 del 2022, il c.d. *Digital Markets Act*[289], all'art. 2, n. 32,

[284] Le incertezze sorte nell'interpretazione del testo della Direttiva del 1995 hanno determinato una formulazione più precisa per il Regolamento. BYGRAVE e TOSONI, in KUNER, BYGRAVE e DOCKSEY (a cura di), *op. cit., sub* art. 4. Cfr. KOSTA, *Consent in European Data Protection Law*, Leiden-Boston, Brill-Martinus Nijhoff Publishers, 2013

[285] Art. 2, lett. *h*, reg. Ce n. 45/2001: «Ai fini del presente regolamento s'intende per: […] h) "consenso dell'interessato": qualsiasi manifestazione di volontà libera, specifica e informata con la quale l'interessato accetta che i dati personali che la riguardano siano oggetto di un trattamento».

[286] Cfr. Corte giust. UE, 5.5.2011, causa C-543/09 (*Deutsche Telekom*), in *eur-lex.europa.eu*.

[287] Art. 3, n. 15), reg. Ue n. 1725/2018: «"consenso dell'interessato": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento».

[288] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, *relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati)*.

[289] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, *relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali)*. Insieme al Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, *relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)*, c.d. *Digital Services Act*, costituisce il pacchetto sui servizi digitali nell'Unione europea

fanno direttamente rinvio all'art. 4, n. 11, del reg. Ue n. 679/2016.

Una prima approfondita lettura delle disposizioni del Regolamento da parte della Corte di giustizia dell'Unione europea si è avuta con la sentenza del 1° ottobre 2019, resa nel caso *Planet49*. Chiamati a decidere sulla domanda di pronuncia pregiudiziale presentata dal *Bundesgerichtshof*, nell'ambito di una controversia tra la Federazione delle organizzazioni di consumatori tedesca e la società di giochi *online* "Planet49", in merito al consenso al trasferimento dei dati personali da parte dei partecipanti a un gioco agli sponsor e ai partner della società, i giudici di Lussemburgo hanno affrontato aspetti legati al consenso dell'interessato al trattamento dei propri dati personali[290].

Il caso, nello specifico, riguardava l'installazione, a scopi commerciali, di *cookies* – particolarmente quelli analitici[291]– da parte della società organizzatrice. L'installazione era effettuata al momento della registrazione dell'utente attraverso una casella, preselezionata e deselezionabile, di prestazione del consenso.

Partendo dall'art. 7, lett. *a*, della Direttiva madre, che richiedeva che la manifestazione consenso, come base giuridica che legittima il trattamento dei dati personali, avvenisse «in maniera inequivocabile», la Corte giunge subito ad individuare il consenso *attivo* come il solo tipo di consenso conforme a quello prescritto dall'allora legislatore comunitario. Prendendo in esame le disposizioni del reg. Ue 2016/679, questa interpretazione non solo trova conferma, ma anche – e a maggior ragione – si impone con più rigore. Infatti, la formulazione dell'art. 4, n. 11, del Regolamento delinea un consenso dell'interessato qualificato, la cui manifestazione avviene mediante dichiarazione o *azione positiva* inequivocabile.

Il considerando 32 ne riprende i tratti definitori e richiede un «atto positivo inequivocabile». Ammette pure che questo inequivocabile atto positivo possa concretizzarsi nella «selezione di un'apposita casella in un sito web», ma, allo stesso tempo, esclude che

[290] Corte giust. UE, 1°.10.2019, causa C-673/17 (*Planet49*), in *Dir. fam. e pers*., 2020.; in *Giur. it*., 2020., con nota di REINALTER e VALE

[291] P. GALLO, *Diritti della personalità e interessi non patrimoniali*, nel *Digesto online*, agg. 2022, in *OneLegale*, par. 25, che fa riferimento alla pronuncia in questione: «I cookies si distinguono in tre categorie, quelli tecnici, quelli analitici e quelli di profilazione; i primi servono per effettuare la navigazione e non necessitano di consenso; i secondi invece servono per raccogliere informazioni aggregate sul numero degli utenti e sulle modalità di visita del sito; i terzi servono per monitorare il navigatore ed individuare le sue abitudini di navigazione e di consumo per finalità pubblicitarie, anche a favore di soggetti terzi; sia l'installazione dei cookies analitici che di quelli di profilazione richiede il previo consenso del navigatore; un tale consenso, che deve essere espresso in via preventiva, può essere dato anche spuntando un'apposita casella; non è invece consentito che la casella appaia già spuntata, con conseguente necessità per l'utente, intenzionato a negare il consenso, di deselezionare una casella sulla quale risulti già apposto il flag».

sia configurabile il consenso nella «preselezione di caselle»[292].

Per la Corte, quindi, quando i trattamenti di dati personali sono autorizzati mediante una casella preselezionata che l'utente deve deselezionare per dissentire, il consenso non è validamente espresso[293].

La nozione di consenso dell'interessato risulta dunque limitata dalla giurisprudenza della Corte di giustizia, che ne chiarisce i confini. Gli assunti della sentenza *Planet49* vengono ripresi e specificati dalla sentenza dell'11 novembre 2020, resa nel caso *Orange Romania*, che ritorna sul consenso dell'interessato[294]. La pronuncia ribadisce, infatti, che la manifestazione di volontà, cui accede l'art. 4, n. 11, del Regolamento, è solo quella espressa per mezzo di una dichiarazione o azione positiva, accoglie cioè la lettura che richiede un consenso attivo[295].

Nella sentenza *Orange Romania*, la Corte prende in esame le caratteristiche del consenso dell'interessato, tanto alla luce della Direttiva madre quanto a quella del Regolamento e rileva, innanzitutto, che esso deve corrispondere a una manifestazione di volontà *specifica*, con ciò dovendo intendersi che si deve riferire «precisamente al trattamento dei dati interessati e non può essere desunta da una manifestazione di volontà avente un oggetto distinto». A questo proposito, precisa, passando dal testo dell'art. 4, n. 11, del Regolamento a quello dell'art. 7, par. 2, dello stesso, che, quando il consenso venga prestato nel contesto di una dichiarazione scritta, inerente anche ad altre questioni, la richiesta di consenso dev'essere presentata in modo chiaramente distinguibile dalle altre materie. Il rilievo si completa con quanto si può leggere al considerando 42, per cui «una siffatta dichiarazione deve essere presentata in forma comprensibile e facilmente accessibile ed essere formulata in un linguaggio semplice e chiaro, in particolare quando si tratti di una dichiarazione di consenso da redigere preventivamente da parte del responsabile del trattamento dei dati personali».

[292] Per il considerando 32 non dovrebbe configurare consenso nemmeno il silenzio o l'inattività. V. punto 62 della sentenza.

[293] Punti 63 e 65 della sentenza. Nel caso di specie si trattava di archiviazione di informazioni o accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente di un sito Internet.

[294] Corte giust. UE, 11.11.2020, causa C-61/19 (*Orange Romania*), in *Foro amm.*, 2020, 2073

[295] In quel caso, la questione pregiudiziale riguardava la configurabilità del consenso al trattamento, per contratti sottoscritti da utenti con un fornitore di servizi di telecomunicazione mobile, l'"Orange Romania", in cui la clausola sulla conservazione di copie degli atti, contenenti dati personali a fini di identificazione, era posta in relazione a una casella, che talvolta risultava spuntata e talvolta no. A fronte della effettiva conservazione di copie di documenti d'identità dei suoi clienti, la società era stata sanzionata, non avendo dimostrato che tali clienti avessero prestato il loro valido consenso, e avverso il provvedimento che irrogava la sanzione presentava ricorso.

Come anticipato, il consenso dev'essere *informato*, ciò implicando, sia nell'ambito del Regolamento sia già in quello della Direttiva n. 46 del 1995, che il responsabile del trattamento trasmetta all'interessato un'informazione alla luce di tutte le circostanze che corredano il trattamento dei dati, con le medesime caratteristiche di comprensibilità, accessibilità, semplicità e chiarezza, cosicché egli sappia il tipo di dati che devono essere trattati, l'identità del responsabile del trattamento, la durata, le modalità e le finalità. Tale informazione deve permettere all'interessato di individuare agevolmente le conseguenze della prestazione del consenso e assicurare che venga espresso con piena cognizione di causa[296].

A una corretta informazione è connessa la *libertà* del consenso. In particolare, la Corte osserva che, per garantire all'interessato la libertà di scelta, le clausole del contratto «non devono indurre la persona interessata in errore circa la possibilità di stipulare il contratto anche qualora essa rifiuti di acconsentire al trattamento dei suoi dati»[297].

L'intreccio di questi caratteri si raccoglie e confluisce nel rispetto del principio di responsabilizzazione, o *accountability*, espresso all'art. 5, par. 2, del Regolamento, e di cui è derivazione l'art. 7, par. 1. Secondo tale disposizione, infatti, quando la legittimazione del trattamento riposa sul consenso dell'interessato, il titolare deve essere in grado di dimostrare che questi lo abbia prestato. Per la Corte, l'onere della prova dell'esistenza di un valido consenso grava sul titolare del trattamento anche in virtù della previsione per cui la manifestazione del consenso deve avvenire *in modo inequivocabile*.

Con queste premesse, la Corte conclude per l'inidoneità del contratto – in una serie di ipotesi – alla dimostrazione di una valida manifestazione del consenso.

---

[296] V. punto 40. Secondo il considerando 42, «ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali». Si può comprendere allora come il requisito dell''informatezza' del consenso sia strettamente legato all'osservanza di quanto disposto dal Regolamento circa l'informativa all'interessato e, quindi, a venire in gioco sono soprattutto gli artt. 13 e 14 dello stesso. V. GIOVANNANGELI, *L'informativa agli interessati e il consenso al trattamento*, in PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, cit. Prende in esame il 'dovere di informativa', nel contesto della l. n. 675 del 1996, BARBA, *Le modalità del trattamento*, in CUFFARO e RICCIUTO (a cura di), *La disciplina del trattamento dei dati personali*, Torino, Giappichelli, 1997.

[297] Punto 41. Il riferimento normativo è all'art. 10, lett. *c*, secondo trattino, della Direttiva, e dell'art. 13, par. 2, lett. *b* e *c*, del Regolamento, letto insieme al considerando 42. Per il considerando 42, «il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio». Ma v. anche quanto espresso al considerando 43. In merito alla valutazione sulla libertà del consenso prestato, trova applicazione l'art. 7, par. 4, del Regolamento. Cfr. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. e dir. priv.*, 2016.

Sul modo di intendere il consenso dell'interessato è intervenuta anche l'attività interpretativa del Gruppo di lavoro "Articolo 29", fornendo una lettura attenta dei suoi caratteri, affinché possa dirsi espresso validamente.

Tenuto conto che a legittimare il trattamento di dati personali possono essere anche altre basi giuridiche, diverse dal consenso, nelle "Linee guida sul consenso ai sensi del regolamento (UE) 2016/679" il Gruppo di lavoro ribadisce, con riguardo alla posizione del titolare, che «l'invito ad accettare il trattamento dei dati dovrebbe essere soggetto a criteri rigorosi, poiché sono in gioco i diritti fondamentali dell'interessato e il titolare del trattamento intende svolgere un trattamento che senza il consenso sarebbe illecito».

Il rigore esegetico in ordine al consenso e al suo quadruplice requisito – di *libertà*, *specificità*, *informatezza* e *inequivacobilità* – è mantenuto dal Comitato europeo per la protezione dei dati, che, nelle sue Linee guida sul consenso, del 2020, offre riflessioni approfondite e attuali.

Tra i vari aspetti del consenso, che vengono individuati declinando i requisiti previsti dal Regolamento, giova ricordare la *granularità* e la necessità di manifestazione *previa*. Il consenso dev'essere, infatti, granulare, cioè prestato in relazione ad ogni finalità del trattamento e, quindi, se un'attività di trattamento di dati personali presenta più finalità, l'interessato deve poter esprimere il suo consenso in relazione a ciascuna di esse[298]. E, com'è implicito nelle disposizioni del Regolamento, esso va prestato prima dell'inizio delle operazioni di trattamento, dovendo fungere da base per la legittimazione del trattamento.

Il consenso dell'interessato, inoltre, come pure messo in luce nella menzionata giurisprudenza della Corte di giustizia, è soggetto alle disposizioni dettate dall'art. 7. Tra queste, particolare attenzione merita la previsione di cui al par. 3, che ne sancisce la revocabilità: il consenso al trattamento dei dati personali è sempre *revocabile*.

La revoca del consenso è un diritto incondizionato, che si esercita nei confronti di un trattamento che è stato legittimamente iniziato sulla base del consenso stesso dell'interessato.

[298] «Un servizio può comportare trattamenti multipli per più finalità. In tal caso, l'interessato dovrebbe essere libero di scegliere quale finalità accettare anziché dover acconsentire a un insieme di finalità. […] Se il titolare del trattamento ha riunito diverse finalità di trattamento e non ha chiesto il consenso separato per ciascuna di esse non c'è libertà». *Ivi*, 13. Tale profilo emerge anche dal considerando 32, secondo cui «il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste». Si consideri pure che granularità del consenso viene a combinarsi con il principio di limitazione delle finalità, *ex* art. 5, par. 1, lett. *b*, del Regolamento, nell'ottica di una elevata tutela della persona. Cfr. ORLANDO, *Per un sindacato di liceità del consenso* privacy, in *Persona e mercato*, 2022, fasc. 4. Con particolare riguardo alle finalità di trattamento per scopi di ricerca scientifica, v. il considerando 33.

Va tenuta distinta dall'opposizione al trattamento dei dati, *ex* art. 21, la quale, invece, è un diritto condizionato, ai motivi connessi alla situazione particolare dell'interessato e alla cogenza dei motivi legittimi del titolare del trattamento, che si esercita nei confronti di un trattamento legittimamente iniziato non sulla base del consenso dell'interessato, ma sulla base dei presupposti di cui all'art. 6, par. 1, lett *e* e *f*, del Regolamento. In entrambi i casi si ha per conseguenza un diritto di cancellazione.

Alla particolare ipotesi del consenso riferibile a un minorenne è dedicato l'art. 8, il cui par. 1 individua nel compimento del sedicesimo anno di età il momento a partire dal quale il consenso prestato al trattamento dei dati personali può valere come base giuridica ai sensi dell'art. 6 del Regolamento. La disposizione, dettata con riguardo all'offerta diretta di servizi della società dell'informazione ai minori, prevede poi che il consenso vada prestato o autorizzato dal "titolare della responsabilità genitoriale", qualora, invece, il minore interessato abbia meno di sedici anni[299].

Ma all'interno del reg. Ue n. 679 del 2016, il consenso non si ritrova solo come base giuridica che legittima il trattamento dei dati personali, ai sensi dell'art. 6, o deroga al divieto di trattamento di dati sensibili, *ex* art. 9. Esso assume un'ulteriore e varia consistenza in relazione ad altre situazioni giuridiche. È così per il consenso al trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, ai sensi dell'art. 49, par. 1, lett. *a*, o per il consenso alla possibilità di assoggettarsi a una decisione basata unicamente sul trattamento automatizzato, ai sensi dell'art. 22, par. 2.

È il caso di osservare come, in queste ultime due ipotesi, il consenso si presenti, al pari di come descritto all'art. 9, con la qualificazione di 'esplicito'. Si tratta di fattispecie in cui il legislatore eurounitario ha inteso offrire una garanzia più stringente, per la difesa dell'interessato, per via di «circostanze nelle quali emergono gravi rischi per la protezione dei dati e in cui si ritiene quindi appropriato un livello elevato di controllo individuale sui dati personali».

La prestazione del consenso, infine, non cancella il rispetto di tutti gli altri principi e le regole propri della protezione dei dati personali da parte del titolare del trattamento, che deve comunque sempre osservare[300].

---

[299] A. THIENE, *Gioventù bruciata online: quale responsabilità per i genitori?*, in ANNONI e A. THIENE (a cura di), *op. cit* che analizza, in senso critico, la scelta operata dal legislatore italiano, all'art. 2 *quinquies* del Codice della privacy, di abbassare la soglia d'età a quattordici anni. Sul consenso dei minori, v. anche BOZZI, *I dati del minore tra protezione e circolazione: per una lettura non retorica del fenomeno*, in *Eur. e dir. priv.*, 2020, 251 ss.;

[300] THOBANI, *Il consenso al trattamento dei dati personali*, cit., 134.

Sembra importante aggiungere, a queste considerazioni, che del consenso al trattamento dei dati personali il diritto eurounitario fornisce una regolamentazione in autonomia, o meglio il consenso – tanto quanto, del resto, altre fattispecie inerenti a questa materia, come, ad esempio, la nozione stessa di dato personale – si trova disciplinato nel Regolamento e in esso trova il suo inquadramento, senza un rinvio ai concetti propri delle tradizioni giuridiche nazionali. E ciò, implicitamente, suggerirebbe la necessità di utilizzare nell'interpretazione le categorie del diritto dell'Unione, sempre se ve ne siano. Invece la dottrina ha fatto ricorso alle categorie interne per interpretare la figura del consenso nel Regolamento. A tal proposito, anche se si comprende bene la posizione di chi nutre dubbi della legittimità di tale percorso logico, cioè del radicamento nella dogmatica nazionale – si pensa soprattutto al caso italiano – di istituti del diritto eurounitario e del rispecchiarsi delle idee della tradizione interna nelle disposizioni del Regolamento, non si ritiene comunque privo di alcuna utilità il raffronto con i concetti tradizionali dell'ordinamento nazionale[301].

2.1. *Consenso al trattamento di dati neutri*

Ai sensi dell'art. 6, par. 1, lett. *a*, del Regolamento, il trattamento di dati personali è lecito se «l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità».

Come già anticipato, la norma individua nel consenso la base giuridica che legittima il trattamento di dati personali. Non è la sola, essendo previste, infatti, altre fattispecie produttive dello stesso effetto, alle lett. da *b* a *f* dell'art. 6, par. 1. Se non ricorre nessuna di tali ipotesi e l'interessato non presta il consenso, un eventuale trattamento dei suoi dati personali risulta illecito.

Il consenso dell'interessato, quindi, permette che si svolgano lecitamente operazioni di trattamento di dati personali[302].

È opportuno tornare a considerare, anche in questa sede, come sia necessario il rispetto delle condizioni di liceità dettate dall'art. 6 del Regolamento, tanto che si tratti di dati neutri quanto che si tratti di dati sensibili, con la differenza che, per quel che riguarda questi ultimi, il trattamento può aversi solo se ricorre una delle eccezioni al divieto di trattamento.

---

[301] V. A.M. GAROFALO, *Regolare l'irregolabile: il consenso al trattamento dei dati nel GDPR*, in ORLANDO e CAPALDO (a cura di), *Annuario 2021 Osservatorio Giuridico sulla Innovazione Digitale*, Roma, Sapienza Università Editrice, 2021., e i riferimenti ivi contenuti

[302] Cfr. GENOVESE, *Trattamento dei dati personali e consenso dell'interessato*, in MORACE PINELLI (a cura di), *op. cit.*, 2023.

Il dibattito sul consenso dell'interessato, in dottrina, si è concentrato sulla natura giuridica dell'atto e, in estrema sintesi, si è polarizzato – pur nella varietà delle opinioni – attorno a due letture[303].

Secondo una prima interpretazione, il consenso al trattamento dei dati personali sarebbe stato un atto di autorizzazione[304]. Manifestazione unilaterale di volontà del soggetto o atto non negoziale, che giustifica – o scrimina, come consenso dell'avente diritto[305] – un comportamento altrimenti illecito, ossia il trattamento.

Per una seconda interpretazione, invece, il consenso dell'interessato si sarebbe potuto ricondurre entro i confini della negozialità e forse anche della sinallagmaticità. Manifestazione di volontà, quindi, afferente a un accordo tra le parti, che si spiega nell'ambito di un rapporto di tipo contrattuale[306].

A ciascuno di questi due modi di intendere il consenso era sottesa una peculiare visione della protezione dei dati personali e della relativa disciplina[307]. La prima lettura era, infatti, espressione della visione personalista delle norme in materia di trattamento di dati personali. Essa si coniugava bene con la considerazione del dato personale come parte di identità della persona e con la proiezione di una corporeità umana – presidiata dal diritto – nella dimensione digitale. Identità digitale, corpo digitale, consenso come strumento di protezione della persona nella sfera digitale[308].

La seconda lettura, d'altro canto, muoveva dall'approccio economico e dalla concezione liberale del mercato[309]. Seguiva una linea strettamente privatistica[310], affine all'idea del dato personale come una *res* di cui poter disporre e sulla quale vantare uno *ius excludendi alios*, che conduceva il consenso al trattamento dei dati personali nell'orbita concettuale del contratto.

Il diverso modo di vedere il consenso e di descriverne la natura implicava l'approdo a differenti soluzioni interpretative, specialmente in ordine alla revocabilità del consenso

---

[303] V. GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, cit.; CAGGIA, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit., sub* art. 7, reg. Ue n. 679/2016.

[304] RODOTÀ, *Tecnologie e diritti*, cit; D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998

[305] PATTI, in C.M. BIANCA e BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196, Codice della privacy*, cit., *sub* art. 23

[306] RICCIUTO, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, cit.,

[307] ALPA, *La "proprietà" dei dati personali*, in ZORZI GALGANO (a cura di), *op. cit.*,.

[308] P. GALLO, Big data *e diritto allo sfruttamento economico dei dati personali*, in D'AURIA (a cura di), *I problemi dell'informazione nel diritto civile, oggi. Studi in onore di Vincenzo Cuffaro*, Roma Tre press, 2022

[309] ZENO-ZENCOVICH, voce «Cosa», nel *Digesto IV ed., Disc. priv., sez. civ.*, III, Torino, Utet, 1998.;

[310] Cfr. OPPO, *Sul consenso dell'interessato*, *ivi.*

stesso: se fosse stato atto autorizzativo, si sarebbe potuto revocare, mentre, se fosse stato atto negoziale, non sarebbe stato liberamente revocabile[311]. Oggi, l'espressa previsione, della revocabilità del consenso, all'art. 7 del Regolamento, chiude sostanzialmente, o almeno in buona parte, il dibattito sulle conseguenze della distinzione teorica.

La contrapposizione fra queste due classiche impostazioni nell'interpretazione del consenso e le due prospettive generali sulla protezione dei dati personali pare superata ora da una terza lettura, che fa tesoro dell'esperienza tanto teorica e sapienziale quanto pratica e concreta, sul trattamento dei dati personali. Secondo questa posizione, infatti, per comprendere il consenso bisogna guardare più alla sua funzione che alla sua struttura. Prendendo atto, da un lato, dell'estrema difficoltà – per non dire impossibilità – di ricostruire in modo univoco il consenso e, dall'altro, dell'esistenza effettiva, anche per il diritto, di un mercato dei dati, ma senza abdicare al personalismo, questa terza via arriva a concepire il consenso dell'interessato come dotato di una natura articolata, composita o poliedrica, dipendente dalla tipologia del dato personale cui si riferisce e potenzialmente, almeno in parte, anche dal contesto in cui è inserito[312].

Il binomio consenso dell'interessato e contratto non si esaurisce però in questa rappresentazione teorica e continua, attraverso le norme, per l'interpretazione di altre disposizioni o l'introduzione di regole nuove, a interrogare la scienza del diritto.

Abbiamo ricordato che il trattamento dei dati personali può legittimarsi, ai sensi dell'art. 6, par. 1, lett. *b*, del Regolamento, quando sia necessario all'esecuzione di un contratto di cui l'interessato è parte. In questo caso, l'interessato ha prestato un consenso, ma per la conclusione del contratto, non al trattamento dei suoi dati[313]. Come sottolineato dal Comitato europeo per la protezione dei dati, consenso e contratto sono due basi giuridiche distinte e – almeno teoricamente – non possono fondersi l'una nell'altra, dal momento che, per essere espresso validamente, il consenso al trattamento dev'essere libero e tale non sarebbe in un vincolo contrattuale[314].

---

311 THOBANI, *I requisiti del consenso al trattamento dei dati personali*, cit., 2 ss.; EAD., *Il consenso al trattamento dei dati personali*, cit., 134 s. È pur vero che, come osservato in dottrina, anche nell'ambito contrattuale, non sempre la manifestazione di volontà del soggetto che si inserisce in un accordo si traduce in un atto irrevocabile. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, cit.

312 POLETTI, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 6, reg. Ue n. 679/2016

313 Cfr. C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit.

314 «L'articolo 7, paragrafo 4, indica, tra l'altro, che è altamente inopportuno "accorpare" il consenso all'accettazione delle condizioni generali di contratto/servizio o "subordinare" la fornitura di un contratto o servizio a una richiesta di consenso al trattamento di dati personali che non sono necessari per l'esecuzione del

Dobbiamo inoltre osservare che l'espressione del consenso al trattamento dei dati personali, nella misura in cui trasferisce le informazioni e ne permette l'utilizzo, potrebbe, invece, valere come "controprestazione", al pari del pagamento del prezzo e anche in sua sostituzione, all'interno di uno schema contrattuale[315].

Le riflessioni sul punto, particolarmente stimolate con la presentazione della proposta di Direttiva sulla fornitura di contenuti digitali[316], devono tenere in considerazione il testo – approvato dal Parlamento europeo e dal Consiglio e già entrato in vigore – della Direttiva n. 770 del 2019[317].

Si evince, dall'insieme delle sue disposizioni, che l'interessato – o meglio, in questo contesto, il consumatore – può fornire dati personali in cambio di contenuti digitali[318].

Allo stesso tempo, però, è rifiutata la visione del dato personale come merce di scambio[319] e la normativa eurounitaria in materia di protezione dei dati personali è ritenuta prevalente[320]. In particolare, vengono mantenute l'autonomia concettuale del consenso dell'interessato, come base giuridica per il trattamento, e, con essa, l'applicabilità della

---

contratto o servizio. Si presume che il consenso prestato in una tale situazione non sia stato espresso liberamente (considerando 43). L'articolo 7, paragrafo 4, mira a garantire che la finalità del trattamento dei dati personali non sia mascherata né accorpata all'esecuzione di un contratto o alla prestazione di un servizio per il quale i dati personali non sono necessari. In tal modo, il regolamento assicura che il trattamento dei dati personali per cui viene richiesto il consenso non possa trasformarsi direttamente o indirettamente in una controprestazione contrattuale. Le due basi legittime per la liceità del trattamento dei dati personali, ossia il consenso e l'esecuzione di un contratto, non possono essere riunite e rese indistinte». European Data Protection Board, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, Versione 1.1*, cit., 11. V. KOTSCHY, *op. cit*; DE CRISTOFARO, *Die datenschutzrechtliche Einwilligung als Ge- genstand des Leistungsversprechens*, cit.

[315] G. RESTA e ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. e proc. civ*., 2018.;

[316] DE FRANCESCHI, *La circolazione dei dati personali nella proposta di Direttiva UE sulla fornitura dei contenuti digitali*, cit.;

[317] Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, *relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali*.

[318] Art. 3, par. 1, secondo periodo della Direttiva: «La presente direttiva si applica altresì nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti». Il testo dell'art. 3, per il vero, è stato modificato rispetto a quello che era stato proposto, a seguito delle critiche ufficiali mosse alla equiparazione dei dati personali a una risorsa che potesse essere scambiata effettivamente come un prezzo

[319] Al considerando 24 si legge che la Direttiva riconosce «appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce».

[320] Art. 3, par. 8, della Direttiva: «Il diritto dell'Unione in materia di protezione dei dati personali si applica a qualsiasi dato personale trattato in relazione ai contratti di cui al paragrafo 1. In particolare, la presente direttiva fa salvo il regolamento (UE) 2016/679 e della direttiva 2002/58/CE. In caso di conflitto tra le disposizioni della presente direttiva e del diritto dell'Unione in materia di protezione dei dati personali, prevale quest'ultimo».

relativa disciplina del Regolamento[321].

Il legislatore italiano, nel dare attuazione alla dir. Ue n. 770/2019, con il d.lgs. 4 novembre 2021, n. 173, è intervenuto modificando il d.lgs. 6 settembre 2005, n. 206, c.d. Codice del consumo e, in particolare, inserendo, nel Titolo III della Parte IV, il nuovo Capo I *bis*, "Dei contratti di fornitura di contenuto digitale e di servizi digitali", che comprende gli articoli da 135 *octies* a 135 *vicies ter*. L'operazione ha recepito nel diritto interno la possibilità di concludere contratti, tra consumatore e professionista, nei quali il contenuto o il servizio digitale viene fornito a fronte della comunicazione, da parte del consumatore, di suoi dati personali, fatta sempre salva l'applicazione delle norme del reg. Ue n. 679/2016 e del d.lgs. n. 101/2018[322].

La previsione normativa, tracciata dalla Direttiva n. 770 del 2019, si orienta, in coerenza con il dettato del Regolamento generale sulla protezione dei dati, specialmente l'art. 6, prendendo in considerazione – e ammettendo, in questa cornice contrattuale – il consenso al trattamento del dato per finalità estranee al servizio o prodotto ricevuto dall'operatore economico, che è il titolare del trattamento.

Come osservato in dottrina, in questi casi, il consenso dell'interessato al trattamento dei suoi dati personali appartiene a un momento diverso e logicamente successivo a quello del consenso del consumatore alla conclusione del contratto e tale differenza disegna una duplicità di consensi che implica la duplicità di discipline applicabili: quella sulla protezione dei dati personali per il consenso al trattamento e quella del contratto per il consenso al perfezionamento della fattispecie contrattuale[323].

Poiché, il rilascio del consenso al trattamento dei propri dati personali, conformemente a quanto sancito dal reg. Ue n. 679/2016, non può essere oggetto di un'obbligazione coercibile, per comprendere tale atto si è fatto ricorso alla categoria della prestazione condizionale[324]. Questa teoria spiega il collegamento tra la prestazione del consenso al

[321] E così, secondo il considerando 38 della Direttiva, «qualsiasi trattamento di dati personali in relazione a contratti rientranti nell'ambito di applicazione della presente direttiva è lecito solo se è conforme alle disposizioni del regolamento (UE) 2016/679 relativo ai fondamenti giuridici per il trattamento dei dati personali. Quando il trattamento dei dati personali si basa su un consenso, segnatamente a norma dell'articolo 6, paragrafo 1, lettera a), del regolamento (UE) 2016/679, si applicano le disposizioni specifiche di tale regolamento, comprese quelle relative alle condizioni per valutare se il consenso sia stato o meno liberamente prestato».

[322] Sulle novità introdotte con d.lgs. n. 173 del 2021, DE CRISTOFARO, *Legislazione italiana e contratti dei consumatori nel 2022: l'anno della svolta. Verso un diritto "pubblico" dei (contratti dei) consumatori?*, in *Nuove leggi civ. comm.*, 2022,.,

[323] CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali,* cit

[324] C. IRTI, *Consenso "negoziato" e circolazione dei dati personali,* cit.

trattamento, che resta libera, con la fornitura del contenuto o del servizio: «se l'utente non acconsente alla raccolta e al trattamento dei suoi dati mediante *cookies* e *tracking tools* […] il fornitore non agisce in giudizio, ma il servizio non viene fornito»[325].

Pur senza affrontare questi peculiari profili ricostruttivi, anche la giurisprudenza della Cassazione, partendo dalle disposizioni nazionali anteriori alle modifiche apportate dal d.lgs. n. 101/2018, è giunta a riconoscere la distinzione fra il consenso prestato per la conclusione del contratto e quello, invece, dato, nel contratto, per il trattamento dei dati personali[326].

2.2. *Consenso al trattamento di dati sensibili*

Ai sensi dell'art. 9, par. 2, lett. *a*, del Regolamento, il consenso dell'interessato costituisce una delle ipotesi eccezionali, in presenza delle quali non si applica il divieto di trattamento dei dati personali appartenenti alle categorie particolari.

Qualora non ricorra almeno una delle altre fattispecie di deroga di cui all'art. 9, par. 2, del Regolamento, il consenso è necessario per poter trattare tali dati personali.

Il consenso al trattamento dei dati sensibili, trattandosi sempre del consenso dell'interessato, deve presentare tutte le caratteristiche richieste, in generale, per lo stesso[327], quindi dovrà essere una preventiva manifestazione di volontà libera, specifica, informata e inequivocabile.

Come già precisato, la disposizione richiede però, in questo caso, che il consenso sia anche *esplicito*. L'aggiunta di tale requisito è intesa per innalzare il livello di tutela, in favore della persona, considerato il rischio per i diritti e le libertà fondamentali dell'interessato insito nel trattamento di questi dati[328].

Il termine 'esplicito' è riferito alla modalità con cui l'interessato deve esprimere il suo consenso. Ciò comporta che la manifestazione di volontà debba tradursi in una dichiarazione esplicita di consenso, ma, come chiarito dal Comitato europeo per la protezione dei dati, non

---

[325] *Ivi*, 104. Cfr. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, cit..

[326] V. Cass., 2.7.2018, n. 17278, cit. Cfr. CAGGIA, *Cessione di dati personali per accedere al servizio digitale gratuito: il modello del "consenso rafforzato"*, in D'AURIA (a cura di), *op. cit*

[327] Cfr., nella giurisprudenza italiana riferibile ancora all'applicazione delle norme del Codice della privacy non modificate dal d.lgs. n. 101/2018, Cass., 21.10.2019, n. 26778, in *Dir. inf*., 2020, con nota di THOBANI, *Richieste preventive di consenso al trattamento dei dati: quando la cautela rischia di essere eccessiva*. V. anche il provvedimento dell'Autorità garante norvegese, del 24/01/2021, Datatilsynet, DT-20/02136, cit., 1.

[328] Nel procedimento per l'approvazione del testo del Regolamento non si è arrivati a estendere questo requisito ad ogni consenso, ma la soluzione di compromesso ha permesso di richiedere in ogni caso che la manifestazione di volontà sia sempre inequivocabile. ALBRECHT, *Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung. Überblick und Hintergründe zum finalen Textfür die Datenschutz-Grundverordnung derEU nach der Einigung im Trilog*, in *Computer und Recht*, 2016, vol. 32, n. 2.

deve necessariamente trattarsi di una dichiarazione resa per iscritto. Il requisito del consenso esplicito, infatti, può essere soddisfatto anche in altri modi, come ad esempio con la compilazione di un modulo elettronico, l'invio di un'e-mail, il caricamento di un documento scansionato con la propria firma o l'utilizzo di una firma elettronica. Può bastare anche una dichiarazione verbale, come avviene in una conversazione telefonica, con una conferma specifica, ma in questo modo, verosimilmente, risulterebbe assai gravosa la dimostrazione da parte del titolare del trattamento della sussistenza degli elementi per un valido consenso esplicito[329].

Prima dell'avvento del Regolamento gli Stati membri potevano legislativamente prevedere requisiti ulteriori che accompagnassero il consenso al trattamento di dati sensibili. Nell'ordinamento italiano, ad esempio, era prevista l'autorizzazione preventiva del Garante. Ora, invece, alla luce del nuovo quadro giuridico, non si ritiene che possa più ammettersi[330].

Va osservato poi che la lett. *a* dell'art. 9, par. 2, del Regolamento – pressoché in continuità con la corrispondente lett. *a* dell'art. 8, par. 2, della Direttiva madre – consente al diritto dell'Unione o degli Stati membri di escludere l'ammissibilità del consenso esplicito dell'interessato come fattispecie di deroga al divieto di cui al par. 1. Ciò è avvenuto, ad esempio, proprio con riferimento ai dati relativi alla salute, in Francia, laddove, all'art. 1111-18 del *Code de la santé publique*, si è vietato l'accesso al *dossier médical partagé*, al di fuori dei casi previsti agli artt. 1111-15 e 1111-16, anche in presenza del consenso dell'interessato stesso[331].

Tale possibilità è prevista nella considerazione della condizione di debolezza in cui può versare il soggetto interessato e per difenderlo dall'approfittamento che altri ne faccia. La sottrazione dei dati sensibili dal raggio d'azione della volontà del singolo funge da limite alla sua autodeterminazione, elevando una barriera anche contro il suo volere stesso. La norma pare quindi funzionare in un modo che somiglia, per certi versi, all'operare del divieto di atti di disposizione del proprio corpo, sancito all'art. 5 del Codice civile italiano, e ricorda quell'orizzonte di parallelismi fra autodeterminazione informativa e autodeterminazione sul

[329] European Data Protection Board, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, Versione 1.1*, cit.

[330] GRANIERI, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, cit.

[331] V. PEIGNÉ, *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, in *Riv. it. med. leg.*, 2011: «Il bilanciamento degli interessi, che permette di derogare al potere di riservare l'informazione quando la società vi ha interesse, deve anche poter andare nel senso di una limitazione al potere di divulgare. Il consenso della persona non può quindi essere una condizione sufficiente alla circolazione dei dati. Il divieto alla divulgazione è fondamentale per rendere l'autonomia della persona e quella del titolare del trattamento compatibile con il rispetto degli interessi individuali e collettivi che meritano tutela».

proprio corpo, in un *continuum* fra corpo materiale e corpo digitale[332].

Implicitamente essa riconosce e ammette un regime di indisponibilità dei dati sensibili, che accede a uno statuto pubblicistico o costituzionale, in cui la circolazione dei dati stessi è rimessa al controllo esclusivo di soggetti diversi dall'interessato.

Ragionare del consenso al trattamento di dati personali appartenenti alle categorie particolari permette, in ogni caso, di tornare sul dibattito circa la natura giuridica del consenso dell'interessato, per vagliarne gli assunti e fare qualche ulteriore precisazione.

La figura del consenso dell'avente diritto sembra calzare bene per il consenso al trattamento di dati sensibili[333]. In sua assenza – e in mancanza dei presupposti per l'applicazione di una delle altre deroghe al divieto – il trattamento è illecito e non perché mancante di una base giuridica che lo legittimi, ma perché posto in essere in violazione di un espresso divieto. Il consenso *ex* art. 9, par. 2, lett. *a*, scrimina una condotta vietata, antigiuridica.

Diversamente, il trattamento di dati neutri non è espressamente vietato e il consenso a tale trattamento non pare 'giustificare' una condotta altrimenti antigiuridica di per sé.

Il consenso al trattamento dei dati comuni, ai sensi dell'art. 6, costituisce base giuridica del trattamento, semplicemente, come presupposto di legittimazione. Si può dire, al più, che operi come autorizzazione, nel senso di dispositivo che rimuove un limite ai poteri e alle facoltà del soggetto – in questo caso il titolare del trattamento – posto a tutela della persona. Se oggetto del trattamento sono dati sensibili, invece, esso opera anche come causa di giustificazione, a giustificare appunto una condotta – almeno in astratto – riconducibile all'illecito. E infatti il consenso *ex* art. 9 – che, giova ripetere, può essere anche escluso dal diritto dell'Unione o degli Stati membri – va riferito esplicitamente ai dati sensibili trattati.

Vi può essere, quindi, il caso di trattamento di dati sensibili che avrebbe come base giuridica il consenso prestato dall'interessato, ma che sarebbe comunque illecito, in quanto posto in essere in violazione dell'art. 9. Si tratta dei casi in cui il consenso prestato integra gli estremi della base giuridica di cui all'art. 6, ma non quelli della eccezione al divieto di cui all'art. 9. Si pensi ad esempio al consenso prestato al trattamento, per una o più specifiche finalità, dei propri dati personali, in generale, ma non di quei dati sensibili, nello specifico, oppure al consenso che non possa dirsi 'esplicito', ai sensi della lett. *a*, dell'art. 9, par. 2, o

[332] RODOTÀ, *La persona*, cit. Cfr. P. PERLINGIERI, *Il "diritto privato europeo" tra riduzionismo economico e dignità della persona*, cit.

[333] Cfr. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. e impr.*, 2019

ancora del consenso esplicito, pur riferito ai dati sensibili, ma non ammesso dal diritto nazionale[334].

Occorre poi sgombrare il campo della riflessione da una questione che potrebbe sorgere pensando al consenso in relazione ai dati appartenenti alle categorie particolari, ossia se il dato sensibile possa entrare nel contratto, cioè se possa rientrare, ad esempio, fra i dati personali che il consumatore comunica al fornitore di contenuti o servizi digitali. Una risposta affermativa, che aprirebbe a una negoziabilità di pressoché tutte le categorie di dati personali senza distinzioni, richiede comunque che siano soddisfatte alcune condizioni. In primo luogo dovrà ritenersi ammissibile – e valido – un contratto in cui una delle prestazioni consista nel rilascio del consenso al trattamento di dati sensibili. Cosa non scontata e rimessa alla volontà del legislatore o alla prudenza dell'interprete[335]. In secondo luogo, dovrà essere soddisfatto tanto il requisito della deroga al divieto di trattamento di dati sensibili, *ex* art. 9 par. 2 del Regolamento, quanto quello della base giuridica per il trattamento stesso, ai sensi dell'art. 6 del Regolamento.

La duplice – o molteplice – direzione in cui pare muoversi dunque il consenso dell'interessato sembra rispecchiare quella 'doppia anima' che è propria del Regolamento generale sulla protezione dei dati. Una ambivalenza in cui i differenti aspetti convivono e si scambiano nell'avvicendarsi delle funzioni del dispositivo del consenso, due facce della stessa medaglia

---

[334] Nel momento in cui il soggetto presta il proprio consenso esplicito al trattamento di particolari categorie di dati, quel consenso, integrando i requisiti tanto dell'art. 6 quanto dell'art. 9, vale sia a far caducare il divieto *ex* art. 9 che a soddisfare le condizioni di liceità *ex* art. 6. I due piani, però, restano distinti. Infatti, possono aversi casi in cui l'operazione di trattamento sia scriminata, ai sensi dell'art. 9, ma sia comunque illecita poiché priva di una base giuridica ai sensi dell'art. 6. Si fa rinvio a quanto già evidenziato precedentemente.

[335] In Francia è vietato trasferire a titolo oneroso dati sanitari, a prescindere dal consenso dell'interessato. V. l'art. 1111-8, VII, del *Code de la santé publique*. Si osserva, peraltro, come ai sensi dell'art. 3, par. 5, lett. *c*, della Direttiva n. 770 del 2019, la stessa non si applichi ai contratti concernenti «servizi sanitari, ai sensi dell'articolo 3, lettera a), della direttiva 2011/24/UE», e di conseguenza si applichi invece ad altri tipi di contratti laddove il contenuto o servizio digitale non rientri nell'ambito dell'assistenza sanitaria, senza però che sia specificato il contenuto dei dati personali. V. il considerando 29 della Direttiva n. 770 del 2019: «La presente direttiva non dovrebbe applicarsi all'assistenza sanitaria, come definita nella direttiva 2011/24/UE del Parlamento europeo e del Consiglio. L'esclusione dell'assistenza sanitaria dall'ambito di applicazione della presente direttiva dovrebbe applicarsi anche ai contenuti digitali o servizi digitali che costituiscono un dispositivo medico, quale definito nelle direttive 93/42/CEE e 90/385/CEE del Consiglio e dalla direttiva 98/79/CE del Parlamento europeo e del Consiglio, laddove il dispositivo medico in questione sia prescritto o fornito da un professionista sanitario ai sensi della direttiva 2011/24/UE. La presente direttiva dovrebbe tuttavia applicarsi a qualsiasi contenuto digitale o servizio digitale che costituisce un dispositivo medico, come le applicazioni sanitarie, e che può essere ottenuto dal consumatore senza che sia prescritto o fornito da un professionista sanitario». Cfr. LUCARELLI TONINI, *op. cit.*

2.3 Consenso al trattamento di dati relativi alla salute

Esseno i dti relativi alla salute una delle categorie particolari di dati personali il cui trattamento è vietato ai sensi dell'art. 9, par. 1, del Regolamento, il consenso esplicito dell'interessato al trattamento dei suoi dati sanitari rientra nelle fattispecie di deroga del divieto, cioè in quella di cui all'art. 9, par. 2, lett. *a*.

Le considerazioni svolte generalmente con riguardo al consenso del trattamento di dati sensibili valgono quindi anche, nello specifico, per il consenso al trattamento di dati relativi alla salute.

Come per il consenso al trattamento sanitario, anche il consenso al trattamento di dati relativi alla salute può considerarsi una causa di giustificazione, per di più non essendo le operazioni di trattamento di questi dati connotate in astratto da alcun carattere positivo.

Ma, al di là dell'inquadramento giuridico sistematico dell'istituto[336], va tenuto presente soprattutto che il consenso, in generale, rappresenta lo strumento principale con cui si realizza l'autonomia della persona[337].

Un discorso a sé merita il tema del consenso al trattamento dei dati relativi alla salute per finalità di ricerca.

L'esigenza di avvalersi delle informazioni di carattere sanitario, connaturata alla ricerca in ambito medico e non solo, è apparsa da sempre confliggente con la diversa esigenza di garantire ai soggetti cui le informazioni si riferiscono la riservatezza e la protezione dei dati personali, nella misura in cui le varie normative in materia di privacy hanno richiesto, con rigore, la previa acquisizione del consenso degli interessati.

Si è visto che il Regolamento offre una soluzione alla problematica – strettamente connessa all'uso secondario dei dati personali – attraverso varie sue disposizioni, come l'art. 5, lett. *b* ed *e*, l'art. 9, par. 2, lett. *j*, e l'art. 89.

Si deve aggiungere invece che, proprio in questo ambito, si è ragionato del consenso cercando di intenderlo in vario modo, osservandolo attraverso un prisma di possibili strutture e declinandolo tenendo a mente lo scopo che avrebbe avuto di mira la specifica normativa,

[336] Il consenso «assume un ruolo diverso in ciascuna delle attività con cui si realizza il trattamento dei dati». BILOTTA, *L'emersione del diritto alla privacy*

[337] BATTELLI, *Questioni di fine vita e consenso informato*, in SINISI e POSTERARO (a cura di), *Questioni di fine vita. Atti del convegno tenutosi a Roma Tre il 29 aprile 2019*, RomaTrepress, 2020: «Il consenso informato, quindi, ed è questo, dal punto del civilista, il cuore della questione, lungi dal rilevare solo come problema di tecnica giuridica e di collocazione dogmatica (presupposto di liceità, causa di esclusione della tipicità, causa di giustificazione) costituisce espressione primaria della tutela dell'autonomia privata».

anche con riferimento alle caratteristiche peculiari delle biobanche di ricerca[338].

Per distinguere i numerosi modi di concepirlo, lo si è accompagnato con altrettanti aggettivi: *presumed*[339], *blanket*[340], *open*[341], *broad*[342], *multi-layered*[343], *dynamic*[344].

Gli sforzi creativi attorno alla figura del consenso hanno cercato di contemperare le esigenze della ricerca – in ambito biomedico – con quelle della protezione dei dati personali e della riservatezza degli interessati, nel tentativo di superare gli stretti confini di un consenso specifico per ogni sviluppo delle ricerche scientifiche pur sempre garantendo la tutela dei diritti e delle libertà fondamentali della persona.

La finalità di ricerca presenta chiaramente il legame con l'interesse pubblico: da un trattamento di dati a questi fini la collettività può trarre numerosi vantaggi e benefici. La soddisfazione di un interesse pubblico può aversi però anche con il trattamento di dati sanitari per altri scopi, non sempre precisamente determinabili in via normativa a priori.

«Il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato». Con questo esordio, il considerando 54 del Regolamento porta subito all'attenzione l'eventualità di un trattamento di dati sensibili necessario in ambito sanitario, che possa pertanto prescindere dal consenso dell'interessato. Per i settori della sanità pubblica, a venire in gioco tra le varie categorie particolari di dati personali sono soprattutto, e com'è ovvio, i

[338] Tenendo sempre a mente che il consenso prestato a partecipare alla ricerca dev'essere tenuto distinto dal consenso inteso come fondamento legittimo per il trattamento dei dati personali. BERNES, *La protezione dei dati personali nell'attività di ricerca scientifica*

[339] Il riferimento emblematico è al progetto della società deCODE, che fu accolto dal Parlamento islandese con l'approvazione dell'Act on a Health Sector Database, con cui furono autorizzate la raccolta e l'elaborazione di dati sanitari e genetici anonimizzati dell'intera popolazione islandese. Nell'atto non si prevedeva il dovere di richiedere il consenso dei soggetti al trasferimento di dati dai registri delle amministrazioni sanitarie al nuovo database, il consenso si presumeva.

[340]Un consenso come adesione alla finalità di ricerca scientifica in generale, senza specificazione dei progetti. «Si tratta, quindi, di un consenso alla ricerca, intesa in senso omnicomprensivo, esclusivo della possibilità di esercitare un futuro controllo sulle proprie informazioni». TOMASI, Genetica e Costituzione. Esercizi di eguaglianza, solidarietà e responsabilità, cit

[341] Consenso alla ricerca, ma nella consapevolezza di non poter essere letteralmente 'informato'. Il soggetto acconsente a un utilizzo generale dei propri dati, ammettendo e accettando l'«inattuabilità di un processo informativo contenutisticamente qualificato». Ivi.

[342] Un consenso ampio, anche per impieghi futuri, ma accompagnato da meccanismi differenti che offrano tutele specifiche, come ad esempio una verifica preventiva delle caratteristiche della ricerca da parte di comitati etici o la predisposizione di idonee garanzie di anonimizzazione di dati e campioni. Ivi. Trattasi, peraltro, di un modello di consenso spesso ritenuto il frutto di un buon bilanciamento fra le contrapposte esigenze.

[343] Consenso a varie opzioni, che prevede la possibilità di scegliere a quale impiego dei propri dati personali acconsentire, con riguardo agli obiettivi perseguibili dalla ricerca condotta con essi. TOMASI, Genetica e Costituzione. Esercizi di eguaglianza, solidarietà e responsabilità, cit.

[344] Consenso esprimibile più volte nel tempo a più utilizzi, di cui gli interessati vengano resi edotti, implicando una comunicazione e un'interazione continua fra gli stessi e chi si occupa della ricerca. Ivi.

dati relativi alla salute[345].

Come già si è cercato di mettere in luce, il trattamento di dati sanitari può, quindi, avvenire anche senza il consenso della persona, in presenza di una delle altre fattispecie di deroga al divieto di trattamento, ai sensi dell'art. 9 del Regolamento. Beninteso, in mancanza di queste, il consenso resta necessario e il trattamento che venga posto in essere in sua assenza si configura come illecito.

Il trattamento necessario per motivi di interesse pubblico nei settori della sanità pubblica, che prescinde quindi dal consenso dell'interessato – aggiunge il considerando 54 –«dovrebbe essere soggetto a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche». La prospettiva del Regolamento, nella consapevolezza della problematicità e dei rischi propri di questo tipo di trattamento, apre all'individuazione di strumenti appositi – diversi dal consenso – per la difesa della persona e dei suoi diritti fondamentali.

È opportuno ribadire che il par. 4 dell'art. 9, proprio in relazione al trattamento di dati relativi alla salute, concede agli Stati membri un margine di discrezionalità ragguardevole, consentendo che questi mantengano o introducano ulteriori condizioni, comprese limitazioni. Il Regolamento, dunque, nell'ammettere la possibilità che il trattamento di dati sanitari venga condizionato o limitato dagli ordinamenti nazionali, sembra non escludere che il diritto interno lo possa subordinare al ricorrere di altri requisiti, tra cui potrebbe esservi il consenso. In tal caso, la natura di questo consenso sarebbe ancora una volta da riconsiderare, a seconda di come la normativa nazionale disciplinasse la manifestazione di volontà[346].

Del resto, se in relazione al trattamento di dati sanitari proprio il consenso è stato considerato strumento privilegiato di tutela della persona, è perché nel consenso si è ritrovata l'espressione dell'autonomia della persona, la norma che recepisce il diritto all'autodeterminazione informativa e che può, almeno astrattamente, tenere conto della particolare delicatezza delle informazioni in questione. Occorre peraltro chiedersi come possa

[345] Distinguendo fra *privacy* e *data protection*, MCCLELLAND e HARPER, *Information Privacy in Healthcare — The Vital Role of Informed Consent*, in *European Journal of Health Law*, in *brill.com*, 27 ottobre 2022, evidenziano come, se per la disciplina della protezione dei dati personali si ammette tranquillamente la possibilità di un trattamento di dati sanitari a prescindere dal consenso dell'interessato, al ricorrere di determinati presupposti, in relazione alla *privacy* – almeno nel *common law* – continui ad essere fondamentale il consenso della persona.

[346] Nell'ordinamento italiano, per quanto riguarda nello specifico il trattamento di dati genetici, è demandata al Garante per la protezione dei dati personali, *ex* art. 2 *septies*, comma 6°, del Codice della privacy, la possibilità, con le misure di garanzia, di individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato, a norma dell'art. 9, par. 4, del Regolamento, o altre cautele specifiche.

tradursi la regola del consenso, in termini applicativi, per difendere effettivamente la personalità dell'individuo, proprio con riguardo alle condizioni di salute del soggetto.

Sul consenso al trattamento di dati relativi alla salute, particolarmente incisive furono le osservazioni svolte dal Gruppo di lavoro "Articolo 29", nel documento del 2007, sulle cartelle cliniche elettroniche. Attesa l'esigenza di assicurare ai pazienti la protezione dei dati, il diritto alla riservatezza e il rispetto dei loro diritti fondamentali e allo stesso tempo di favorire lo sviluppo delle tecnologie informatiche per una maggiore efficienza in ambito sanitario – com'è, appunto, per le cartelle cliniche elettroniche –, si rende necessario riconoscere le adeguate garanzie in un quadro giuridico unitario e completo[347].

Anche se un sistema di cartelle cliniche elettroniche non è interamente fondato sul consenso come base giuridica – ma lo stesso può dirsi per una banca dati che raccolga informazioni sulla sua salute, per più finalità – «la decisione del paziente sul come e il quando usare i suoi dati deve rivestire un ruolo fondamentale come garanzia importante». Quindi il Gruppo di lavoro, al consenso come base giuridica del trattamento, cioè il consenso che deve rispettare i requisiti propri delle condizioni di liceità e della rispettiva fattispecie di deroga al divieto di trattamento, affianca il consenso inteso nel senso di *accettazione*. «L'accettazione come garanzia non deve necessariamente essere data in forma esplicita e preventiva (*opt-in*): la possibilità di autodeterminazione potrebbe – in funzione della situazione – anche essere conferita sotto la forma di un diritto al rifiuto (*opt-out*)».

La riflessione prosegue diversificando i dati relativi alla salute in base al diverso "potenziale di arrecare pregiudizio"[348], e, in ragione di ciò, concludendo con l'opportunità di distinguere le «categorie di utilizzo con vari gradi di possibilità d'esercizio dell'autodeterminazione». In tal senso, per i dati "meno riservati" si potrebbe adottare lo schema dell'*opt-out*, mentre a quelli potenzialmente più pregiudizievolisarebbe da riservare il meccanismo dell'*opt-in.*

Questo passaggio, in particolare, merita attenzione. Del diverso gradiente di sensibilità dei dati relativi alla salute si è già detto. Di come da questa constatazione discenda anche un diverso modo di concepire la regola del consenso è bene dire ora[349], tenendo a mente che si guarda al consenso – o forse, meglio, alla volontà – come dispositivo in grado di esprimere

[347] Per questa e le considerazioni a seguire, si v. Gruppo Articolo 29, *Documento di lavoro sul trattamento di dati personali relativi alla salute nelle cartelle cliniche elettroniche (EHR)*, cit., 13 s.

[348] Sul punto si rinvia a quanto osservato in relazione alla sensibilità del dato relativo alla salute

[349] Il Gruppo di lavoro esemplificava, per questa categoria, riferendosi ai dati psichiatrici o ai dati su un aborto.

l'autodeterminazione della persona[350].

Già da tempo si sono immaginati «diversi "gradi" di riservatezza» per le informazioni di carattere sanitario. Gli approdi di allora possono opportunamente essere contestualizzati nell'orizzonte normativo di oggi, in cui la privacy del singolo deve bilanciarsi con i diritti, non necessariamente di natura economica, di altri soggetti e con gli interessi della collettività alla circolazione dei dati personali.

Accantonando il meccanismo dell'*opt-in*, cioè del consenso esplicito preventivo, per il trattamento di dati relativi alla salute, in osservanza dell'elenco stesso di eccezioni al divieto, potrebbe ancora avere senso parlare di consenso in termini di *opt-out*. Lo schema dell'*opt-out*, cioè della volontà come dissenso, potrebbe riservarsi al trattamento dei dati più sensibili fra i dati sanitari, garantendo al contempo l'autodeterminazione della persona, l'*empowerment* del paziente, e – a contrario – una più libera circolazione dei dati sulla salute, che non presentino un profilo di più elevata sensibilità.

Secondo il Gruppo di lavoro, infine, «nessuno può essere costretto a far parte dei sistemi» di cartelle cliniche elettroniche. Pertanto le normative che li disciplinano dovrebbero anche regolare l'eventualità di un completo ritiro da detti sistemi, precisando se da ciò derivi l'obbligo di cancellare del tutto i dati dal sistema o semplicemente di impedirne l'accesso e permettendo all'interessato di scegliere[351].

Anche in relazione a un sistema di cartelle cliniche elettroniche nel suo complesso si potrebbe pensare alla rimodulazione del consenso, corrispondentemente al livello di sensibilità dei dati sanitari da trattare.

Con riguardo alla condizione di sieropositività all'HIV, la Corte europea dei diritti dell'uomo, nella menzionata sentenza *Z. c. Finlandia*, affermò che qualsiasi misura statale che imponesse la comunicazione o la divulgazione di tali informazioni senza il consenso del paziente richiedeva la maggiore attenzione, così come le salvaguardie volte a garantire una protezione effettiva, in considerazione della natura estremamente intima e sensibile di tali dati[352].

---

[350] In un documento di quattro anni successivo, l'*advice paper* sulle particolari categorie di dati, del 2011, il Gruppo di lavoro annoverava fra i dati specialmente sensibili quelli su particolari patologie o disabilità, distinguendoli dai dati meno sensibili come quelli relativi a un 'semplice' raffreddore. «*This leads to difficulties in practice, as the individual's consent is required even for unproblematic processing of such data*». Gruppo Articolo 29, *Advice paper on special categories of data ("sensitive data")*, cit

[351] Cfr. ZATTI, *Il diritto all'identità e l'«applicazione diretta» dell'art. 2 Cost.*, cit.

[352] Oltre a ciò, il Gruppo di lavoro aggiungeva che «in linea di principio un paziente dovrebbe sempre avere la possibilità, se lo desidera, di impedire la comunicazione dei suoi dati medici, raccolti da un operatore sanitario durante la cura, ad altri operatori sanitari».

Questi rilievi, anche per la specificità delle disposizioni che potrebbero richiedere, non si traducono in norme nel tessuto del Regolamento, che resta appunto generale, ma possono ben valere per il legislatore nazionale.

L'avvicendarsi di tutte queste riflessioni attorno al consenso, spesso frutto di incontro fra ambiti di studio differenti, e il modo in cui al consenso si è guardato e si continua a guardare sembrano confermare l'importanza del ruolo che può assumere, nella veste più diversa, a difesa dell'individuo e della personalità.

Il consenso in generale, non necessariamente consenso come base giuridica che legittima il trattamento di dati personali o scrimina il trattamento di dati sensibili. Consenso – assenso o dissenso – e basta. O, forse, solo volontà.

3. *Ascesa e declino del "mito del consenso".*

Riconoscere le mitologie giuridiche, andare oltre e «liberarsi delle ombre gigantesche abilmente create da una straordinaria lanterna magica»[353]. Riconoscere negli istituti giuridici, come diceva Paolo Grossi, i tratti mitologici, le enfasi sproporzionate, gli ingigantimenti leggendari, per smascherare il vero volto delle regole, ciò che possono e non possono fare realmente. Riconoscere, allo stesso modo, nel consenso dell'interessato come base giuridica del trattamento di dati personali un istituto carico di aspettative, celebrato dalla teoria, ma in concreto sempre più limitato: la storia dell'ennesima mitologia.

Oggi, con una maggiore distanza temporale da quella prima direttiva sulla privacy e dall'entusiasmo che accoglieva le nuove norme e con la maturità degli studi in materia, ci si può accostare alla disciplina sulla protezione dei dati personali con questa chiave di lettura.

La tutela della persona è stata affidata, in origine, al consenso dell'interessato. Il consenso era visto come lo strumento per mezzo del quale il soggetto poteva esercitare un controllo sulla circolazione delle informazioni che lo riguardavano, nel suo duplice senso: in positivo, quando prestato, legittimando il trattamento dei dati personali e permettendo al titolare del trattamento di svolgere le relative operazioni; e in negativo, quando non prestato, rendendo illecito il trattamento che fosse comunque avvenuto e che non trovasse altra base giuridica e quindi attivando il meccanismo sanzionatorio.

La Direttiva n. 46 del 1995, che contemplava il consenso dell'interessato quale base giuridica del trattamento di dati personali al menzionato art. 7, lett. *a*, lasciava agli Stati membri il consueto margine di discrezionalità nell'attuare anche questa previsione, come

[353] GROSSI, *Mitologie giuridiche della modernità*, 3a ed., Milano, Giuffrè, 2007.

disposto all'art. 5[354].

La scelta del legislatore italiano fu quella di attribuire al consenso una funzione di perno della disciplina della protezione dei dati personali[355], attorno al quale far ruotare l'esercizio dei diritti dell'interessato. Così la l. 675/1996 apriva, del Capo III, la Sezione II, "Diritti dell'interessato nel trattamento dei dati", sancendo, all'art. 11, comma 1°, che «il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dall'interessato»[356] e facendo seguire, all'art. 12, i "casi di esclusione del consenso"[357].

Il consenso era inteso come presupposto generale del trattamento dei dati personali, essendo finalità della legge garantire che il trattamento «si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale»[358].

La struttura più articolata del Codice della privacy recepiva poi la regola mitigandone la portata, ma senza abbandonare del tutto l'impianto consensocentrico che aveva caratterizzato la legge del '96, senza smentire quindi l'ascesa del consenso a principio del trattamento dei dati personali[359].

Ciò non significa che già allora non vi fossero eccezioni che permettevano il trattamento a prescindere dal consenso, ma piuttosto che il modo di concepire la protezione dei dati personali passava inevitabilmente attraverso una speciale considerazione del consenso dell'interessato, tanto come espressione del diritto di autodeterminazione quanto come condizione di liceità del trattamento stesso. E ciò valeva in misura particolare, come

---

[354] Art. 5 della Direttiva n. 46/1995: «Gli Stati membri precisano, nei limiti delle disposizioni del presente capo, le condizioni alle quali i trattamenti di dati personali sono leciti».

[355] SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, cit., 626.

[356] È definito «uno dei principi fondamentali della normativa sui dati personali» da PATTI, *Il consenso dell'interessato al trattamento dei dati personali,* cit.

[357] Peraltro, l'impianto della legge includeva la tutela penale. Così, ai sensi dell'art. 35, comma 1°, era previsto che «salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 11, 20 e 27, è punito con la reclusione sino a due anni o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da tre mesi a due anni».

[358] Così l'art. 1, comma 1°, l. n. 675/1996. Come scrive PUTIGNANI, *Consenso e disposizione della privacy*, cit., 231, «nella prospettiva della legge n. 675 del 1996 la protezione della persona nei riguardi del potere informatico è realizzata articolando una disciplina del trattamento dei dati, la cui finalità è espressa all'art. 1 ("rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche") e il cui presupposto è il consenso del titolare del dato».

[359] Si parlava allora di *rivincita del dogma del consenso*. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica,* cit.

anticipato, per il trattamento di dati sensibili[360].

Il panorama è mutato con l'entrata in vigore del Regolamento generale sulla protezione dei dati e il conseguente intervento normativo sul Codice della privacy, ad opera del d.lgs. n. 101 del 2018.

Va detto, però, che da tempo, o forse addirittura sin dagli albori della riflessione in tema di protezione dei dati personali, si è colta l'inconsistenza del consenso dell'interessato al trattamento come dispositivo di controllo nella circolazione dei dati. Un'inconferenza a più livelli, gradata, per così dire, se parametrata alle condizioni normali di un individuo, un utente medio dei servizi digitali[361].

È stato messo in luce, infatti, come il più delle volte il consenso sia prestato senza nessuna consapevolezza, con disattenzione[362]. La possibilità o la necessità di accedere rapidamente a un servizio e la configurazione dello stesso ambiente digitale, alla portata di tutti, in qualsiasi luogo e in qualsiasi momento, su un computer, uno smartphone, un tablet, influenzano i soggetti inibendo la considerazione che possono avere – per quanto minima sia – del valore della privacy e dello stretto legame con il trattamento dei loro dati personali[363].

E quando l'interessato cerchi invece di comprendere ciò cui sta acconsentendo, spesso non è in grado di capirlo. La complicatezza delle operazioni di trattamento, condizionata dalla complessità tecnologica degli strumenti stessi, mina l'intelligibilità dell'attività che con esso si compie e delle procedure messe in atto, la quale spesso può richiedere conoscenze

---

[360] «Deve osservarsi che il sistema di protezione dei dati sensibili contenuto nel D.Lgs. n. 196 del 2003 si fonda sul principio generale della necessità del consenso espresso dell'interessato al trattamento di tali dati, in quanto dotati di uno rigoroso statuto normativo di garanzia della riservatezza, derogabile soltanto nelle ipotesi espressamente previste nella stessa legge o mediante diretta previsione normativa o mediante rinvio al potere conformativo-autorizzatorio del Garante». Cass., sez. un., 27.12.2017, n. 30984, cit., punto 8.

[361] Come afferma SIRGIOVANNI, *op. cit.*, 1010, «Tutti noi che utilizziamo i servizi informatici attraverso *smartphone*, *tablet* o i "tradizionali" computer abbiamo acquisito consapevolezza della vacuità del consenso al trattamento dei dati personali, consenso che si atteggia a mero *flautus vocis*».

[362] Cfr. AULINO, *Consenso al trattamento dei dati e carenza di consapevolezza: il* legal design *come un rimedio* ex ante, in *Dir. inf*., 2020..

[363] Riferendosi agli aspetti particolari legati all'uso delle app per la salute, sono le riflessioni del Comitato nazionale per la bioetica, *"Mobile-health" e applicazioni per la salute: aspetti bioetici*, 28 maggio 2015, in *www.bioetica.governo.it*, al punto 5.3. «Le informazioni digitali sono tante, scritte con caratteri piccoli da visualizzare su smartphones […]. Già è stata sollevata la preoccupazione che il consenso informato visualizzato sullo schermo e non su carta, porti a cliccare in modo immediato senza il tempo sufficiente per una scelta consapevole e senza la possibilità di accertare la effettiva volontarietà. Inoltre la moltiplicazione dei consensi può portare ad una irritazione da parte dell'utente o spesso ad acconsentire solo per velocizzare la procedura, senza - anche qui - adeguata consapevolezza. In questo senso si svuoterebbe il significato del consenso informato. Questa necessità di informare gli utenti e di ricevere il loro consenso diventa ancor più complessa nel momento in cui le app vengono utilizzate da minori, come avviene con grande frequenza, sia mediche che non mediche».

tecniche che non sono in possesso dell'uomo medio e forse nemmeno appartengono alla cultura oggi condivisa nella società. Talvolta è l'informazione che chi opera il trattamento offre all'interessato ad essere minata da questa complessità, e di conseguenza ostacola la comprensione del trattamento per cui è richiesto il consenso, talaltra è anche solo il modo in cui l'informazione è resa che impedisce di comprendere[364].

E, ancora, qualora tale consapevolezza vi sia, la scelta viene ad essere vincolata, pena la non erogazione del servizio correlato al trattamento. Così può essere che l'interessato abbia contezza delle operazioni di trattamento dei suoi dati personali, in relazione a cui è richiesto di prestare il consenso, e dei rischi connessi, per la sua riservatezza e non solo, e ciononostante acconsenta, per mancanza di alternative o per il bisogno di quel bene o di quel servizio[365].

Da questo scorcio, si può notare anche una posizione di debolezza del soggetto, dinnanzi al titolare del trattamento, dinanzi all'operatore, all'erogatore di servizi, alla piattaforma. In questi termini, la controparte 'forte' di tale relazione asimmetrica potrebbe addirittura preferire il consenso, come base giuridica del trattamento: essendo un consenso, in pratica, obbligato, dunque facile da ottenere, e che, a differenza delle altre basi giuridiche normativamente previste, non necessita del soddisfacimento di ulteriori requisiti, può essere il modo più conveniente per superare il vaglio di liceità del trattamento.

Del consenso si è parlato allora in termini di 'paradosso'[366]. Le riflessioni comprese nell'ampia espressione "*privacy paradox*" raccolgono queste osservazioni[367] ed evidenziano come il consenso dell'interessato, pensato come strumento di tutela della persona e manifestazione dell'autodeterminazione informativa, possa rivelarsi l'esatto opposto, quando al consenso prestato non corrisponda una reale volontà piena o addirittura nessuna volontà e quando si traduca in un *escamotage* per aggirare la necessità di legittimazione del trattamento[368].

Tutto ciò assume tratti forse anche più marcati nel contesto sanitario, se si considera che non può aversi trattamento sanitario in assenza di trattamento di dati relativi alla salute del

---

[364] Cfr. *ibidem*: «le app più scaricate dagli utenti […] chiedono l'accesso a una gran quantità di dati, senza ancora spiegare adeguatamente per quali scopi queste informazioni sarebbero usate e sugli eventuali dati personali che verranno raccolti e sul loro uso».

[365] «A volte manca la reale alternativa del dissenso o del cambiamento della scelta». *Ibidem*.

[366] A.M. GAROFALO, *Regolare l'irregolabile: il consenso al trattamento dei dati nel GDPR*, cit.,

[367] Cfr. SOLOVE, *Introduction: privacy self-management and the consent dilemma*, in *Harvard Law Review*, 2013, 1880 ss. *Privacy paradox* è appunto un'espressione ampia perché con essa ci si riferisce a un insieme di nozioni e di considerazioni.

[368] A.M. GAROFALO, *Regolare l'irregolabile: il consenso al trattamento dei dati nel GDPR*, cit.

paziente, da parte del medico[369].

Quello del consenso, dunque – per usare le parole di Stefano Rodotà – è un mito[370] o una parvenza di tutela, quantomeno lo è il consenso inteso nel senso di base giuridica per la legittimità del trattamento dei dati personali. E la mitologia ha preso forma attraverso una retorica del consenso, che, forse semplicisticamente, credeva di risolvere la problematica sottesa al diritto alla privacy e alla protezione dei dati personali, al bilanciamento con altri diritti, indirizzando la soluzione all'individuo, inteso come singolo che può e deve decidere sulle questioni che lo riguardano[371].

Se è vero che il consenso è stato il principio che informava quella prima disciplina della protezione dei dati personali, è vero anche che oggi esso non ha più questo ruolo. La disciplina contenuta nel reg. Ue n. 679 del 2016, infatti – come già sottolineato – lo colloca fra le varie ipotesi delle condizioni di liceità del trattamento e tra le molteplici fattispecie di deroga al divieto di trattamento di dati appartenenti alle particolari categorie.

Ma l'impatto della nuova disciplina nell'ordinamento italiano non è dovuto tanto a una novità nel contenuto delle disposizioni, quanto ai diversi effetti propri dell'atto normativo scelto dal legislatore eurounitario, cioè il Regolamento e non più la Direttiva. Resa direttamente applicabile la norma del diritto dell'Unione e tolta di mezzo – seppur solo in parte – l'intermediazione del legislatore nazionale, l'impostazione consensocentrica della protezione dei dati personali, propria dell'ordinamento italiano, viene sostituita dall'articolata trama delle basi giuridiche del trattamento e delle eccezioni al divieto[372].

Il cambio di rotta si muove nella direzione più favorevole per lo sviluppo del mercato dei

---

[369] FINOCCHIARO, *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, cit

[370] RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit. ALPA, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit.*, *sub* art. 1, d.lgs. 30 giugno 2003, n. 196: «è dunque fallace rimettere il controllo al semplice *consenso* dell'individuo alla raccolta dei dati che lo riguardano. Questa è un'altra regola che Rodotà enuncia nel suo programma di intervento legislativo, ma è ben consapevole del fatto che il consenso non basta: perché una volta acquisito, il consenso non può più inseguire il modo in cui le informazioni sono catalogate, organizzate, manipolate, conservate e messe in circolazione. Al consenso occorre affiancare il controllo: di qui, per l'appunto il titolo del libro che parla di elaboratori e di *controllo sociale*».

[371] BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione. Commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale*, cit, reputava già che la necessità dell'autorizzazione del Garante segnasse la caduta del "mito del consenso", che parte della dottrina aveva esaltato oltre misura.

[372] V. il considerando 13 del Regolamento: «Per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali». Per GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, cit: «Occorre dunque arrendersi all'idea che nell'approccio normativo corrente il fondamento della legittimazione del titolare a trattare dati non è il consenso dell'interessato, che è se mai solo un limite (e neppure sempre), ma appunto la libertà di circolazione dei dati e in generale il principio capitalistico sotteso al mercato».

dati, orientando l'assetto normativo verso la circolazione dei dati personali. L'assestamento del diritto, dunque, non solo non è in contrasto, ma anzi è in adesione a un fenomeno – la circolazione delle informazioni – che, a ben vedere, non è mai stato possibile impedire e nemmeno seriamente ostacolare[373]. Il riposizionamento sistematico del consenso appare allora come un sintomo della presa di coscienza dell'ineluttabilità di tale fenomeno[374] e, conseguentemente, della convenienza di trarne vantaggio.

Presa di coscienza, altresì, della labilità del consenso dell'interessato come strumento che possa consentire effettivamente di esercitare un controllo sui propri dati personali e come regola in grado di rispondere alle nuove esigenze dello sviluppo tecnologico[375]. Una presa di coscienza della crisi di un modello[376], che ha portato ad elaborare altre soluzioni, spostando il baricentro della protezione dei dati dalla manifestazione di volontà del soggetto verso altri istituti, altre figure, altre strutture giuridiche, forse nuove o forse estranee al diritto privato[377].

Dalla primazia dell'autodeterminazione informativa a un orizzonte di *eterodeterminazione informativa*[378].

Emblematica manifestazione di questo passaggio nel modo di intendere il consenso, è stata la decisione di rendere automatica l'alimentazione del fascicolo sanitario elettronico[379],

---

[373] «L'esigenza principale a cui è indirizzata la disciplina del reg. UE 2016/679 è la circolazione dei dati ed essa è realizzata dettando regole di tutela della persona, volte cioè a fare in modo che quel fenomeno circolatorio, necessario e perciò inevitabile, non si spinga oltre il limite della dignità della persona». SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, cit.

[374] SIRGIOVANNI, *op. cit*.

[375] Cfr. MAESTRI, *Il feticcio della privacy nella sanità. Cura del paziente e biobanking genetico prima e dopo l'entrata in vigore del GDPR*, cit.

[376] THOBANI, *I requisiti del consenso al trattamento dei dati personali*, cit.

[377] «La procedimentalizzazione formale dell'analisi del rischio, la regolamentazione in linea con la più ampia tendenza delle normative moderne incentrate sul *risk management*, rappresentano un messaggio chiaro del legislatore agli operatori. Un messaggio che, come nelle precedenti evoluzioni del quadro normativo in materia di tutela dei dati, ha origine nella crisi del modello anteriore. Il modello del consenso informato, dell'autovalutazione ad opera dell'interessato è infatti definitivamente entrato in crisi sul finire del passato millennio (ma [v.] già Rodotà, [*Elaboratori elettronici e controllo sociale*]), quando lo sviluppo del *cloud computing*, l'emergere dei moderni strumenti di *data analytics* e, da ultimo, la nuova stagione dell'intelligenza artificiale […] hanno delineato uno scenario in cui l'interessato, in molti casi, non è più in grado di operare una consapevole valutazione del rischio […]. Da qui il ritorno alla valorizzazione di un'analisi preventiva ad opera di chi tratta i dati (art. 35) ed una nuova enfasi, in tale contesto, sul ruolo di supervisione delle autorità di controllo (art. 36). Tali nuove tecnologie hanno poi anche segnato il concretizzarsi di forme diverse di atteggiarsi del rischio, non più solo rilevante a livello individuale, ma tale da assumere anche una connotazione collettiva […], nonché sempre più legato alle conseguenze *lato sensu* discriminatorie dell'impiego dei dati con fini analitico-predittivi […]».

[378] S. CORSO, *Sanità digitale e riservatezza. Interpretazioni sul fascicolo sanitario elettronico*, cit.

[379] Scelta fatta anche sulla base di quanto espresso dal Garante per la protezione dei dati personali. «La perdita della centralità del consenso e la sua portata, ormai residuale, tra le basi giuridiche di liceità del trattamento, anche per quanto attiene al trattamento dei dati relativi alla salute, ha trovato, da ultimo, conferma nel Provvedimento dell'Autorità garante del 7 marzo 2019. Con tale pronuncia è stata ribaltata l'impostazione "consenso-centrica" del passato». ESCUROLLE, *Le novità sul Fascicolo Sanitario Elettronico (FSE)*, in *Ciberspazio e diritto*, 2020.

cioè l'inserimento in esso dei referti, dei documenti sanitari, inclusi i dati relativi alla salute del paziente, che consiste nel caricamento *online*.

Nella disciplina sulla protezione dei dati, però, il consenso non si riduce a consenso come base giuridica soltanto, che pure ha natura variegata, ma assume più sfaccettature, più funzioni e più modi di operare, anche in relazione ai diritti dell'interessato.

Si è osservato che il consenso può presentarsi nella duplice veste di consenso espresso e di non opposizione. Da questa prospettiva si può cogliere come anche l'opposizione – intesa in senso lato – si riconduca alla fenomenologia del consenso.

Passando ad esaminare però le forme in cui il Regolamento ha convogliato questo modo di intendere il consenso e le sue logiche conseguenze, si può riscontrare ancora la subordinazione della volontà del soggetto a esigenze estranee o superindividuali alla circolazione – o meglio al trattamento – dei dati personali.

Se ne ha conferma analizzando l'istituto della cancellazione.

Garantire al soggetto il diritto di cancellare i suoi dati personali, o con altre parole il diritto all'*oblio*, è uno dei modi in cui – ormai tradizionalmente – il sistema cerca di rispondere alle sempre nuove istanze della *golden age of surveillance*[380].

Posto che la cancellazione stessa si considera a sua volta un'operazione di trattamento di dati, il reg. Ue n. 679 del 2016, in parte discostandosi dalla Direttiva madre[381], sancisce esplicitamente ed autonomamente il diritto alla cancellazione, come diritto dell'interessato, all'art. 17.

Secondo il par. 1 dell'art. 17, «l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali», ma solo se sussiste un motivo specifico, che rientri nelle ipotesi elencate al medesimo paragrafo.

Come si è già avuto modo di evidenziare, tra le fattispecie che determinano il diritto alla

[380] La Direttiva n. 46 del 1995 non prevedeva in modo concettualmente autonomo – e non disciplinava – un diritto alla cancellazione, ma riconosceva – come garanzia che avrebbero dovuto osservare gli Stati membri – che la persona interessata avesse diritto a ottenere dal responsabile del trattamento, a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non fosse conforme alle disposizioni della Direttiva stessa, in particolare a causa del carattere incompleto o inesatto dei dati. E tale disposizione era contenuta nell'art. 12 – in particolare alla lett. *b* – rubricato "Diritto di accesso", quasi che la cancellazione fosse una parte di questa situazione giuridica. Il legislatore italiano, nel recepire la Direttiva, annoverava la cancellazione fra i diritti dell'interessato, all'art. 13 della l. n. 675/1996 e poi all'art. 7 del d.lgs. n. 196/2003.

[381] SPATARO, *Il diritto all'oblio tra definizione sostanziale e rimedi di tutela. Riflessioni alla luce della giurisprudenza più recente della Corte di Cassazione e della Corte di Giustizia dell'Unione Europea in materia di deindicizzazione*, in *Dir. cost.*, 2023, fasc. 1.

cancellazione vi sono la revoca del consenso[382] e l'esercizio del diritto di opposizione[383]. Entrambe queste fattispecie mirano a realizzare l'autodeterminazione informativa della persona ed entrambe sono legate al consenso, nella misura in cui traducono una manifestazione di volontà.

Il diritto di opposizione, poi, per come è delineato dal Regolamento, è pure in grado di far emergere e prendere in considerazione le specifiche e particolari condizioni personali del soggetto, che altrimenti non potrebbero avere rilievo. L'art. 21, infatti, stabilisce che «l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua *situazione particolare*, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f)»[384].

Tuttavia, nella continua e delicata opera di bilanciamento condotta dal legislatore eurounitario, anche al diritto di cancellazione sono apposti dei limiti e così, ai sensi del par. 3 dell'art. 17 non può aversi cancellazione quando il trattamento dei dati personali sia *necessario* per una serie tassativa di finalità. Tra queste, è appena il caso di ricordare, per la rilevanza in relazione ai dati sanitari, quella di cui alla lett. *c*, ossia l'ipotesi di trattamento necessario «per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3».

Dunque, la volontà del soggetto, che, di regola, condurrebbe alla cancellazione dei suoi dati personali, viene messa da parte, in presenza di specifiche circostanze connotate da necessità[385].

Eppure, nonostante le proclamazioni e la retorica che hanno accompagnato il consenso, nonostante il tramonto del suo storico ruolo[386], si percepisce che in esso, come espressione

[382] Art. 17, par. 1, lett. *b*: «l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento».

[383] Art. 17, par. 1, lett. *c*: «l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2».

[384] «Il titolare del trattamento – prosegue – si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria».

[385] Cfr. CIANCIMINO, *Protezione e controllo dei dati in àmbito sanitario e intelligenza artificiale. I dati relativi alla salute tra novità normative e innovazioni tecnologiche*, cit.

[386] A. THIENE., *La regola e l'eccezione. Il ruolo del consenso in relazione al trattamento dei dati sanitari alla luce dell'art. 9 GDPR*, cit.

dell'autodeterminazione della persona, vi è un *quid*[387], forse una traccia o un principio, di quello che può persistere a difesa della personalità dell'individuo. Mito del mito[388], allora, e non semplice mitologia, poiché qualcosa di questa mitica creatura può salvarsi e servire ancora, per la tutela della persona.

Il pensiero va al consenso inteso non tanto come assenso e men che meno come base giuridica, quanto come *dissenso*. Al di là delle forme prestabilite[389] della revoca o della opposizione, che si scontrano con il limite del diritto di cancellazione.

Si pensi a un consenso conforme al modello di *opt-out*[390]. Ma non un dissenso generalizzato, bensì una volontà da far valere in casi circoscritti – di speciale sensibilità del dato – che permetta così la tutela della persona, garantendo una forma di controllo sulle informazioni più delicate – o più dolorose – che lo riguardano, e insieme ottimizzi la circolazione di tutti quei dati personali, che tale speciale sensibilità non hanno, e il cui trattamento possa giovare alla collettività[391].

4. *L'*amministrativizzazione *della protezione dei dati personali*

Com'è stato efficacemente osservato in dottrina, l'innovazione del reg. Ue n. 679/2016 «configura il passaggio da una concezione fondata esclusivamente sul consenso informato ad una concezione caratterizzata prevalentemente sul controllo, nella consapevolezza che il consenso non è sufficiente e che anzi è, per certi versi, fuorviante e inidoneo di fatto a garantire il rispetto della persona»[392].

Questa svolta, come si è cercato di illustrare, appare frutto di una elaborazione che prende avvio da molto lontano, cioè dagli inizi delle riflessioni sulla protezione dei dati

[387] E non si tratta necessariamente della responsabilità, che ha rappresentato e resta uno dei profili forse più strettamente legati alla figura del consenso dell'interessato, tuttora di primaria importanza. Cfr. DI CIOMMO, *Civiltà tecnologica, mercato ed insicurezza: la responsabilità del diritto*, in RUSCELLO (a cura di), *Studi in onore di Davide Messinetti*, II, Napoli, Edizioni Scientifiche Italiane, 2008.

[388] SOLOVE, *The Myth of the Privacy Paradox*, in *GW Law Faculty Publications & Other Works*, in *www.scholarship.law.gwu.edu*, 1° febbraio 2020

[389] Ripensare il consenso, oltre le categorie note. Cfr. SOLOVE, *Introduction: privacy self-management and the consent dilemma*, in *Harvard Law Review*, 2013;

[390] «La prospettiva del consenso non è da tutti giudicata sufficiente a proteggere l'interessato. Alcuni AA., ad es., propongono – soprattutto in relazione ai dati relativi alla salute – di passare da un "*opt-in model*" (basato cioè sul consenso come prerequisito per la circolazione soprattutto "secondaria") ad un "*opt-out approach*" (in cui la circolazione è tendenzialmente "libera" ma può essere impedita da una specifica manifestazione di volontà dell'interessato) […]. Secondo questa opinione la trasformazione del consenso da "elemento di *routine*" ad elemento eccezionale gioverebbe all'interessato, rendendolo più attento e prudente e quindi in condizione di effettuare una scelta più consapevole». PELLECCHIA, *Scelte contrattuali e informazioni personali*, cit,

[391] S. CORSO, *Sanità digitale e riservatezza. Interpretazioni sul fascicolo sanitario elettronico*, cit.

[392] P. PERLINGIERI, Privacy *digitale e protezione dei dati personali tra persona e mercato*, cit.

personali e la legislazione in materia.

Peraltro, già il meccanismo delle autorizzazioni del Garante, previsto dalla l. n. 675 del 1996, era un modo per offrire una tutela della persona, distinto dal consenso e ad esso alternativo, o forse addirittura un contrappeso alla valenza generale del consenso e al rischio che si traducesse in un'insidia per l'interessato, nella sua posizione di debolezza[393]. Il pensiero giuridico si è mosso, dunque, alla ricerca di altri strumenti, diversi dal consenso, per garantire la protezione dei dati personali – specie quelli sensibili – e, con essa, la protezione della persona.

La via intrapresa ha condotto le riflessioni verso una serie di misure e accorgimenti, soprattutto di natura tecnica, in grado di intervenire preventivamente rispetto alla possibile violazione di dati personali. E questi si sono poi tradotti in principi e regole, che possono, in larga parte, ricondursi al concetto di 'sicurezza'.

Si pensi alle nozioni di *privacy by design* e *privacy by default*, la riservatezza per progettazione e per impostazione[394]. Il sistema giuridico che impone al sistema informatico di conformarsi, sin dall'origine, alla protezione dei dati personali. Ciò significa che sin dalla sua costruzione l'ambiente digitale va pensato come un insieme di strutture che garantiscano il diritto alla protezione dei dati personali e l'architettura dello spazio elettronico deve rispondere a questa logica[395].

In tal senso, la privacy non è più vista come un qualcosa di aggiunto, un diritto che va esercitato in un contesto di circolazione delle informazioni, bensì come un diritto che è tutelato certo in quel contesto, ma anche da quel contesto, e a prescindere dall'esercizio della pretesa del singolo. Un diritto, quindi, che partecipa all'edificazione dell'ambiente digitale[396].

---

[393] PELLECCHIA, *Scelte contrattuali e informazioni personali*, cit

[394] V. l'art. 25 del Regolamento, rubricato "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita".

[395] BRAVO, *Data Management Tools and Privacy by Design and by Default*, in SENIGAGLIA, C. IRTI e A. BERNES (a cura di), *op. cit*

[396] Sulla *privacy by design* come strumento di tutela della persona in ambito sanitario: RUFO, *Social media e consulto medico: tra opportunità e rischi per i pazienti*, in *Inform. e dir*., 2017, fasc. 1-2. «L'implementazione della privacy by design rappresenta senza dubbio un traguardo da raggiungere (per non dire cruciale) in particolare in ambito sanitario. Così che il fulcro della sicurezza del trattamento sia costituito da una serie di misure tecniche, logiche e organizzative preventive, accompagnate da altrettanto efficaci mezzi di ripristino in caso di violazione dei dati personali e sensibili. La prevenzione e l'anticipazione di possibili violazioni dei dati sanitari permettono di raggiungere una percezione di alta affidabilità degli strumenti in uso presso i pazienti e riducono o eliminano interventi architetturali successivi» (p. 392)

Se il codice – informatico – diventa la nuova legge[397], allora il diritto illumina e innerva questo codice in modo che assicuri l'osservanza dei principi e delle regole, che al di fuori dello spazio elettronico è assicurata dalla legge.

Si pensi alla pseudonimizzazione[398]. Una tecnica che consente di sottrarre al dato personale la sua capacità di attribuirsi al soggetto cui si riferisce, rendendolo dato pseudonimizzato. La sottrazione non è irreversibile ed è sempre possibile restituire al dato la sua potenzialità attributiva originaria attraverso l'utilizzo della specifica 'chiave' creata per pseudonimizzare. In ciò si distingue la pseudonimizzazione dall'anonimizzazione, che invece spoglia irreversibilmente il dato personale della possibilità di essere attribuito alla persona e lo rende, appunto, dato anonimo.

L'art. 32, che apre la Sezione 2, "Sicurezza del trattamento", del Capo IV del Regolamento, nel prevedere che i soggetti del trattamento mettano in atto le idonee misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, inizia l'elenco di tali misure proprio con la pseudonimizzazione, al par. 1, lett. *a*.

Il dato pseudonimizzato è ancora dato personale e ne conserva il valore, poiché l'individuo rimane identificabile, ma il trattamento che si svolge diviene più sicuro[399].

Si pensi alle procedure di valutazione del rischio[400]. Nella terminologia del Regolamento, la "valutazione dei rischi per i diritti e le libertà degli interessati" è inclusa nella "valutazione d'impatto sulla protezione dei dati", ai sensi dell'art. 35, par. 7, lett. *c*.

La valutazione d'impatto è richiesta al titolare del trattamento quando il tipo di trattamento che si intende effettuare può presentare un rischio elevato per i diritti e le libertà degli interessati. In questo iter è previsto pure il coinvolgimento dell'autorità di controllo, ai sensi dell'art. 36 del Regolamento: infatti, se la valutazione d'impatto sulla protezione dei dati indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare per attenuare il rischio, questi deve procedere con una consultazione preventiva dell'autorità. Peraltro, il par. 5 dell'art. 36 permette agli Stati membri di prescrivere che i titolari consultino l'autorità di controllo e ne ottengano l'autorizzazione preliminare, in

[397] Secondo la celebre formula "*code is law*". LESSIG, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999

[398] La pseudonimizzazione è definita all'art. 4, n. 5), del Regolamento come: «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile».

[399] PELLECCHIA, *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, cit.

[400] MANTELERO, *La gestione del rischio*, cit

relazione al corrispondente trattamento per l'esecuzione di un compito di interesse pubblico, come «il trattamento con riguardo alla protezione sociale e alla sanità pubblica».

La procedimentalizzazione della consultazione preventiva, operata dall'art. 36, si aggiunge a quella della valutazione d'impatto con l'effetto di premettere grande cautela alle operazioni di trattamento, con speciale riguardo ai profili di rischio per la protezione dei dati personali.

Ma si pensi, soprattutto, al principio di *accountability*, la responsabilizzazione dei soggetti che operano il trattamento dei dati[401].

In forza di questo principio, ai sensi dell'art. 5, par. 2, il titolare del trattamento è competente per il rispetto di tutti i principi del trattamento dei dati personali, di cui al par. 1 dell'art. 5, ed è in grado di comprovarlo. Spetta quindi al titolare assicurare l'osservanza di quei principi e deve dimostrare che, nei trattamenti posti in essere, essi vengono rispettati.

Nell'ipotesi in cui il trattamento si basi sul consenso dell'interessato, il Regolamento, all'art. 7, par. 1, prescrive specificamente – come declinazione della più generale responsabilizzazione del titolare – che questi debba poter dimostrare che il consenso è stato prestato.

Ai sensi dell'art. 24 del Regolamento, il titolare del trattamento, «tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche», tenuto conto cioè di un insieme di circostanze che qualificano il trattamento di dati personali stesso, deve adottare le misure tecniche e organizzative che non solo ne garantiscano la conformità al Regolamento, ma anche gli consentano di dimostrarla.

Il principio di *accountability* «costituisce il nucleo della riforma europea e realizza un nuovo sistema normativo nel trattamento dei dati personali e nella protezione dei diritti della persona»[402]. Con esso la tutela della persona, attraverso la protezione dei dati personali, è traslata dal piano rimediale successivo e della sanzione e dal piano singolare e puntiforme del consenso dell'interessato a quello più generale e preventivo della gestione del rischio.

In ciò, acquista nuova centralità il ruolo del titolare del trattamento[403]: infatti, egli deve ora mettere in atto misure appropriate ed efficaci per assicurare la protezione dei dati, in

[401]M.G. STANZIONE, *La protezione dei dati personali tra «consumerizzazione» della* privacy *e principio di* accountability, in *Comparazione e diritto civile*, 2022.
[402] FINOCCHIARO, *Il principio di* accountability, cit
[403] R. MESSINETTI, *Circolazione dei dati personali e autonomia privata*, cit., 146: «al ridimensionamento della volontà del titolare dei dati personali fa da contrappunto il rafforzamento di un potere del titolare del trattamento: il diritto – appunto – di trattare i dati personali altrui».

conformità ai principi del Regolamento, e deve anche adoperarsi per tenere traccia dell'adozione di queste misure, preparandosi a rispondere a una richiesta di dimostrazione.

Lungi dal restare una norma meramente programmatica, tale principio ha ricadute pratiche e organizzative di non poco momento, tanto in termini operativi, legati alle misure che vanno prese, quanto in termini precauzionali, come precostituzione della prova.
Quindi è il dovere di sicurezza, per le persone i cui dati vengono trattati, e l'obbligo di sicurezza, in capo ai soggetti che operano il trattamento, titolare e responsabile.

A ben vedere, però, una gran parte dei trattamenti di dati personali effettuati è riconducibile ad attività della pubblica amministrazione e ciò è particolarmente vero per i dati relativi alla salute, se si considera che uno degli ambiti più importanti, forse il principale, in cui essi vengono trattati è proprio quello sanitario.

E, se si parla di soggetti pubblici, allora, il campo delle regole non è più quello del diritto privato, ma è quello del diritto pubblico o, meglio, del diritto amministrativo.

La riservatezza, l'informazione, il segreto, la trasparenza sono state a lungo oggetto di studio per questa branca del diritto[404].

La normativa in materia di privacy si trova al confine tra diritto privato e diritto pubblico, compreso il diritto amministrativo, e si è composta attingendo ai criteri propri di ciascuno di questi sistemi, che però mantiene la sua precisa identità, all'interno dello Stato di diritto.

L'approccio orientato alla responsabilizzazione del titolare del trattamento, che connota l'impianto del Regolamento, e l'incidenza delle nuove tecnologie sulla protezione dei dati personali – tecnologie per cui, come si avrà modo di precisare ulteriormente, si avverte sempre più l'esigenza di un quadro normativo definito – richiamano l'attenzione del legislatore nazionale, che deve intervenire – anche per la rilevanza pubblica degli interessi coinvolti – attraverso una normazione di diritto pubblico e amministrativo[405].

Nel dettare i doveri del titolare del trattamento, quindi nel sancire i nuovi compiti della

[404] «L'informazione rappresenta da sempre un tema centrale nell'azione amministrativa, quale *bene* strumentale e *attività* preordinata al corretto esercizio delle funzioni pubbliche». P. PERLINGIERI, *La pubblica amministrazione e la tutela della* privacy. *Gestione e riservatezza dell'informazione nell'attività amministrativa*, in ID., *La persona e i suoi diritti. Problemi del diritto civile*, Napoli, Edizioni Scientifiche Italiane, 2005

[405] «La riservatezza e il corretto trattamento dei dati personali si configurano dunque come oggetto di tutela da parte sia dell'ordinamento europeo, sia del nostro ordinamento nazionale. Dal punto di vista del diritto amministrativo, la protezione dei dati personali si presenta come una finalità in vista della quale vengono definiti un insieme di compiti specifici delle pubbliche amministrazioni, soprattutto dopo che il GDPR ha introdotto un approccio preventivo a questo tipo di tutela». BOMBARDELLI, *op. cit*

pubblica amministrazione, l'ordinamento sembra disegnare una funzione amministrativa[406], funzione di protezione dei dati personali, che significa tanto gestione dei dati personali quanto controllo dei trattamenti di dati.

Questa linea seguita dalla legislazione in materia è coerente all'indirizzo di fondo, cioè di ricerca di altri strumenti, diversi dal consenso dell'interessato, per garantire la tutela della persona. Peraltro, in caso di trattamenti effettuati da pubbliche autorità, anche per lo squilibrio di potere fra i soggetti coinvolti, il consenso non si rivela come la base giuridica più idonea[407] e fondare la legittimazione del trattamento su altre basi non significa necessariamente abdicare a una tutela effettiva della persona o alla prospettiva personalistica.

È appena il caso di ricordare che il Regolamento, nell'elencare le condizioni di liceità del trattamento, all'art. 6, lett. *e*, prevede espressamente la necessità per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento[408] e, fra le ipotesi di deroga al divieto di trattamento delle particolari categorie di dati, all'art. 9, par. 2, lett. *g*, annovera la fattispecie di necessità per motivi di interesse pubblico rilevante[409].

L'indirizzo seguito, in questi termini, riflette un paradigma circolatorio differente, in cui l'affermarsi di regole di natura pubblicistica sembra rispondere a una logica maggiormente ispirata alla solidarietà. A ciò si aggiunga il quadro normativo tracciato dal *Data Governance Act*, reg. Ue n. 868/2022[410], principalmente per il riutilizzo, all'interno dell'Unione, di determinate categorie di dati detenuti da enti pubblici.

Le disposizioni di questo Regolamento, peraltro, non si limitano a fornire riferimenti

---

[406] V. CARULLO, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Torino, Giappichelli, 2018 che, riferendosi alla trasformazione digitale dell'amministrazione, rintraccia un'autonoma "funzione amministrativa dei dati".

[407] «Il considerando 43 indica chiaramente che è improbabile che le autorità pubbliche possano basarsi sul consenso per effettuare il trattamento, poiché quando il titolare del trattamento è un'autorità pubblica sussiste spesso un evidente squilibrio di potere nella relazione tra il titolare del trattamento e l'interessato. In molti di questi casi è inoltre evidente che l'interessato non dispone di alternative realistiche all'accettazione (dei termini) del trattamento. Il Comitato ritiene che esistano altre basi legittime, in linea di principio più appropriate, per il trattamento da parte delle autorità pubbliche». European Data Protection Board, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, Versione 1.1*, cit

[408] V. FRANCARIO, *Protezione dei dati personali e pubblica amministrazione*, in PISANI, PROIA e TOPO (a cura di), *op. cit.*, 679 ss., che si esprime in senso critico verso l'appiattimento sulla matrice privatistica, che, in assenza del consenso, non permetterebbe il trattamento dei dati personali

[409] Tra l'interessato e il titolare del trattamento si instaura un vero e proprio rapporto amministrativo. V. F. CORTESE, in D'ORAZIO, FINOCCHIARO, POLLICINO e G. RESTA (a cura di), *op. cit., sub* art. 2 *sexies*, d.lgs. 30 giugno 2003, n. 196

[410] «Il *Data Governance Act*, pubblicato nella Gazzetta Ufficiale dell'Unione europea il 3 giugno 2022, ha costituito la prima misura della strategia europea in materia di dati e mira a promuoverne la disponibilità». Così Giusella Finocchiaro in VERDOLINI, *Regolare l'economia digitale. Intervista a Giusella Finocchiaro*, in *Pandora Rivista*, 2021, fasc. 3 *Tempi della tecnica*

normativi amministrativistici, ma pure ritornano sul consenso del soggetto e lo valorizzano sotto altra luce. Il *Data Governance Act*, infatti, concepisce il consenso in termini altruistici, prevedendo la possibilità che l'interessato acconsenta al trattamento dei propri dati personali per il raggiungimento di obiettivi di interesse generale. In questo senso, facendo leva sull'adesione del singolo alle scelte pubbliche e sul senso individuale di solidarietà, il consenso dell'interessato viene riletto in una chiave diversa, appunto solidaristica, potendo diventare strumento per la condivisione delle informazioni, il dispositivo su cui fondare il c.d. altruismo dei dati[411].

Uno dei fattori che certamente ha avuto e avrà grande influenza nella conformazione del diritto amministrativo, anche in materia di privacy, è lo sviluppo della tecnologia. La pubblica amministrazione si avvale, infatti di strumenti tecnologici – compresa l'intelligenza artificiale[412] – per trattare tutte le categorie di dati personali. E l'impiego delle nuove tecniche è tanto più possibile, quanto maggiore è la garanzia di sicurezza nelle attività[413].

Anche per questo, è cruciale l'investimento nella c.d. *cybersecurity*[414]. L'emergenza sanitaria da Covid-19 non fa che confermare l'assunto[415].

---

[411] L'altruismo dei dati è definito all'art. 2, n. 16 del *Data Governance Act* come «la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale». Si v. gli artt. 16 ss. del reg. Ue n. 868 del 2022 e, in particolare, l'art. 25, che prevede un 'modulo europeo di consenso all'altruismo'.

[412] RODOTÀ, *Elaboratori elettronici e controllo sociale*, scriveva: «il fatto che molte informazioni delicate (ma non tutte) continuino ad essere schedate con metodi tradizionali, si spiega probabilmente con le scarse garanzie di sicurezza ancora offerte dagli elaboratori e con il senso di potere e di tranquillità derivante dal tenere quelle informazioni in cartelle chiuse in un armadio blindato della propria stanza piuttosto che nella lontana memoria di un elaboratore. Ma, una volta accresciuta la sicurezza delle macchine e rimossi taluni condizionamenti psicologici, anche le informazioni più riservate verranno certamente trattate con l'elaboratore».

[413] . Con riguardo alla digitalizzazione della sanità, scrive MASCOLO, *La sfida della sanità digitale nel post pandemia*, in www.irpa.eu, *Osservatorio sullo Stato digitale*, 30 giugno 2020. «Ora che la pandemia sta contribuendo a mostrare il potenziale della sanità digitale, il suo sviluppo non può restare affidato alle iniziative di singole strutture ospedaliere e soggetti privati, bensì è necessario un quadro regolatorio unitario a livello nazionale, in grado di armonizzare gli applicativi digitali (anche al fine di assicurare l'interoperabilità dei sistemi) e, soprattutto, di assicurare un'infrastruttura robusta e sicura, a salvaguardia del patrimonio dei dati sanitari dei pazienti e dell'efficienza del sistema sanitario». Cfr. HANSEN *et al*., *op. cit*.. Per uno sguardo complessivo al sistema sanitario italiano,

v. PIOGGIA, *La sanità italiana di fronte alla pandemia. Un banco di prova che offre una lezione per il futuro*, in *Dir. pubbl.*, 2020

[414] ALOVISIO, *I nuovi poteri sanzionatori dell'Agenzia per la Cybersicurezza Nazionale in materia di certificazioni*, in www.dirittoegiustizia.it, 24 agosto 2022

[415] «Il trattamento di dati personali oggi, sempre di più, investe una sua dimensione pubblicistica, in ragione della raccolta su larga scala dei dati e dell'uso di tecnologie sofisticate impiegate a tal fine, incluso l'utilizzo di

Sul piano normativo, hanno già assunto rilevanza il Regolamento n. 881 del 2019, c.d. "Cybersecurity Act" e, con riguardo all'esperienza italiana, il d.lgs. n. 123 del 2022, sulla certificazione della cybersicurezza.

In questo scenario il ruolo del Garante per la protezione dei dati personali – che è autorità amministrativa indipendente – già fondamentale sin dalla sua istituzione, acquista un'importanza sempre maggiore, nell'esercizio di tutti i suoi compiti, primo fra tutti quello di controllo e sanzionatorio. E, nello specifico, per i trattamenti di dati relativi alla salute, all'Autorità garante il legislatore italiano ha affidato il compito di adottare le 'misure di garanzia', *ex* art. 2 *septies* del Codice della privacy.

Nel complesso delle norme relative alla protezione dei dati personali nella P.A., non va dimenticato il tassello della trasparenza. Un principio dettato con riguardo all'informazione da rendere all'interessato[416], che, in altro senso, connota l'agire della pubblica amministrazione[417] e che assume nuovi significati con l'evoluzione della tecnologia e del diritto stesso, in materia di privacy[418].

Tutto ciò vale anche per il diritto sanitario. La norma del diritto pubblico che si cala nel contesto della sanità, nella garanzia del diritto alla salute, deve oggi includere la protezione dei dati personali e, specialmente, di quelli sanitari[419].

Come espresso proprio dalla legge Gelli-Bianco, in apertura, all'art. 1, tutte le attività finalizzate alla prevenzione e alla gestione del rischio connesso all'erogazione di prestazioni sanitarie e l'utilizzo appropriato delle risorse strutturali, tecnologiche e organizzative contribuiscono a realizzare la sicurezza delle cure, che è parte costitutiva del diritto alla salute ed è perseguita nell'interesse dell'individuo e della collettività. Con ciò si intende che nella tutela al diritto alla salute vanno ricompresi tutti quei requisiti organizzativi volti a

---

algoritmi. Proprio per tale ragione esso necessita di un enforcement pubblico, la sanzione amministrativa irrogata dall'autorità amministrativa indipendente, che spinga il titolare del trattamento ad adottare tutte le misure appropriate per gestire il rischio connesso al trattamento». SIRGIOVANNI, *op. cit*

[416] Si v. l'art. 12 del Regolamento, nonché i considerando 39, 58, 78 e 100.

[417] *Ex plurimis*, MERLONI (a cura di), *La trasparenza amministrativa*, Milano, Giuffrè, 2008.

[418] Trasparenza come principio che vale, ad esempio, per il trattamento dei dati personali, nel senso che si rendano trasparenti le operazioni di trattamento svolte e, per quanto possibile e utile, il funzionamento della tecnologia impiegata. V. R. MESSINETTI, *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. e impr.*, 2019, 861: «Nel discorso prescrittivo del GDPR, l'obiettivo della sicurezza della circolazione dei dati personali risulta affidato a una strategia complessa incentrata, in primo luogo, su un principio sistemico: la trasparenza dei processi di trattamento dei dati». Il principio di trasparenza nella protezione dei dati personali, ovviamente, non è limitato ai trattamenti di cui è titolare la pubblica amministrazione, ma vale trasversalmente per ogni trattamento, anche per quello posto in essere da privati. In tal senso può rivestire un ruolo fondamentale anche per la protezione dei dati sanitari rispetto alle attività delle grandi imprese tecnologiche.

[419] V. M.A. SANDULLI, *Introduzione*, cit.

garantire trasparenza ed efficienza delle risorse e che implicano l'uso delle tecnologie. La protezione dei dati personali entra a far parte della tutela del diritto alla salute, come diritto della personalità e nell'orizzonte unitario – concettuale, giuridico – della persona umana[420].

Perciò la regolazione amministrativistica prevale su quella privatistica. È questo superamento l'*amministrativizzazione della protezione dei dati personali*[421]

Il fatto che le disposizioni non siano più – o non più tanto – di diritto privato, ma di diritto amministrativo non cambia il modo in cui vanno interpretate, alla luce del principio personalista e della dignità, che perme il nostro ordinamento[422].

[420] «La persona umana si prospetta nella sua unitarietà psico-fisica come un mondo soggettivo condizionato dalle circostanze ambientali, sociali, economiche, sì che diventa impossibile separare il bene salute dal valore complessivo della persona; questa assume una concreta realizzazione nel rispetto della storicità del momento. La libertà della persona ed i suoi effettivi contenuti, il particolare atteggiarsi del rapporto della persona con l'autorità dell'apparato della comunità in cui vive, il grado di socialità ed eticità dell'ambiente, sono elementi che incidono sulla qualità dello sviluppo della persona e pertanto sulla sua salute, intesa come equilibrio psichico, mentale e quindi fisico». P. PERLINGIERI, *La persona e i suoi diritti. Problemi del diritto civile*, cit.

[421] S. CORSO, *Sanità digitale e riservatezza. Interpretazioni sul fascicolo sanitario elettronico*, cit;

[422] ZATTI, *Note sulla semantica della dignità*, cit. Cfr. SCALISI, *L'ermeneutica della dignità*, Milano, Giuffrè, 2018;

CAPITOLO III
PROTEZIONE DEI DATI RELATIVI ALLA SALUTE E INNOVAZIONE TECNOLOGICA IN SANITÀ

1. *La digitalizzazione della sanità*

Nel nostro tempo gli ordinamenti nazionali europei vivono la stagione della digitalizzazione. Il processo di ammodernamento tecnologico investe in modo trasversale le strutture della società contemporanea, tanto pubbliche quanto private[423].

Nel dare impulso a questo processo, l'Unione europea svolge un ruolo fondamentale[424]. La Commissione europea, nella Comunicazione, del 19 febbraio 2020, *Plasmare il futuro digitale dell'Europa*, ha individuato i tre obiettivi chiave nel perseguimento della digitalizzazione per i successivi cinque anni: una tecnologia al servizio delle persone, un'economia equa e competitiva e una società aperta, democratica e sostenibile. La trasformazione digitale è quindi guidata dalle Istituzioni dell'Unione, affinché avvenga sempre nel rispetto dei suoi valori[425].

La visione della Commissione per gli anni a venire ha preso corpo con la Comunicazione del 9 marzo 2021, *Bussola per il digitale 2030*[426]. Con questa si è tracciato il percorso dell'Unione, stabilendo i 'punti cardinali' attorno ai quali si definiranno le tappe fondamentali: due sono incentrati sulle capacità digitali a livello di infrastrutture e di istruzione e competenze, altri due sulla trasformazione digitale delle imprese e dei servizi pubblici[427]. In questo orizzonte, in cui la protezione dei dati personali riveste un ruolo

---

[423] A. SANDULLI, *Lo «Stato digitale». Pubblico e privato nelle infrastrutture digitali nazionali strategiche*, in *Riv. trim. dir. pubbl.*, 2021.

[424] CAMARDI, *Sulla Governance digitale europea: una proposta di confronto*, in *Accademia*, 2023.

[425] «Questa Europa digitale dovrebbe riflettere il meglio dell'Europa: apertura, equità, pluralismo, democrazia e sicurezza». Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Plasmare il futuro digitale dell'Europa*, del 19 febbraio 2020, COM(2020) 67 final, 2. Va ricordato, peraltro, come, per quanto attiene alla trasformazione digitale della pubblica amministrazione, si tratti di un percorso che l'Unione europea sta tracciando da più tempo. Si ricorda la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, del 19 aprile 2016, *Piano d'azione dell'UE per l'eGovernment 2016-2020 Accelerare la trasformazione digitale della pubblica amministrazione*

[426] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, del 9 marzo 2021, COM(2021)

[427] In ordine i 'punti cardinali' sono: "Una popolazione dotata di competenze digitali e professionisti altamente qualificati nel settore digitale"; "Infrastrutture digitali sostenibili, sicure e performanti"; "Trasformazione digitale delle imprese"; "Digitalizzazione dei servizi pubblici". La Commissione ha anche scelto, per ciascuno di

chiave, l'intelligenza artificiale partecipa della digitalizzazione e questa comprende la sanità.

Il 26 gennaio 2022 la Commissione ha presentato il testo della "Dichiarazione europea sui diritti e i principi digitali per il decennio digitale"[428], che è stato poi approvato, con alcune modifiche, e firmato il 15 dicembre 2022, come Dichiarazione comune di Parlamento europeo, Consiglio e Commissione europea[429].

Il diritto alla protezione dei dati personali, unitamente al diritto al rispetto della vita privata, è ribadito dalla Dichiarazione stessa, al punto 17, con l'espressa precisazione che esso «prevede anche che i singoli individui abbiano il controllo di come sono utilizzati i propri dati e con chi sono condivisi».

All'intelligenza artificiale la Dichiarazione dedica, per intero, la prima parte del Capitolo III, "Libertà di scelta", "Interazioni con algoritmi e sistemi di intelligenza artificiale". Secondo quanto enunciato al punto 8, «l'intelligenza artificiale dovrebbe fungere da strumento per le persone, con l'obiettivo ultimo di aumentare il benessere umano».

Mentre, nel Capitolo II, "Solidarietà e inclusione", il punto 7, inerente ai servizi pubblici digitali online, sancisce l'impegno delle istituzioni ad «agevolare e sostenere in tutta l'UE un accesso fluido, sicuro e interoperabile a servizi pubblici digitali concepiti per soddisfare le esigenze delle persone in modo efficiente, compresi in particolare i servizi sanitari e assistenziali digitali, segnatamente l'accesso alle cartelle cliniche elettroniche».

Il 14 dicembre 2022, invece, il Parlamento europeo e il Consiglio hanno adottato la Decisione n. 2481 del 2022, *che istituisce il programma strategico per il decennio digitale 2030*[430]. Con questo atto l'Unione europea ha inteso dare attuazione a quanto espresso nella

---

detti punti, gli obiettivi comuni per mobilitare soggetti pubblici e privati, nominati rispettivamente: "Un continente tecnologicamente esperto in cui tutti sono autonomi e responsabili dal punto di vista digitale"; "Infrastrutture digitali sicure, affidabili e di eccellenza"; "Il continente con un'alta percentuale di imprese digitalizzate"; "Servizi pubblici modernizzati rispondenti alle esigenze della società". Questi obiettivi sono elencati e descritti nell'allegato alla Comunicazione *Bussola per il digitale 2030.*

[428] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali*, del 26 gennaio 2022, COM(2022).

[429] Pubblicato nella Gazzetta ufficiale dell'Unione europea del 23 gennaio 2023, il testo della Dichiarazione è consultabile in *eur-lex.europa.eu*.

[430] Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, *che istituisce il programma strategico per il decennio digitale 2030*. Ai sensi dell'art. 1: «1. La presente decisione istituisce il programma strategico per il decennio digitale 2030 e definisce un meccanismo di monitoraggio e cooperazione per tale programma, concepito per: a) creare un ambiente favorevole all'innovazione e agli investimenti attraverso la definizione di una direzione chiara per la trasformazione digitale dell'Unione e per il conseguimento degli obiettivi digitali a livello di Unione entro il 2030 sulla base di indicatori misurabili; b) strutturare e stimolare la cooperazione tra il Parlamento europeo, il Consiglio, la Commissione e gli Stati

Comunicazione *Bussola per il digitale 2030* e, in particolare, ha tradotto i 'punti cardinali' individuati dalla Commissione in 'obiettivi digitali', cioè in traguardi da raggiungere, ai sensi dell'art. 4, entro il 2030.

Tra questi, speciale attenzione merita, per quanto attiene alla sanità pubblica, la digitalizzazione dei servizi pubblici, che include l'accesso, da parte di tutti i cittadini dell'Unione, al proprio fascicolo sanitario elettronico[431]. Come sottolineato al considerando 18, «i servizi pubblici fondamentali, compreso il fascicolo sanitario elettronico, dovrebbero essere pienamente accessibili su base volontaria, come pure dovrebbe essere accessibile un ambiente digitale della migliore qualità che offra servizi e strumenti di facile uso, efficienti, affidabili e personalizzati, con elevati standard in materia di sicurezza e tutela della vita privata».

L'intelligenza artificiale è presa in considerazione tra le finalità generali del programma strategico per il decennio digitale 2030 sancite all'art. 3, nel dettaglio, in quella di cui alla lett. *e)*, cioè sviluppare un ecosistema globale e sostenibile di infrastrutture digitali interoperabili in cui le alte prestazioni, la computazione di prossimità (*edge computing*), il *cloud*, la computazione quantistica, la gestione dei dati, la connettività di rete e, appunto, l'intelligenza artificiale «lavorano in convergenza, al fine di promuovere la loro diffusione nelle imprese dell'Unione»[432].

L'intelligenza artificiale può inoltre svolgere un ruolo nel conseguimento degli obiettivi del Green Deal europeo[433]. È infatti annoverata, al considerando 6 della Decisione n. 2481/2022, fra le tecnologie digitali, quali il 5G, il 6G, la blockchain, il cloud e la computazione di prossimità, che «dovrebbero accelerare e massimizzare l'impatto delle

membri; c) promuovere la coerenza, la comparabilità, la trasparenza e la completezza del monitoraggio e delle relazioni dell'Unione. 2. La presente decisione istituisce un quadro per i progetti multinazionali».

[431] Art. 4: «1. Il Parlamento europeo, il Consiglio, la Commissione e gli Stati membri cooperano per conseguire gli obiettivi digitali seguenti nell'Unione entro il 2030 («obiettivi digitali»): […] 4) digitalizzazione dei servizi pubblici, laddove: a) il 100 % dei servizi pubblici principali sia accessibile online e, se del caso, sia possibile per le imprese e i cittadini all'interno dell'Unione interagire online con le amministrazioni pubbliche; b) il 100 % dei cittadini dell'Unione abbia accesso al proprio fascicolo sanitario elettronico; c) il 100 % dei cittadini dell'Unione abbia accesso a mezzi di identificazione elettronica sicura (identità digitale — eID) riconosciuti in tutta l'Unione, che consentano loro di avere il pieno controllo sulle transazioni con verifica dell'identità e sui dati personali condivisi».

[432]Coerentemente, l'obiettivo digitale relativo alla trasformazione digitale delle imprese include il raggiungimento almeno del 75 % delle imprese dell'Unione che, in base alle proprie esigenze aziendali, faccia uso di specifiche tecnologie, tra cui l'intelligenza artificiale. V. l'art. 4, par. 1, n. 3, lett. *a*. Le altre tecnologie menzionate sono i servizi di *cloud computing* e i *big data*.

[433] V. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Il Green Deal europeo*, dell'11 dicembre 2019, COM(2019) 640 final.

politiche per affrontare i cambiamenti climatici e proteggere l'ambiente, anche attraverso cicli di vita sostenibili».

Nel processo di digitalizzazione ha avuto, in ogni caso, un influsso considerevole la necessità di far fronte alla pandemia di Covid-19 e di trovare soluzioni condivise, fra gli Stati membri, per rispondere alle nuove esigenze poste dall'emergenza sanitaria[434].

Grazie all'impegno dell'Unione europea[435], il Piano Nazionale di Ripresa e Resilienza italiano prevede un investimento di più di 33 miliardi di euro, alle prime due componenti della missione 1, per la digitalizzazione, e un investimento complessivo di 15,63 miliardi di euro, nella missione 6, 'Salute', che dedica specifica attenzione alla telemedicina e alla digitalizzazione della sanità[436]. Un grande contributo è quindi offerto dal PNRR, per superare le mancanze che hanno caratterizzato la digitalizzazione in Italia[437], e, agevolando la realizzazione della sanità digitale, permetterà il conseguimento di obiettivi di maggiore efficienza, con ricadute in termini di risparmio e riduzione di spesa[438].

Attraverso l'impiego del digitale e delle nuove tecnologie, passando dall'*e-government*

---

[434] MACRÌ, *Le strategie europee per la digitalizzazione e gli obiettivi italiani*, in *Azienditalia*, 2022
«La strategia europea sulla digitalizzazione, inevitabilmente, prende le mosse dalla pandemia causata dal Covid-19 e parte dalla considerazione che la digitalizzazione ha cambiato il suo ruolo, diventando sempre più centrale, ma anche indispensabile per lo sviluppo socio-economico dell'Europa, diffondendosi ad un ritmo accelerato».

[435] Determinante è stato il ruolo dell'Unione europea per il finanziamento stabilito con il Regolamento n. 2094 del 2020 (Regolamento UE 2020/2094 del Consiglio, del 14 dicembre 2020, *che istituisce uno strumento dell'Unione europea per la ripresa, a sostegno alla ripresa dell'economia dopo la crisi COVID-19*), tradotto nello strumento denominato *NextGenerationEU*. Nello specifico, in conformità a quanto previsto dal Regolamento n. 241 del 2021 (Regolamento UE 2021/241 del Parlamento europeo e del Consiglio, del 12 febbraio 2021, *che istituisce il dispositivo per la ripresa e la resilienza*), che dà attuazione alle misure contemplate dal reg. Ue n. 2094/2020, gli Stati membri hanno potuto presentare piani nazionali per la ripresa e la resilienza, che definiscono il programma di riforme e investimenti, per essere ammessi al finanziamento. L'area di intervento relativa all'applicazione del 'dispositivo per la ripresa e la resilienza', definita attraverso una struttura di sei pilastri, include la 'trasformazione digitale' (Art. 3, lett. *b*., reg. Ue n. 241/2021).

[436] Il testo del Piano è consultabile nel sito istituzionale, *www.governo.it.* Le risorse previste dalla seconda componente della missione 6, ossia allo scopo di sostenere l'aggiornamento tecnologico e digitale, nonché formazione, ricerca scientifica e trasferimento tecnologico, sono 8,63 miliardi di euro. Di questi, 1,67 è la somma destinata, nell'investimento 1.3, al rafforzamento dell'infrastruttura tecnologica e degli strumenti per la raccolta, l'elaborazione, l'analisi dei dati e la simulazione. L'obiettivo è il potenziamento del Fascicolo Sanitario Elettronico (FSE) e il rafforzamento del Nuovo Sistema Informativo Sanitario (NSIS).

[437] Secondo l'indice DESI 2022, l'Italia si colloca al 18° posto fra i 27 Stati membri dell'UE, in relazione allo stato di avanzamento digitale, segnando quindi un miglioramento rispetto al passato. «Negli ultimi anni – si legge nella relazione per l'Italia, consultabile in *digitalstrategy.ec.europa.eu* – le questioni digitali hanno acquisito attenzione politica, in particolare grazie all'istituzione di un ministero per l'Innovazione tecnologica e la transizione digitale, all'adozione di varie strategie chiave e al varo di molte misure strategiche. Ciò premesso, la trasformazione digitale sconta ancora varie carenze cui è necessario porre rimedio». Si può consultare in *digital-strategy.ec.europa.eu*.

[438] V. CLERICO, Health Technology Assessment. *Principi, metodi e problemi della valutazione economica*, Milano, Giuffrè, 2014

all'*e-health*, si intende raggiungere una maggiore o migliore garanzia del diritto alla salute. Questa transizione ha del rivoluzionario, da un punto di vista non solo economico e gestionale, per i benefici che potrà arrecare alla società[439], ma anche culturale e identitario.

Un modo in cui si è tradotto il digitale in sanità è lo sviluppo della telemedicina[440]. Se, da un lato, ha mostrato grande utilità proprio durante il periodo delle restrizioni, nella pandemia, dall'altro, essa può essere efficace anche nel garantire l'assistenza domiciliare ai pazienti[441].

Nelle linee guida organizzative contenenti il «Modello digitale per l'attuazione dell'assistenza domiciliare», approvate dal Ministero della Salute, con decreto del 29 aprile 2022, conformemente a quanto previsto nel PNRR, specie in relazione alla prima componente della missione 6, la telemedicina si declina in una serie di servizi erogati in via telematica: la televisita, il teleconsulto medico, la teleconsulenza medico-sanitaria, la teleassistenza, il telemonitoraggio, il telecontrollo, la teleriabilitazione[442].

Dal punto di vista della modalità in cui è fornita l'assistenza, laddove per l'erogazione dei servizi di telemedicina ci si avvalga di dispositivi mobili, come, ad esempio, smartphone e tablet, e delle relative "App", si può osservare come essa partecipi dell'*m- Health*[443].

Ma, forse, lo strumento che maggiormente contraddistingue la digitalizzazione nella sanità è il Fascicolo Sanitario Elettronico (FSE)[444].

---

[439] FINOCCHIARO e POLLICINO, *Perché condividere i dati sanitari aiuta a tutelare i cittadini. Il nuovo regolamento europeo*, in *Il Sole 24 Ore* e in www.digitalmedialaws.com, 20 ottobre 2022.

[440] Secondo l'OMS, per telemedicina si intende: «*The delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities*». Organizzazione Mondiale della Sanità, *A health telematics policy in support of WHO's Health-For-All strategy for global health development: report of the WHO group consultation on health telematics*, 11-16 dicembre 1997, Ginevra, 1998

[441] Evoluzione e superamento della telemedicina è l'assistenza medica intelligente. CASONATO e PENASA, *Intelligenza artificiale e medicina del domani*, in G.F. FERRARI (a cura di), *Le smart cities al tempo della resilienza*, Milano, Mimesis, 2021

[442] Il riferimento delle linee guida è all'Accordo Stato-Regioni del 17 dicembre 2020 (Rep. Atti 215/CSR) "Indicazioni nazionali per l'erogazione di prestazioni in telemedicina".

[443] CAMPAGNA, *Linee guida per la Telemedicina: considerazioni alla luce dell'emergenza Covid-19*, in *Corti supreme e salute*, 2020, fasc. 3.

[444] «La sfida di oggi consiste, allora, nel rendere la digitalizzazione in ambito sanitario un processo organico, lungimirante e sicuro, promuovendo così l'efficienza del sistema e, con essa, l'effettività del diritto alla salute, superando le vulnerabilità della tecnica e minimizzandone i rischi, individuali e collettivi. Il Fse è, in un certo senso, l'emblema di questa sfida, quale elemento imprescindibile di innovazione ed efficienza delle attività diagnostiche e terapeutiche». Così si esprimeva qualche anno fa Antonello Soro. V. Audizione del Presidente del Garante per la protezione dei dati personali nell'ambito dell'indagine conoscitiva in materia di semplificazione dell'accesso dei cittadini ai servizi erogati dal Servizio Sanitario Nazionale - 25 maggio 2020 [doc web n. 9351203], in www.garanteprivacy.it. Che il fascicolo sanitario elettronico sia elemento per antonomasia della digitalizzazione della sanità è vero non soltanto per l'esperienza italiana. Negli Stati Uniti d'America, ad esempio, l'HITECH Act del 2009 ha previsto grandi investimenti proprio per la realizzazione di una rete

Possiamo osservare che le Linee guida per l'attuazione del FSE, adottate con decreto del Ministero della salute del 20 maggio 2022 e pubblicate a luglio dello stesso anno[445], prevedono, tra i vari requisiti obbligatori che dovrà avere il FSE per raggiungere gli obiettivi fissati nel PNRR, l'adozione di strumenti di *Advanced Analytics*, anche basati su tecniche di intelligenza artificiale per l'elaborazione dei dati clinici nel FSE.

La sanità digitale, in tutte le sue declinazioni, del resto, porta a riconsiderare anche il rapporto medico-paziente, non tanto per il suo attuale modo di intendersi, incentrato sull'alleanza terapeutica e senza più paternalismi, quanto per la modalità in cui deve estrinsecarsi, misurandosi con il nuovo apparato di strumenti tecnologici a disposizione del professionista e del paziente stesso, in grado di incidere sulla comunicazione e sulla relazione di cura[446].

Si può capire, dunque, che la digitalizzazione della sanità è un processo che riguarda da vicino la protezione dei dati personali, specialmente quelli relativi alla salute[447].

I benefici sul piano delle cure e dell'assistenza sanitaria sono evidenti, ma altrettanto evidente è la necessità di far fronte a un aumento dei rischi per la privacy delle persone[448]. E la particolare attenzione richiesta alla protezione dei dati sanitari deriva in buona parte proprio dall'ingresso delle tecnologie più nuove, che ha consentito il digitale in sanità[449]. Lo spirito che anima gli interventi dell'Unione e che percorre le enunciazioni di questi atti imprime a tale processo di innovazione europeo un segno di forte personalismo. Quando, il 26 gennaio 2022, la Commissione propose di definire una serie di principi che avrebbero fornito l'indirizzo per una trasformazione digitale sostenibile e basata sui valori, decise che avrebbe dovuto essere una transizione antropocentrica[450]. E quando presentò il testo della "Dichiarazione europea sui diritti e i principi digitali per il decennio digitale", prospettando

---

nazionale di cartelle cliniche elettroniche. V. O'HARROW, *The machinery behind health-care reform*, in *www.washingtonpost.com*, 16 maggio 2009.

[445] I documenti sono consultabili in *www.agid.gov.it.*

[446] FOGLIA, *La relazione di cura nell'era della comunicazione digitale*, in *MediaLaws*, 2020, fasc. 3,

[447] In arg. SARTORIS, *Sanità digitale e tutela dei dati personali*, in ADINOLFI e SIMONCINI (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, Edizioni Scientifiche Italiane, 2022

[448] V. GUPTA e DUTTA, *A Study on Data Protection and Privacy Issues in Healthcare Data*, in MANDAL *et al.* (a cura di), *Proceedings of International Conference on Advanced Computing Applications*, Berlino, Springer, 2022

[449] MARCHESE, *Profili civilistici dell'*information technology *in àmbito sanitario*, Napoli, Edizioni Scientifiche Italiane, 2021

[450] «Crediamo in una transizione digitale antropocentrica. Si tratta di chi vogliamo essere, in quanto europei». Così si esprimeva la Presidente Ursula von der Leyen, nel suo discorso a Sines, il 1º giugno 2021. V. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali*, del 26 gennaio 2022, COM(2022)

sia un quadro di riferimento per le persone sia una guida per le imprese e i responsabili politici, ebbe come obiettivo mettere al centro della trasformazione digitale le persone[451].

2. *L'*European Health Data Space

«Nel corso degli ultimi anni le tecnologie digitali hanno trasformato l'economia e la società, influenzando ogni settore di attività e la vita quotidiana di tutti i cittadini europei. I dati sono un elemento centrale di tale trasformazione, che non fa che cominciare. L'innovazione guidata dai dati genererà benefici enormi per i cittadini, ad esempio tramite il miglioramento della medicina personalizzata, le nuove soluzioni di mobilità e il suo contributo al Green Deal europeo». Così esordisce la Commissione europea, nella citata Comunicazione del 19 febbraio 2020, *Una strategia europea per i dati*, evidenziando i vantaggi della trasformazione tecnologica legata all'utilizzo dei dati e sottolineando come, sia nel settore pubblico che in quello privato, grazie ai dati, sia possibile disporre di strumenti per adottare decisioni migliori[452].

Questa strategia, delineata per orientare le misure politiche e gli investimenti a sostegno dell'economia dei dati per i successivi cinque anni, è stata presentata contemporaneamente alla Comunicazione *Plasmare il futuro digitale dell'Europa* e al Libro bianco sull'intelligenza artificiale, che illustra le modalità con cui la Commissione stessa sosterrà e promuoverà lo sviluppo e l'adozione dell'intelligenza artificiale nell'Unione.

Le azioni della strategia europea includono investimenti nei dati e un rafforzamento delle infrastrutture e delle capacità europee per l'*hosting*, l'elaborazione e l'utilizzo dei dati, l'interoperabilità[453].

Fra le azioni della strategia si annovera la promozione della realizzazione di *spazi*

[451] «Le persone sono al centro della trasformazione digitale nell'Unione europea. La tecnologia dovrebbe essere al servizio e andare a beneficio di tutti gli europei e metterli nelle condizioni di perseguire le loro aspirazioni, in tutta sicurezza e nel pieno rispetto dei loro diritti fondamentali». Così si apre il Capitolo 1 della *Dichiarazione sui diritti e i principi digitali per il decennio digitale*, COM(2022)

[452] «l'Europa – aggiunge – mira a sfruttare i vantaggi di un migliore utilizzo dei dati, compresi una maggiore produttività e mercati competitivi, ma anche miglioramenti in materia di salute e benessere, ambiente, amministrazione trasparente e servizi pubblici convenienti».

[453] In questo senso la Commissione si è proposta di promuovere sinergie tra il lavoro sulla federazione europea del *cloud* e le iniziative degli Stati membri quali GAIA-X. Quest'ultimo infatti è un progetto tedesco per la costruzione di un'infrastruttura europea incentrata sulla tecnologia *cloud*, al fine di trovare soluzioni modulari, per conservare e utilizzare al meglio grandi moli di dati, nei settori "Industria 4.0/PMI", "Salute", "Finanza", "Settore pubblico", "Vita intelligente", "Energia", "Mobilità" e "Agricoltura". Per quanto specificamente concerne il settore "Salute", nell'ecosistema digitale GAIA-X, si è ideato un modello basato su piattaforme intelligenti dedicate, tra l'altro, all'assistenza sanitaria preventiva mediante dispositivi indossabili, alla ricerca genomica sul cancro, al mondo dell'assistenza domiciliare, al rilevamento statistico della diffusione dei virus. G. RESTA e SIMONETTI, *La c.d. sovranità digitale e il progetto Gaia-X*, in *Contr. e impr. Eur*., 2022

comuni europei di dati in settori strategici. Tra questi, anche uno spazio comune europeo di dati sanitari, definito dalla Commissione «essenziale per compiere progressi nella prevenzione, nell'individuazione e nella cura delle malattie, nonché per compiere decisioni consapevoli e basate sulle evidenze al fine di migliorare l'accessibilità, l'efficacia e la sostenibilità dei sistemi di assistenza sanitaria».

Proprio con riguardo alla creazione dello *spazio comune europeo di dati sanitari*, nella menzionata Comunicazione, la Commissione ha preannunciato le direzioni in cui intende muoversi.

Da un lato, un intervento sul piano normativo, soprattutto per migliorare l'accessibilità e la portabilità dei dati sanitari. Questo può permettere di garantire vantaggi tanto per i singoli utenti dei servizi sanitari, che potranno godere di un'assistenza sanitaria più efficiente[454], quanto per le autorità sanitarie, che saranno in grado di decidere avendo a disposizione più informazioni. Dall'altro, un contributo sul versante più operativo, investendo sulle infrastrutture tecnologiche e sull'interoperabilità dei sistemi stessi. A tale proposito, sono stati promossi l'avvio e l'impiego dell'infrastruttura di servizi digitali per l'*eHealth* (*eHealth Digital Service Infrastructure*, eHDSI), per consentire lo scambio di fascicoli elettronici dei pazienti e di prescrizioni elettroniche tra gli Stati membri partecipanti.

Con tutto ciò, anche in questo documento, la Commissione ha dichiarato che la propria visione «scaturisce dai valori e dai diritti fondamentali europei e dalla convinzione che l'essere umano sia e debba rimanere l'elemento centrale».

Facendo seguito a questa Comunicazione della Commissione, il Parlamento europeo, a sua volta, ha approvato una Risoluzione sulla strategia europea per i dati, nella plenaria del 25 marzo 2021. Osservando come con la pandemia di Covid-19 si siano colti «il ruolo e la necessità di banche dati, di informazioni e di una condivisione di dati di alta qualità e in tempo reale, nonché le carenze nelle infrastrutture e nell'interoperabilità delle soluzioni tra gli Stati membri», ha affermato, tra le altre cose, l'essenzialità dell'iniziativa intesa a velocizzare la costituzione di uno spazio comune europeo dei dati sanitari[455].

Così, il primo spazio comune europeo dei dati lanciato dalla Commissione europea è stato proprio quello dei dati sanitari. Il 3 maggio 2022, la Commissione ha presentato la

[454] «I cittadini – aggiunge la Commissione – devono inoltre essere rassicurati in merito al fatto che, una volta che avranno dato il consenso alla condivisione dei loro dati, questi ultimi saranno usati dai sistemi sanitari in maniera etica, e il consenso potrà essere revocato in ogni momento».

[455] Risoluzione del Parlamento europeo del 25 marzo 2021 su una strategia europea per i dati (2020/2217(INI)) (2021/C 494/04).

proposta di Regolamento sull'*European Health Data Space* (**EHDS**)[456], dichiarando, in apertura della relazione che l'accompagna, come questo spazio costituisca una delle sue priorità nel settore della sanità e «sarà parte integrante della costruzione di un'Unione europea della salute»[457]. Il 5 marzo 2025 il **Regolamento sullo spazio europeo dei dati sanitari** è stato pubblicato ufficialmente nella Gazzetta ufficiale dell'Unione Europea ed è entrato in vigore il 26 marzo 2025, data che segna l'inizio della fase di transizione verso la piena attuazione. Sebbene la pubblicazione del regolamento sullo spazio europeo dei dati sanitari costituisca una tappa importante, va tenuto a mente che il suo effetto non sarà immediato. Si tratterà infatti di un processo graduale che si protrarrà nel tempo. Anche se diversi elementi possono essere anticipati dagli Stati membri su base volontaria, la maggior parte degli obblighi inizierà ad applicarsi soltanto a 4 anni dall'entrata in vigore del regolamento. Le tappe fondamentali verso una piena atuazione del Regolamento sono scandite come segue: Marzo 2027 rappresenta il termine entro il quale la Commissione deve adottare diversi atti di esecuzione fondamentali, con norme dettagliate per rendere il regolamento operativo; entro Marzo 2029 è prevista l'entrata in vigore delle principali parti del regolamento sullo spazio europeo dei dati sanitari, compreso, per l'uso primario, lo scambio del primo gruppo di categorie prioritarie di dati sanitari (profili sanitari sintetici dei pazienti, prescrizioni/dispensazioni elettroniche) in tutti gli Stati membri dell'UE. Anche le norme sull'uso secondario inizieranno ad applicarsi per la maggior parte delle categorie di dati (ad esempio i dati delle cartelle cliniche elettroniche). A Marzo 2031, per l'uso primario, lo scambio del secondo gruppo di categorie prioritarie di dati sanitari (immagini mediche, risultati di laboratorio e lettere di dimissione ospedaliera) dovrebbe essere operativo in tutti gli Stati membri dell'UE. Anche le norme sull'uso secondario inizieranno ad applicarsi per la parte restante delle categorie di dati (ad esempio i dati genomici). Infine a Marzo 2034: i paesi extra UE e le organizzazioni internazionali potranno chiedere di aderire a

[456] Proposta di Regolamento del Parlamento europeo e del Consiglio, del 3 maggio 2022, sullo spazio europeo dei dati sanitari COM(2022) 197 final. Come riportato nel comunicato stampa relativo (*Unione europea della salute: lo spazio europeo dei dati sanitari al servizio delle persone e della scienza*, del 3 maggio 2022, in *ec.europa.eu*), tale spazio consentirà alle persone di controllare e utilizzare i propri dati sanitari sia nel proprio paese che in altri Stati membri, promuoverà un mercato unico dei servizi e dei prodotti digitali in campo sanitario e costituirà un quadro normativo coerente, affidabile ed efficiente per l'uso di tali dati nelle attività di ricerca, innovazione, elaborazione delle politiche e regolamentazione, sempre nel rispetto degli elevati standard di protezione dei dati dell'Unione

[457] Definito dal Vicepresidente della Commissione europea, Margaritis Schinas, come un 'nuovo inizio' per la politica dell'Unione in materia di salute digitale, lo spazio europeo dei dati sanitari costituisce – per usare le parole di Stella Kyriakides, Commissaria per la Salute e la sicurezza alimentare – un pilastro dell'Unione europea della salute, nonché un cambio di paradigma fondamentale per la trasformazione digitale delle cure nell'UE. «Esso mette al centro di tutto i cittadini e darà loro il pieno controllo sui propri dati, affinché ottengano migliori cure sanitarie in tutta l'UE».

HealthData@EU per l'uso secondario.

Attraverso lo spazio europeo dei dati sanitari l'Unione mira a garantire l'accesso immediato e semplice da parte di ciascuno ai propri dati in formato elettronico, un'agevole loro condivisione con i professionisti sanitari – anche in un altro Stato membro – nonché un controllo sui dati stessi, in una cornice di interoperabilità e sicurezza.

Il Regolamento sull'European Health Data Space (EHDS), che si inserisce nel filone del Data Governance Act, di cui è un importante e strategico filone verticale, ha l'obiettivo di rafforzare l'accesso e il controllo delle persone fisiche sui propri dati sanitari elettronici nell'ambito dell'assistenza sanitaria. Inoltre, mira a favorire l'utilizzo di tali dati per finalità di interesse collettivo come la ricerca, l'innovazione, la definizione di politiche sanitarie, la preparazione e la risposta alle minacce per la salute (incluse la prevenzione e la gestione di future pandemie), la sicurezza dei pazienti, la medicina personalizzata, le statistiche ufficiali e le attività normative. Parallelamente, il Regolamento punta a migliorare il funzionamento del mercato interno stabilendo un quadro giuridico e tecnico uniforme per lo sviluppo, la commercializzazione e l'utilizzo dei sistemi di cartelle cliniche elettroniche (EHR systems), in linea con i valori europei. L'EHDS rappresenterà un elemento chiave per la costruzione di un'Unione europea della Salute più forte e resiliente. A tal fine, il Regolamento stabilisce regole comuni, standard, infrastrutture e un quadro di governance per facilitare l'accesso ai dati sanitari elettronici, sia per il loro utilizzo primario (nell'erogazione delle cure) sia per usi secondari (come ricerca e innovazione).

Il Regolamento relativo all'EHDS è strutturato in tre sezioni principali, ciascuna indirizzata a specifici destinatari:

• Capitolo II – Uso primario dei dati: rafforza i diritti dei pazienti e definisce l'infrastruttura tecnica necessaria per garantirne l'attuazione. Gli Stati membri sono tenuti a predisporre le infrastrutture necessarie a livello nazionale e ad assicurare che gli operatori sanitari siano connessi al sistema.

• Capitolo III – Sistemi di cartella clinica elettronica (EHR): riguarda i produttori e gli operatori economici che immettono sul mercato questi sistemi. Introduce requisiti in materia di interoperabilità e tracciabilità, oltre a stabilire meccanismi di sorveglianza del mercato, demandando agli Stati membri la designazione delle autorità competenti per il controllo e la supervisione del settore.

• Capitolo IV – Uso secondario dei dati: disciplina l'accesso e l'utilizzo dei dati sanitari da parte dei detentori e degli utenti di tali informazioni. Impone agli enti che gestiscono i dati

l’obbligo di renderli disponibili e definisce le modalità di utilizzo per la ricerca e altre finalità. Inoltre, prevede l’istituzione degli organismi di accesso ai dati sanitari (Health Data Access Bodies – HDABs) e l’infrastruttura necessaria al loro funzionamento.
Inoltre è prevista la possibilità di partecipazione al sistema unico di dati europei da parte di Paesi terzi. In questo caso la Commissione verifica che le misure legali, organizzative, operative, semantiche, tecniche e di cybersicurezza di un Paese terzo siano equivalenti a quelle applicabili negli Stati membri. Se il punto di contatto nazionale di tale Paese supera questa verifica, la Commissione può adottare un atto di esecuzione per connetterlo a MyHealth@EU, con il coinvolgimento degli Stati membri nel processo decisionale.
Una volta collegato, il Paese terzo potrà scambiare i sommari dei pazienti e altre categorie prioritarie con gli Stati membri, permettendo ai professionisti sanitari di accedere alle informazioni dei pazienti UE in caso di necessità di cure. Allo stesso modo, le informazioni sanitarie dei cittadini di quel Paese potranno essere condivise con l’UE.

La Commissione manterrà un elenco pubblico dei punti di contatto nazionali dei Paesi terzi connessi a MyHealth@EU, tuttavia, questi non saranno membri del gruppo direttivo, ma potranno partecipare come osservatori. Le decisioni operative sulla gestione dell’infrastruttura transfrontaliera resteranno di competenza esclusiva degli Stati membri.

Parallelamente, il Regolamento punta a migliorare il funzionamento del mercato interno stabilendo un quadro giuridico e tecnico uniforme per lo sviluppo, la commercializzazione e l’utilizzo dei sistemi di cartelle cliniche elettroniche (EHR systems), in linea con i valori europei. L’EHDS rappresenterà un elemento chiave per la costruzione di un’Unione europea della Salute più forte e resiliente. A tal fine, il Regolamento stabilisce regole comuni, standard, infrastrutture e un quadro di governance per facilitare l’accesso ai dati sanitari elettronici, sia per il loro utilizzo primario (nell’erogazione delle cure) sia per usi secondari (come ricerca e innovazione).
Il regolamento EHDS definisce chiaramente la titolarità e la gestione dei dati sanitari. **I cittadini restano titolari dei propri dati personali**, con il diritto di accedere gratuitamente ai propri dati sanitari elettronici, correggerli, aggiungere informazioni, limitarne l'accesso e conoscere chi li utilizza e per quali scopi.
Accanto ai cittadini, il regolamento identifica i cosiddetti **"health data holder"** (titolari di dati sanitari), ovvero soggetti pubblici e privati che, per obbligo o diritto, trattano dati sanitari personali o sono in grado di rendere disponibili dati non personali. In questa

categoria rientrano ospedali e strutture sanitarie, enti pubblici sanitari, aziende farmaceutiche, assicurazioni sanitarie, sviluppatori di prodotti e servizi sanitari e centri di ricerca.

Questa distinzione tra titolari dei dati (i cittadini) e detentori dei dati (gli enti che li gestiscono) è fondamentale per comprendere le dinamiche di potere e responsabilità nel nuovo quadro normativo europeo. Stando alle previsioni, l'EHDS dovrebbe: generare risparmi per 11 miliardi di euro nel prossimo decennio migliorando l'accessibilità dei dati; accrescere l'efficienza dei servizi sanitari in tutti gli Stati membri dell'UE; favorire un'espansione del 20-30% del comparto della sanità digitale; favorire lo sviluppo delle politiche e la ricerca scientifica**;** portare a migliori risultati in campo sanitario per i cittadini europei.

3. L' Ecosistema dei Dati Sanitari (EDS)

Per allinearsi al regolamento europeo, l'Italia ha istituito l'Ecosistema dei Dati Sanitari (EDS) con il Decreto Ministeriale 31 dicembre 2024 n. 53, pubblicato in Gazzetta Ufficiale il 5 marzo 2025 e che sarà operativo entro il 2026. Si tratta di un sistema digitale federato che consente la raccolta, gestione e analisi dei dati sanitari mantenendo i dati clinici nei sistemi locali dove sono generati, ma garantendo al contempo l'interoperabilità e l'accesso controllato su base nazionale. Questo approccio supera il modello centralizzato precedente, raccogliendo i dati in formato strutturato secondo standard europei. L'innovazione principale dell'EDS sta nel suo approccio integrato, che potenzia il Fascicolo Sanitario Elettronico (FSE) già esistente, rafforzando la sicurezza e la trasparenza dei dati, il controllo da parte dei cittadini sui propri dati, l'interoperabilità tra sistemi diversi e, in ultima analisi, la qualità del Servizio Sanitario Nazionale e i servizi per pazienti e professionisti. Secondo quanto stabilito dall'articolo 3 del Decreto Ministeriale sull'EDS, l'ecosistema si alimenta con i dati del Fascicolo Sanitario Elettronico (FSE), che includono informazioni anagrafiche e amministrative dei pazienti (ad esempio, esenzioni per reddito o patologia, contatti e delegati), oltre a una vasta gamma di documenti sanitari: referti, lettere di dimissione, verbali di pronto soccorso, prescrizioni farmaceutiche e specialistiche, cartelle cliniche, registri delle vaccinazioni e dell'erogazione di farmaci, prestazioni specialistiche e annotazioni personali dell'assistito. Inoltre, vengono integrati i dati disponibili tramite il Sistema Tessera Sanitaria. Queste informazioni possono essere consultate ed elaborate

all’interno dell’EDS attraverso operazioni di ricerca, estrazione e analisi, con la possibilità di sviluppare strumenti innovativi come il Dossier Farmaceutico. Quest’ultimo, introdotto come novità normativa, raccoglie dati dettagliati sulle prescrizioni e l’erogazione dei farmaci, compresi i piani terapeutici e le modalità di somministrazione, contribuendo a una gestione più efficace delle terapie.

Le informazioni sottoposte a oscuramento nel Fascicolo Sanitario Elettronico non vengono trasferite all'Ecosistema Dati Sanitari. In conformità con la legislazione corrente sulla tutela dei dati personali, la titolarità del trattamento è attribuita alle regioni e alle province autonome, mentre l'Agenzia nazionale per i servizi sanitari regionali (Agenas) assume il ruolo di responsabile del trattamento su designazione delle stesse.

Rivoluzionario è anche l’approccio all’accesso all’EDS, regolato in base alle finalità specifiche per cui i dati vengono utilizzati:

• Per la cura dei pazienti (art. 13 del DM EDS), possono accedere le strutture sanitarie e socio-sanitarie, i medici convenzionati e altri professionisti sanitari coinvolti nell’assistenza, escludendo però soggetti come periti, compagnie assicurative, datori di lavoro e personale medico-legale;

• per la prevenzione (art. 14), l’accesso è consentito agli enti del Servizio Sanitario Nazionale (SSN) e ai servizi sociosanitari regionali, attraverso i dipartimenti competenti in materia di prevenzione;

• per la profilassi internazionale (art. 15), i dati possono essere consultati dagli uffici del Ministero della Salute responsabili della sanità marittima, aerea e di frontiera, nel rispetto delle normative sanitarie internazionali;

• per il governo del sistema sanitario (art. 16), l’accesso è riservato agli uffici del Ministero della Salute, Agenas e alle autorità regionali competenti;

• per la ricerca scientifica (art. 17), l’EDS rappresenta un’opportunità significativa, con un’apertura regolamentata che potrebbe contribuire a superare molte delle attuali criticità del settore.

Questo sistema innovativo punta a trasformare la gestione dei dati sanitari in Italia, migliorando la qualità dell’assistenza e promuovendo un utilizzo più efficiente e sicuro delle informazioni. Il decreto stabilisce che l’accesso ai dati anonimizzati dell’EDS è riservato al personale qualificato del Ministero della Salute, di Agenas e delle regioni e province autonome, attraverso appositi servizi di estrazione, ma introduce anche un’importante apertura verso il settore privato, consentendo anche a enti pubblici e privati impegnati nella

ricerca medica, biomedica ed epidemiologica di richiedere ad Agenas l'estrazione di dati anonimizzati. Tale richiesta dovrà essere accompagnata da un progetto di ricerca conforme agli standard metodologici, etici e, se applicabile, alle norme deontologiche previste per il trattamento dei dati a fini statistici e di ricerca scientifica.

La governance dell'EDS è affidata pertanto a un sistema articolato che coinvolge il Ministero della Salute, il Ministero dell'Economia e delle Finanze, il Dipartimento per la trasformazione digitale, l'Agenzia per i servizi sanitari regionali (Agenas) e le Regioni e Province autonome. Questo sistema di governance mira ad assicurare responsabilità chiare e un sistema di autorizzazioni rigoroso per l'accesso ai dati, bilanciando le esigenze di efficienza con quelle di sicurezza e rispetto della privacy.

L'EDS si inserisce armoniosamente nel quadro della legge sulla privacy italiana, rispettando sia il GDPR sia il Codice della Privacy nazionale (istituito con il decreto legislativo n.196 del 2003), con particolare riferimento all'articolo 110, che disciplina specificamente il trattamento dei dati sanitari. È stato progettato per garantire massima sicurezza, trasparenza e tutela della privacy in ogni fase del trattamento dei dati sanitari, richiedendo un consenso libero, specifico, informato, inequivocabile ed esplicito da parte dell'interessato per ciascuna finalità, con la possibilità di revoca in qualsiasi momento.

L'introduzione dell'EHDS e del Data Act comporta una profonda ridefinizione delle dinamiche tra soggetti pubblici e privati nella gestione dei dati sanitari, creando tensioni strutturali tra interessi diversi e talvolta contrastanti.

Da un lato, gli interessi pubblici puntano a massimizzare la disponibilità di dati di qualità per la ricerca e l'innovazione sanitaria, mantenendo la fiducia dei cittadini e la tutela della privacy. Dall'altro, per le aziende private i dati rappresentano un asset strategico e competitivo. L'obbligo di condividere dati per usi secondari può quindi entrare in tensione con la protezione della proprietà intellettuale e i modelli di business basati sull'esclusività dei dati. Questa tensione si manifesta concretamente nella necessità, per le aziende, di rivedere profondamente le proprie strategie commerciali. La condivisione obbligatoria dei dati impone infatti una valutazione attenta dei rischi e dei costi associati, un rafforzamento delle misure tecniche e organizzative per tutelare la posizione competitiva, la modifica di prodotti e servizi per adeguarsi ai requisiti di interoperabilità e l'aggiornamento dei modelli contrattuali per garantire conformità alle nuove regole. Queste trasformazioni possono portare a quella che alcuni esperti definiscono una "ricostruzione forzata" dei modelli di business tradizionali, con particolare impatto sulle aziende che hanno costruito il proprio

valore sulla proprietà esclusiva dei dati e che ora devono ripensare le proprie strategie in un contesto di maggiore apertura e condivisione.

A complicare ulteriormente il quadro vi è la persistente frammentazione normativa tra gli Stati membri dell'Unione Europea. Nonostante gli sforzi di armonizzazione, le differenze nell'implementazione delle normative e nelle prassi amministrative possono creare incertezze e aumentare i costi di compliance, soprattutto per i piccoli operatori e per le aziende attive in più paesi.

Per quanto riguarda i produttori di sistemi EHR, dal 26 marzo 2029 questi potranno immettere sul mercato solo sistemi conformi alle specifiche comuni per la gestione dei primi dati prioritari, mentre dal 26 marzo 2031 l'obbligo si estenderà anche ai sistemi che trattano le altre categorie di dati. I detentori di dati sanitari dovranno inviare agli organismi di accesso ai dati sanitari (HDAB) la descrizione dei dataset detenuti entro il 26 marzo 2029 o 2031, a seconda della categoria di appartenenza ai sensi dell'articolo 51, e potranno essere obbligati a rendere disponibili i dati in seguito a specifiche autorizzazioni.

4. *Dati relativi alla salute e intelligenza artificiale*

Il comunicato stampa del Garante per la protezione dei dati personali, del 18 gennaio 2023, riferiva della delibera della Regione Veneto, per cui «non sarebbero più i medici di medicina generale a scegliere la classe di priorità della prestazione richiesta per il paziente, ma un sistema basato sull'intelligenza artificiale. Sarebbe in sostanza un algoritmo a stabilire i tempi di attesa per le prestazioni prescritte»[458].

Appena un mese prima, l'Autorità garante aveva sanzionato tre Asl del Friuli Venezia Giulia per aver posto in essere trattamenti di dati personali di pazienti, specialmente dati sanitari, presenti nelle banche dati aziendali, a fini di stratificazione statistica e di medicina d'iniziativa, in violazione degli artt. 5, par. 1, lett. *a*, 9, 14 e 35 del Regolamento generale sulla protezione dei dati (c.d. GDPR) e dell'art. 2 *sexies* del Codice della privacy[459]. Per il Garante mancava un'idonea base giuridica del trattamento, non erano state fornite agli

[458] Garante per la protezione dei dati personali, Comunicato stampa del 18 gennaio 2023, *Sanità: liste di attesa, Garante privacy avvia istruttoria su algoritmo Regione Veneto*, [doc web n. 9845106], consultabile in *www.garanteprivacy.it*. «Di fronte ad un possibile trattamento su larga scala di dati particolarmente delicati come quelli sulla salute, che coinvolgerebbe peraltro un numero rilevante di pazienti, il Garante ha deciso di avviare un'istruttoria».

[459] Si tratta dei provvedimenti dell'Autorità garante nn. 415, 416 e 417, del 15 dicembre 2022 [doc web nn. 9844989, 9845156, 9845312]. La sanzione amministrativa pecuniaria irrogata ammonta a una somma pari a 55.000 euro.

interessati le informazioni necessarie e non era stata effettuata preliminarmente la valutazione d'impatto[460]. Nel trattamento dei dati per la classificazione degli assistiti, svolta avendo riguardo al rischio di sviluppare complicanze in caso di infezione da Covid-19, si faceva uso dell'algoritmo L'utilizzo in ambito sanitario dell'intelligenza artificiale o di algoritmi[461] ha davvero molte applicazioni. Lungi dal limitarsi alla programmazione della sanità o alla medicina predittiva, trova impiego anche, ad esempio, a fini diagnostici, nel percorso di cura oppure a scopi terapeutici.

Numerosi sono i vantaggi che derivano da queste applicazioni pratiche e numerosi anche i rischi connessi. Perciò si avverte l'esigenza di un diritto che sappia trovare soluzioni, coniugando l'innovazione tecnologica e l'interesse della collettività con le libertà e i diritti fondamentali delle persone.

Anche con riferimento al contesto medico, buona parte delle riflessioni in materia si è concentrata sul problema della responsabilità, che qui è spesso legato all'impiego del robot da parte del professionista[462].

Altro e differente ordine di problemi è invece quello inerente al trattamento di dati personali realizzato con l'intelligenza artificiale, in ambito sanitario, il quale si deve rapportare alla specificità del dato attinente alla condizione di salute[463].

Il funzionamento di un sistema di intelligenza artificiale, infatti, implica il trattamento algoritmico di dati. Se il sistema è rivolto o connesso alla persona, il trattamento avrà ad oggetto dati personali e, se si tratta di una tecnologia per la salute, oggetto del trattamento saranno anche dati sanitari[464].

---

[460] Peraltro, tutti e tre i provvedimenti sono stati impugnati – dinanzi al Tribunale rispettivamente di Pordenone, Udine e Trieste – e il giudice ne ha disposto in via cautelare la sospensione dell'efficacia esecutiva

[461] Spesso si usano le parole 'intelligenza artificiale' e 'algoritmo' come sinonimi, ma a rigore indicano cose diverse. La nozione comune e generale di 'algoritmo', come sequenza finita di istruzioni, ben definite e non ambigue, tali da poter essere eseguite meccanicamente e produrre un determinato risultato, «quando è applicata a sistemi tecnologici, è ineludibilmente collegata al concetto di automazione ossia a sistemi di azione e controllo idonei a ridurre l'intervento umano. […] Cosa diversa è l'intelligenza artificiale», laddove «l'algoritmo contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole *software* e i parametri preimpostati […] ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico». Questa distinzione, che non è priva di ricadute sul piano giuridico, è stata offerta dal Consiglio di Stato in una sentenza pronunciata con riguardo alla valutazione dell'offerta tecnica in una gara di appalto, avente ad oggetto la fornitura di pacemaker. Di un dispositivo, quindi, che funziona attraverso il trattamento algoritmico di dati relativi alla salute. Cons. Stato, 25.11.2021, n. 7891, in *MediaLaws*, 2022, fasc. 3

[462] C. PERLINGIERI, *Responsabilità civile e robotica medica*, in *Tecnologie e diritto*, 2020, 161 ss. Cfr. i contributi, pubblicati in *Resp. med.*, di COLARUOTOLO, *Intelligenza artificiale e responsabilità medica: novità, continuità e criticità*, 2022

[463] CIANCIMINO, *AI Based Decision-Making Process in Healthcare*, in *Journal of European Consumer and Market Law*, vol. 11, n. 5, 2022

[464] Va tenuto presente che per i sistemi di intelligenza artificiale utilizzati nel contesto sanitario, qualora rientrino nella categoria di 'dispositivo medico', trova applicazione il reg. Ue n. 745 del 2017

Il Regolamento sull'intelligenza artificiale, Regolamento sull'Intelligenza Artificiale (AI Act) del 13 giugno 2024 (Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio) è entrato in vigore il 1 agosto 2024 e stabilisce regole armonizzate sull'intelligenza artificiale (noto anche come Regolamento sull'intelligenza artificiale o AI Act). L'obiettivo del Regolamento è creare un quadro normativo orizzontale armonizzato per lo sviluppo, l'introduzione nel mercato dell'Unione europea e l'utilizzo di prodotti e servizi di intelligenza artificiale (AI), con particolare attenzione alla gestione dei rischi per salute, sicurezza e diritti fondamentali. Il Regolamento non è pensato per l'introduzione di basi giuridiche per il trattamento di dati personali e al considerando 41 espressamente lo dichiara[465]. Come chiarito anche nella relazione della Commissione, esso «non pregiudica il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679) e la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (direttiva (UE) 2016/680) e li integra con una serie di regole armonizzate applicabili alla progettazione, allo sviluppo e all'utilizzo di determinati sistemi di IA ad alto rischio»[466].

Guarda alla strategia europea per i dati, per definire una cornice normativa tale da permettere la realizzazione di sistemi di intelligenza artificiale che operino in modo sicuro e nel rispetto dei principi del diritto dell'Unione.

In particolare, nell'impostazione la strategia per i dati può essere utile per contrastare il rischio di discriminazione algoritmica, insito negli usi di queste tecnologie[467]. Così, nella relazione che accompagna il Regolamento, si evidenzia come la disciplina integri il diritto dell'Unione in materia di non discriminazione «con requisiti specifici che mirano a ridurre al minimo il rischio di discriminazione algoritmica, in particolare in relazione alla progettazione e alla qualità dei set di dati utilizzati per lo sviluppo dei sistemi di IA».

Il rinvio operato è all'*European Health Data Space*. Come si legge al considerando 45

[465] Considerando 41: «Il presente regolamento non dovrebbe essere inteso come un fondamento giuridico per il trattamento dei dati personali, comprese, ove opportuno, categorie particolari di dati personali».

[466] Secondo il par. 5 dell'art. 10, peraltro, i fornitori di sistemi di intelligenza artificiale ad alto rischio 'possono' trattare dati sensibili, compresi quindi i dati relativi alla salute, nella misura in cui ciò sia strettamente necessario per garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi stessi, fatte salve in ogni caso le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche, come ad esempio la pseudonimizzazione. La previsione è coerente con il considerando 45, per cui,
«ai fini dello sviluppo di sistemi di IA ad alto rischio, è opportuno concedere ad alcuni soggetti, come fornitori, organismi notificati e altre entità pertinenti, quali i poli dell'innovazione digitale, le strutture di prova e sperimentazione e i ricercatori, l'accesso a set di dati di elevata qualità e la possibilità di utilizzarli nell'ambito dei rispettivi settori di attività connessi al presente regolamento». La disposizione, che forse meriterebbe un raccordo migliore con la disciplina in materia di protezione dei dati personali, non esclude l'applicazione delle norme del Regolamento generale sulla protezione dei dati, in particolare l'art. 9.

[467] In arg. FALLETTI, *Discriminazione algoritmica. Una prospettiva comparata*, Torino, Giappichelli, 2022

della proposta sull'intelligenza artificiale, «gli spazi comuni europei di dati istituiti dalla Commissione e l'agevolazione della condivisione dei dati tra imprese e con i governi, nell'interesse pubblico, saranno fondamentali per fornire un accesso affidabile, responsabile e non discriminatorio a dati di elevata qualità a fini di addestramento, convalida e prova dei sistemi di IA. Ad esempio, per quanto riguarda la salute, lo spazio europeo di dati sanitari agevolerà l'accesso non discriminatorio ai dati sanitari e l'addestramento di algoritmi di intelligenza artificiale su tali set di dati in modo sicuro, tempestivo, trasparente, affidabile e tale da tutelare la vita privata, nonché con un'adeguata governance istituzionale».

Si può notare l'intreccio sistematico e teleologico delle disposizioni contenute in entrambe le proposte, che si intende tradurre nei contenuti del futuro diritto dell'Unione, in un continuo dialogo con il diritto già vigente. Gli innesti nel tessuto normativo eurounitario e – conseguentemente – nazionale tendono a costruire le strutture giuridiche dell'evoluzione tecnologica ed economica degli Stati membri, in cui il ruolo dei dati si fa sempre più pregnante.

Il Regolamento generale sulla protezione dei dati, pur non dettando una disciplina speciale sul trattamento di dati personali operato da sistemi di intelligenza artificiale, non manca di affrontare alcuni aspetti legati al funzionamento di queste tecnologie, che si avvalgono del trattamento automatizzato di dati personali, e lo fa riprendendo e aggiornando regole che già contemplava la Direttiva madre, del 1995, all'art. 15.

È il tema della c.d. 'decisione automatizzata'[468], ascrivibile ai sistemi di intelligenza artificiale, cui è dedicato l'art. 22 del Regolamento.

Preme osservare, sin da subito, il variegato atteggiarsi del consenso in questo frangente, in cui si intersecano, pur mantenendo una loro logica autonomia, diverse fattispecie: il consenso dell'interessato al trattamento dei dati personali; il consenso esplicito al trattamento di dati sensibili o relativi alla salute, per la specifica finalità; il consenso alla decisione automatizzata; il consenso al trattamento sanitario, se la decisione sia inerente a una relazione di cura fra medico e paziente; e ancora, eventualmente, il consenso negoziale, qualora, ad esempio, vi sia la stipula di un contratto, come quello con il professionista o con una struttura sanitaria.

Al par. 1 dell'art. 22 è sancito il diritto di non essere sottoposto a una decisione basata

[468] P. STANZIONE, *Decisioni automatizzate e ruolo della privacy*, in SALANITRO (a cura di), *SMART la persona e l'infosfera*, Pisa, Pacini, 2022

unicamente sul trattamento automatizzato[469], includendo espressamente una delle procedure di più frequente applicazione, ossia la 'profilazione[470]'.

Collocato, nell'impianto del Regolamento, alla fine dei diritti riconosciuti all'interessato, dal Capo III, insieme al diritto di opposizione al trattamento di dati personali, nella sezione quarta, può rappresentare, con quest'ultimo, uno strumento di valorizzazione del consenso dell'individuo – come dissenso o come assenso, ai sensi del par. 2 – nella misura in cui possa tradursi in una manifestazione di volontà della persona.

Coerentemente, all'art. 13, par. 2, lett. *f,* il Regolamento dispone che tra le informazioni che il titolare del trattamento fornisce all'interessato, in caso di raccolta presso questi di dati che lo riguardano, oltre a quelle di base, indicate al par. 1 dell'art. 13, vi sia, come informazione necessaria per garantire un trattamento corretto e trasparente, quella relativa all'«esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato»[471].

Se questo sia effettivamente un diritto oppure se invece sia da considerare un divieto è discusso[999]. La posizione del Gruppo di lavoro "Articolo 29", espressa nelle Linee guida sul processo decisionale automatizzato adottate, nella versione revisionata, il 6 febbraio 2018, è orientata verso questa seconda interpretazione, nel senso di un divieto generale[472].

Peraltro, pure è discusso se dalle disposizioni del Regolamento sia ricavabile un diritto alla spiegazione, un modo per 'aprire' la *black box.*

Dall'analisi dell'art. 22, tuttavia, sembra emergere anche un'altra questione, attinente alla

[469]Previsioni di tenore analogo sono contenute in altri atti di diritto derivato dell'Unione, come all'art. 11 della Direttiva n. 680 del 2016 o agli artt. 24 e 77 del Regolamento n. 1725 del 2018. Sul piano del diritto internazionale, la disposizione trova corrispondenze nell'art. 9 della c.d. Convenzione 108 – nella versione modernizzata del 2018 – e nella Raccomandazione del Consiglio d'Europa, adottata dal Comitato dei Ministri il 21 novembre 2020, '*Protection of individuals with regard to automatic processing of personal data in the context of profiling - Recommendation CM/Rec(2021)8 (2021)*', che prende il posto della precedente Raccomandazione del 2010.

[470] Con ciò intendendosi, secondo l'art. 4, n. 4), del Regolamento, «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica». V. anche il considerando 71.

[471] Analoga disposizione è prevista all'art. 14, par. 2, lett. *g*, del Regolamento, relativamente alle informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato, e all'art. 15, par. 1, lett. *h*, in relazione alle informazioni cui l'interessato ha diritto di accedere, insieme ai propri dati personali. Cfr. MESSINETTI, *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, cit., 861 ss

[472] Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 6 febbraio 2018, WP 251 rev.01, 25.

possibilità per il soggetto di autodeterminarsi dinanzi alla decisione algoritmica. Una questione tanto più critica, quanto più sensibili siano i dati oggetto del trattamento automatizzato.

L'operatività dell'istituto è circoscritta dall'art. 22, par. 1, che, per la sua integrazione, richiede la sussistenza di una pluralità di elementi inerenti alla 'decisione'.

Così, perché possa dirsi che l'interessato abbia diritto a non esservi sottoposto, la decisione dev'essere basata su un trattamento di dati automatizzato *unicamente* – cioè, se vi è un coinvolgimento umano nel processo decisionale, la fattispecie esce dell'ambito applicativo dell'art. 22[473] – e deve produrre effetti giuridici che riguardano l'interessato o incidere in modo analogo significativamente sulla sua persona[474].

Però, poiché si ritiene opportuno permettere l'adozione di decisioni sulla base di tale trattamento, come espresso al considerando 71 del Regolamento, l'art. 22, par. 2, deroga a quanto disposto nel par. 1 in tre ipotesi, cioè quando la decisione: «a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato».

I tre casi, in cui il diritto di non (o il divieto di) essere sottoposto alla 'decisione automatizzata' non trova applicazione, sono riconducibili rispettivamente all'ambito contrattuale, a quello generale – o forse di interesse collettivo o superindividuale – dell'autorizzazione normativa e a quello della volontà del soggetto. In tutti e tre i casi la deroga viene circostanziata. Nel primo, infatti, deve rispondere al principio di necessità, com'è anche, del resto, per la condizione di liceità del trattamento *ex* art. 6, par. 1, lett. *b*; nel secondo caso, si specifica che la fonte giuridica che provvede all'autorizzazione deve

[473] Ha reso un contributo interpretativo il Gruppo di lavoro "Articolo 29", secondo cui, «per aversi un coinvolgimento umano, il titolare del trattamento deve garantire che qualsiasi controllo della decisione sia significativo e non costituisca un semplice gesto simbolico. Il controllo dovrebbe essere effettuato da una persona che dispone dell'autorità e della competenza per modificare la decisione. Nel contesto dell'analisi, tale persona dovrebbe prendere in considerazione tutti i dati pertinenti». Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 23.

[474] Per agevolare l'interpretazione, il considerando 71 esemplifica facendo riferimento al «rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani». Perché un trattamento di dati sia considerato incidente in maniera significativa su una persona, secondo il Gruppo di lavoro "Articolo 29", «i suoi effetti devono essere sufficientemente rilevanti o importanti da meritare attenzione», ossia la decisione deve poter «incidere in maniera significativa sulle circostanze, sul comportamento o sulle scelte dell'interessato; avere un impatto prolungato o permanente sull'interessato; o nel caso più estremo, portare all'esclusione o alla discriminazione di persone». *Ivi*, 24

precisare idonee misure che tutelino i diritti, le libertà e gli interessi legittimi dell'interessato; mentre, nel terzo, il riferimento è al consenso dell'interessato, qualificato come esplicito.

Tale qualificazione – di consenso *esplicito* – come già si è notato, ricorre anche per altri 'consensi', nel Regolamento, laddove, per via dei rischi gravi legati al trattamento dei dati, si è inteso apprestare un livello di controllo individuale elevato.

Quando ricorre la deroga basata sul contratto o sul consenso – cioè quando non si applica il par. 1 dell'art. 22, ma non per autorizzazione normativa – il Regolamento impone al titolare del trattamento, ai sensi del par. 3, di attuare «misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato» e specifica che, fra questi diritti, devono essere senz'altro tutelati quelli «di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione». Ciò significa che l'interessato può sempre chiedere una revisione della decisione basata unicamente sul trattamento automatizzato, a meno che quest'ultima non sia stata autorizzata normativamente. In questa ipotesi, potrebbe comunque ricevere una tutela analoga, dal momento che la lett. *b* del par. 2 richiede esplicitamente di contemplare "misure adeguate" a ciò[475].

Il par. 4 dell'art. 22 è dedicato, invece, alla decisione automatizzata basata su dati personali appartenenti alle categorie particolari di cui all'art. 9, quindi anche sui dati relativi alla salute[476].

5. *Il problema della decisione automatizzata basata sul trattamento di dati sanitari*

La regola dettata dall'art. 22, par. 4, è un divieto[477]: «Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1».

La previsione si stringe al generale divieto di trattamento di dati personali appartenenti alle categorie particolari e si salda quindi all'interpretazione data al testo dell'art. 9.

Fondare una decisione algoritmica sul trattamento automatizzato di dati sensibili può mettere a repentaglio la tutela delle libertà e dei diritti fondamentali della persona, considerati anche la sfuggevolezza della modalità in cui vengono prese in considerazione queste informazioni e gli ambiti della vita cui la decisione può afferire.

---

[475] BYGRAVE, *op. ult. cit.*

[476] C. PERLINGIERI, *eHealth and Data,* cit., 135. Cfr. A.G. GRASSO, *GDPR e intelligenza artificiale: limiti al processo decisionale automatico in sanità*, cit., 183 ss.

[477] La formulazione è, in realtà, involuta e sembra voler derogare alla deroga più che proibire. Il riferimento al par. 2, però, può interpretarsi anche come indicazione logica di prevalenza del divieto sulle eccezioni. BYGRAVE, *op. ult. cit.*, 539. Cfr. LAGIOIA, SARTOR e SIMONCINI, *op. cit*., 385

Non come divieto, ma in termini precauzionali si orienta il considerando 71, per cui «il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni»[478].

E così il divieto viene mitigato dalla previsione di ipotesi a loro volta eccezionali. La decisione automatizzata non si basa sui dati sensibili «a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato».

Il rinvio è di nuovo all'art. 9 – nel dettaglio, al par. 2 – ma stavolta le eccezioni previste al divieto sono solo due, ossia il consenso esplicito dell'interessato e la necessità del trattamento per motivi di interesse pubblico rilevante[479].

Considerato che la decisione automatizzata ha conseguenze sulla persona e sui suoi diritti, il rischio correlato può essere maggiore se ad essere trattati sono dati appartenenti alle categorie particolari anziché dati neutri e, al contempo, può emergere una più percepita esigenza di autodeterminazione del soggetto[480]. Le deroghe al divieto, in questo caso, si riducono quindi a due.

Pertanto l'interessato può essere sottoposto a una decisione basata unicamente sul trattamento automatizzato di dati personali, compresi i dati relativi alla salute, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, come, ad esempio, una decisione che riguardi la prognosi, la diagnosi o il trattamento[481], se esprime un consenso esplicito al trattamento dei propri dati sensibili oppure se il trattamento è necessario per motivi di interesse pubblico rilevante.

Il ricorrere delle fattispecie di cui all'art. 9, par. 2, lett. *a* e *g*, peraltro, sembra non

[478] A tal proposito, pare opportuno osservare che la *Recommendation on the Protection and Use of Health-Related Data*, adottata il 6 novembre 2019, in seno alle Nazioni Unite, al capitolo XV, punto 33 ("*Health-related data and automated decision making*"), ripropone lo stesso schema dell'art. 22 del reg. Ue n. 679/2016, ma senza replicare il divieto e aggiungendo invece espressamente un diritto alla spiegazione del processo decisionale automatizzato

[479] C. PERLINGIERI, *eHealth and Data*, cit., 135 s. Cfr. A.G. GRASSO, *GDPR e intelligenza artificiale: limiti al processo decisionale automatico in sanità*, cit., 183 ss.

[480] Anche il Regolamento generale sulla protezione dei dati tiene conto, del resto, del problema della discriminazione algoritmica. Come recita il considerando 71: «Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti».

[481] Cfr. la citata *Recommendation on the Protection and Use of Health-Related Data*, al punto 33.1

eliminare il meccanismo derogatorio di cui al par. 2 dell'art. 22. Quindi, perché possa aversi la decisione automatizzata, senza che si applichi il diritto (o il divieto) di cui al par. 1, si dovrebbe comunque integrare una delle ipotesi elencate al par. 2[482].

Il quadro giuridico che restituisce allora il Regolamento si connota per la scelta di cautela. Non è ammessa una decisione algoritmica assoluta, perché l'interessato ha diritto alla contestazione e, se vi è un intervento umano, la decisione non è più interamente automatizzata.

Da tutto ciò, tuttavia, si evince la possibilità che una decisione automatizzata, basata su dati sensibili, come quelli relativi alla salute, possa essere adottata a prescindere dalla volontà della persona[483]. Ciò potrà verificarsi se il trattamento di dati sanitari sia necessario per motivi di interesse pubblico rilevante (art. 9, par. 2, lett. *g*) e la decisione automatizzata sia autorizzata dal diritto (art. 22, par. 2, lett. *b*).

Lo spazio di autodeterminazione della persona è rimesso al legislatore, nell'adozione delle misure a garanzia dei diritti, delle libertà e degli interessi del soggetto[484]. La contestabilità e la possibilità di revisione della decisione – nella quale l'eventuale effettiva incidenza dell'intervento dell'uomo è tutta da meditare – non sembrano di per sé in grado di sottrarre il soggetto alla decisione stessa.

E questo vale a prescindere dal gradiente di sensibilità del dato stesso, cioè non rileva se sia trattato, ad esempio, tanto il dato su un episodio di raffreddore quanto il dato sulla condizione di sieropositività all'HIV.

Il diritto di opposizione, riconosciuto all'interessato dall'art. 21 del Regolamento, che pure può dare rilevanza giuridica alla 'situazione particolare' del soggetto, è costruito come un dispositivo che interferisce – e pur, come visto, limitatamente – con il trattamento, ma non necessariamente con la decisione.

Il Regolamento generale sulla protezione dei dati presenta allora punti di insensibilità normativa alla situazione specifica del soggetto e di distanza dalla reale molteplicità dei casi concreti.

La giustificazione di questa scelta riposerebbe principalmente nella natura pubblicistica

---

[482] Diversamente il soggetto vedrebbe una tutela per la decisione basata unicamente sul trattamento automatizzato di dati neutri maggiore rispetto a quella per la decisione automatizzata riferita ai dati sensibili. È appena il caso di osservare e ribadire l'eterogeneità dei vari 'consensi'.

[483] Il tema intreccia, ma senza sovrapposizione, quello dell'esistenza o meno di un diritto di spiegazione della decisione automatizzata R. MESSINETTI, *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, cit

[484] CIANCIMINO, *Protezione e controllo dei dati in àmbito sanitario e intelligenza artificiale. I dati relativi alla salute tra novità normative e innovazioni tecnologiche*, cit.,

dell'interesse da controbilanciare. Espressione, forse, di quel medesimo influsso pubblicistico, osservabile negli sviluppi più dettagliati e più nuovi della disciplina in materia, che consente di parlare di *amministrativizzazione* della protezione dei dati personali.

Che sia data rilevanza alla dimensione dell'interesse pubblico non è affatto un male, anzi. Il sistema, grazie a ciò, realizza la possibilità di una circolazione e di un utilizzo dei dati personali a beneficio della collettività – secondo un paradigma nuovo, solidaristico – che altrimenti non riuscirebbe ad ottenere od otterrebbe solo a costi insostenibili.

Meno prudente appare invece l'approccio se l'attenzione alla dimensione pubblica porti a scartare il rilievo della personalità dell'individuo e delle circostanze particolari in cui venga a trovarsi. A questo approdo il Regolamento non arriverebbe, forse, se, nel classificare le particolari categorie di dati personali, tenesse conto della diversa sensibilità che connota i dati personali appartenenti a categorie particolari e, specialmente, i dati relativi alla salute.

Una previsione di questo tipo sarebbe, in fondo, consona al personalismo proprio dei principi europei che guidano il processo della digitalizzazione.

6. *La parentesi della pandemia di Covid-19*

Dal 2020 al 2023[485] l'emergenza pandemica per la diffusione del Covid-19 ha segnato la vita delle persone in tutto il mondo, mettendo a dura prova le strutture della società, compresi il ruolo delle istituzioni e gli ordinamenti giuridici a livello nazionale, sovranazionale e internazionale[486].

Non è stata solo una crisi sanitaria. Le gravi ripercussioni subite dalla popolazione sono state di tipo economico, con perdite ingenti del PIL, attività cessate e aumento della povertà; di ordine sociale, per la chiusura delle frontiere, limitazioni alla libertà di circolazione, isolamento, solitudine e depressione; di carattere politico, in senso lato, con divisioni fra Paesi e all'interno degli stessi e disinformazione dilagante. La crisi ha anche messo a nudo la realtà delle diseguaglianze, sacrificando le persone più povere e vulnerabili[487].

Il lento ritorno alla normalità, in seguito, se certo ha consentito il superamento di tante

[485] Con dichiarazione del 30 gennaio 2020, il Direttore Generale dell'OMS, sulla base del parere del Comitato di Emergenza, annunciò che la diffusione del virus costituiva una emergenza di sanità pubblica di rilevanza internazionale. Il 5 maggio 2023, ha dichiarato la fine dell'emergenza di rilevanza internazionale. I documenti sono consultabili in *www.who.int.* Cfr. quanto riportato in *www.osservatoriosullefonti.it.*
[486] G. THIENE (a cura di), *op. cit.*
[487] V. *WHO Director-General's opening remarks at the media briefing*, 5 maggio 2023, in *www.who.int.*

difficoltà, non ha completamente rimarginato le ferite nel tessuto socio-economico, che talvolta si sono anzi acuite per via del concomitante scoppio della guerra in Ucraina.

Gli sconvolgimenti causati dalla pandemia nella società si sono rispecchiati nel diritto, che è andato incontro a mutamenti – evoluzioni o involuzioni – nell'intento di fornire adattamenti e rimedi ai problemi che via via si presentavano, spesso con una produzione di norme alluvionale e disorganica, di difficile coordinamento nel sistema delle fonti.

La risposta dell'ordinamento ha implicato numerose riflessioni, pressoché in tutti gli ambiti del diritto. Soprattutto, l'esigenza di tutelare il diritto alla salute ha messo in luce l'importanza del buon funzionamento del Servizio sanitario nazionale, mentre l'esigenza di bilanciarlo con altri diritti fondamentali ha evidenziato il bisogno di ricercare strumenti idonei, che sacrifichino il meno possibile gli interessi dei singoli e della collettività.

Con l'emergenza pandemica, il settore che ha mostrato il bisogno maggiore di un ammodernamento tecnologico e la possibilità di trarne il più grande vantaggio, forse, è proprio quello della sanità. E gli strumenti cui si è pensato, per contenere il diffondersi del virus, hanno richiesto un bilanciamento – specialmente, ma non solo – con il diritto alla privacy e alla protezione dei dati personali.

La disciplina del trattamento di dati sanitari è stata quindi al centro della tensione fra diritti – almeno apparentemente[488] – contrapposti, alla salute e alla riservatezza.

Le applicazioni di tracciamento hanno potuto operare grazie al trattamento di dati relativi alla salute[489]. L'idea si fonda sull'utilità di seguire la trasmissione del virus per controllare l'andamento della pandemia e cercare di prevenire i contagi. Il tracciamento dei contatti personali a fini di sorveglianza sanitaria è avvenuto attraverso l'adozione di sistemi di *contact tracing* e in Italia è stato pensato con l'utilizzo dell'App *Immuni*[490].

Limitando l'analisi al quadro normativo generale, in relazione alla protezione dei dati

[488] COLAPIETRO e IANNUZZI, *App di* contact tracing *e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali*, in www.dirittifondamentali.it, 10 giugno 2020

[489] G. RESTA E ZENO-ZENCOVICH, *Rise and Fall of Tracing Apps*, in SENIGAGLIA, C. IRTI e BERNES (a cura di), *op. cit.* Più specificamente sulla geolocalizzazione GAMBINO e TUZZOLINO, *Location Data and Privacy*, in SENIGAGLIA, C. IRTI e BERNES (a cura di), *op. cit.*, 141 ss. Il tracciamento dei contatti è stato impiegato massicciamente in Corea del Sud, anche in base all'esperienza maturata anni prima, nel 2015, in occasione dell'epidemia della c.d. Mers. Il modello sudcoreano non sarebbe stato adottabile nel contesto europeo, per la pervasività dei mezzi, contraria ai principi che regolano la privacy e la protezione dei dati. Cfr. MICOZZI, *Le tecnologie, la protezione dei dati e l'emergenza Coronavirus: rapporto tra il possibile e il legalmente consentito*, in *BioLaw Journal - Rivista di BioDiritto*, 2020, fasc. 1, 623 ss.

[490] Le norme di riferimento sono contenute nell'art. 6, d.l. 30 aprile 2020, n. 28, convertito con modificazioni dalla l. 25 giugno 2020, n. 70. Sul tema v.: AMORE, Covid-19 *e Protezione dei dati personali*, in *Studium iuris*, 2020, 1159 ss.; DELLA MORTE, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, in *Diritti umani e diritto internazionale*, 2020

relativi alla salute, si osserva come si siano ritenute applicabili alla fattispecie l'eccezione prevista dall'art. 9, par. 2, lett. *i*, del Regolamento, ossia la necessità per motivi di interesse pubblico nel settore della sanità pubblica – è proprio questo il caso della protezione da gravi minacce per la salute a carattere transfrontaliero – nonché la base giuridica di cui all'art. 6, par. 1, lett. *d* ed *e*, e par. 3, cioè le condizioni di liceità del trattamento corrispondenti alla necessità per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento[491].

A prescindere dalla questione della liceità del trattamento dei dati personali, l'uso della App *Immuni* è rimasto fondato sul consenso della persona. Si è deciso, infatti, di non rendere in alcun modo obbligatorio il *download* dell'applicazione così come non si è sancito nessun obbligo di installazione e di utilizzo. E ciò è stato deciso nonostante il pericolo della pandemia in corso.

Il Garante stesso espresse parere favorevole in merito alla corrispondente proposta normativa, anche perché quel sistema di *contact tracing* «si fonda sull'adesione volontaria dell'interessato»[492].

In questo caso, il consenso è il presupposto del trattamento, non tanto la base giuridica che lo legittima[493].

Lo scaricamento di una App sul proprio dispositivo, infatti, richiede una manifestazione di volontà, che è riconducibile al consenso negoziale, mentre il consenso dell'interessato al trattamento dei dati personali – base giuridica del trattamento – è un atto logicamente distinto, che può essere oggetto di una prestazione.

Terminata l'emergenza sanitaria in Italia, dal 31 dicembre 2022 si sono dismesse la piattaforma nazionale per la gestione del Sistema di allerta Covid-19 e la relativa App *Immuni*. Ciò ha comportato il ritiro dell'applicazione dagli *store*, la cessazione del suo funzionamento per allertare dei contagi e per acquisire le certificazioni verdi Covid-19 (c.d.

---

[491] PERTOT, *Immuni e tracciamento digitale: fra protezione dei dati personali, problemi di efficacia e qualche prospettiva futura*, cit., 1131 ss.

[492] «In ragione del rilevante impatto individuale del tracciamento, l'adesione al sistema deve essere frutto di una scelta realmente libera da parte dell'interessato. La mancata adesione al sistema non deve quindi comportare svantaggi né rappresentare la condizione per l'esercizio di diritti». Provvedimento del Garante per la protezione dei dati personali del 29 aprile 2020, n. 79, "Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19", consultabile in *www.garante- privacy.it.*

[493] ZANOVELLO, Contact tracing *ed emergenza sanitaria: una sfida difficile*, cit., 293 s.; PERTOT, *Immuni e tracciamento digitale: fra protezione dei dati personali, problemi di efficacia e qualche prospettiva futura*, cit., 1155 ss. Così si è espresso il citato provvedimento del Garante n. 79 del 29 aprile 2020

green pass), che nell'App possono solo essere conservate. Quindi, dalla stessa data è stato interrotto ogni trattamento di dati personali effettuato dal Ministero della salute ai sensi dell'art. 6 d.l. n. 28/2020[494].

Il *green pass* è un altro strumento che si basava sul trattamento di dati sanitari, utilizzato per cercare di tenere sotto controllo e, possibilmente, ridurre l'andamento dei contagi. Stabilito dall'Unione europea con il Regolamento n. 953 del 2021[495] e, in Italia, dal d.l. 22 aprile 2021, n. 52[496], in particolare dall'art. 9, era una certificazione che comprovava lo stato di avvenuta vaccinazione contro il coronavirus o guarigione dall'infezione ovvero l'effettuazione di un test antigenico rapido o molecolare, e veniva richiesto per accedere a luoghi, servizi e prestazioni[497].

Anche l'introduzione e l'applicazione delle relative disposizioni ha richiesto una particolare attenzione – dimostrata dall'Autorità garante per la protezione dei dati personali – affinché fossero rispettati il diritto alla protezione dei dati e il diritto alla riservatezza degli interessati.

Cessando l'applicabilità del reg. Ue n. 953 del 2021 il 30 giugno 2022, ai sensi dell'art. 17 dello stesso, è pure terminato il rilascio di nuovi *green pass*.

Per fronteggiare la situazione emergenziale, pure si sono impiegati strumenti che erano già in uso, ma in modi differenti. Così è stato per la ricetta medica dematerializzata[498].

---

[494] Art. 6, comma 6°, d.l. n. 28/2020 (modificato dall'art. 2, comma 1°, lett. *b*, d.l. 7 ottobre 2020, n. 125,convertito con modificazioni dalla l. 27 novembre 2020, n. 159, e successivamente dall'art. 15, comma 1°,del d.l. 24 dicembre 2021, n. 221, convertito con modificazioni dalla l. 18 febbraio 2022, n. 11): «L'utilizzo dell'applicazione e della piattaforma, nonché ogni trattamento di dati personali effettuato ai sensi al presente articolo sono interrotti alla data di cessazione delle esigenze di protezione e prevenzione sanitaria, legate alla diffusione del COVID-19 anche a carattere transfrontaliero, individuata con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro della salute, e comunque entro il 31 dicembre 2022, ed entro la medesima data tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi».

[495] Regolamento (UE) 2021/953 del Parlamento europeo e del Consiglio, del 14 giugno 2021, *su un quadro per il rilascio, la verifica e l'accettazione di certificati interoperabili di vaccinazione, di test e di guarigione in relazione alla COVID-19 (certificato COVID digitale dell'UE) per agevolare la libera circolazione delle persone durante la pandemia di COVID-19*.

[496] Recante "Misure urgenti per la graduale ripresa delle attività economiche e sociali nel rispetto delle esigenze di contenimento della diffusione dell'epidemia da COVID-19", c.d. Decreto riaperture

[497] V. G. GRASSO, Green pass *e tutela della salute pubblica: dall'ordinamento eurounitario al diritto costituzionale nazionale. Elementi di comparazione tra le esperienze italiana e francese*, in *Corti supreme e salute*, 2022, fasc. 1, 213 ss

[498] La dematerializzazione aveva preso avvio con il d.m. 2 novembre 2011, del Ministero dell'economia e delle finanze – in adempimento a quanto previsto dall'art. 50, d.l. 30 settembre 2003, n. 269 (Sistema Tessera Sanitaria), e in particolare il comma 5 *bis*, introdotto dall'art. 1, comma 810, l. 27 dicembre 2006, n. 296, e dall'art. 11, comma 16, d.l. 31 maggio 2010, n. 78 –, il quale disponeva che la ricetta medica a carico del Servizio sanitario nazionale fosse sostituita dalla ricetta elettronica generata dal medico. CFR. VICIANI, *Sicurezza e privacy nella "prescrizione elettronica"*, in *Giust.civ.com*, 28 giugno 2016; G.M. CAVO,

Stante allora la necessità di evitare ogni forma di assembramento che si sarebbe potuta determinare, anche nella permanenza nelle sale di attesa dei medici prescrittori, si pensò di intervenire sulle modalità di consegna della ricetta, individuando alternative alla stampa del promemoria cartaceo. In relazione allo schema di decreto del Ministero dell'economia e delle finanze – di cui alle note del 26 febbraio e del 17 marzo 2020 –, il Garante per la protezione dei dati personali espresse parere favorevole[499].

Dopo aver manifestato alcune perplessità sulla delimitazione delle modalità alternative, prevista in una prima versione dello schema di decreto, alla sola consultazione del fascicolo sanitario elettronico, considerata la sua non completa attuazione sull'intero territorio nazionale e la – allora – facoltatività di attivazione dello stesso da parte dell'interessato, l'Autorità apprezzò la modifica che apriva all'individuazione di canali ulteriori per la consegna all'assistito del "promemoria dematerializzato" della ricetta elettronica.

Il d.m. 25 marzo 2020, del Ministero dell'economia e delle finanze, recante "Estensione della dematerializzazione delle ricette e dei piani terapeutici e modalità alternative al promemoria cartaceo della ricetta elettronica", ha quindi contemplato[500], come canali alternativi di consegna del promemoria, il portale del Sistema di Accoglienza Centrale (SAC), il fascicolo sanitario elettronico dell'assistito[501], la posta elettronica e gli SMS[502]

L'approdo a soluzioni come questa, raggiunte sulla spinta dei bisogni legati alla pandemia, si è tradotto in novità normative che possono sopravvivere alla contingenza, soddisfacendo esigenze più generali di efficienza o semplificazione.

Una previsione più drastica e, per certi versi, eccentrica, sempre finalizzata al contrasto alla diffusione dei contagi e frutto della stagione di decretazione d'urgenza del 2020, è stata quella dell'art. 17 *bis*, d.l. 17 marzo 2020, n. 18, rubricato "Disposizioni sul trattamento dei

---

Informatizzazione della ricetta medica e raccordo con il Fascicolo Sanitario Elettronico, in *Salute e società*, 2017, fasc. 2, 71 ss.

[499] Provvedimento del 19 marzo 2020, n. 58, "Parere sulle modalità di consegna della ricetta medica elettronica". Al riguardo v. ZANOVELLO, *Emergenza epidemiologica da COVID-19 e modalità di consegna della ricetta medica: il parere del Garante Privacy*, in www.rivistaresponsabilitamedica.it, 6 aprile 2020. Cfr. Ministero della salute, *Covid-19, ricetta medica via email o con messaggio sul telefono*, in *www.salute.gov.it*, 20 marzo 2020, nella sezione *News e media - Notizie*.

[500] Ciò è stato previsto con l'introduzione dell'art. 3 *bis* al d.m. 2 novembre 2011.

[501] Allora, con la specificazione che ciò avvenisse solo a fronte del rilascio del consenso all'alimentazione del fascicolo stesso

[502] Con decreto del Ministero dell'economia e delle finanze del 30 dicembre 2020, recante "Dematerializzazione delle ricette mediche per la prescrizione di farmaci non a carico del Servizio sanitario nazionale e modalità di rilascio del promemoria della ricetta elettronica attraverso ulteriori canali, sia a regime che nel corso della fase emergenziale da COVID-19", si è poi provveduto alla dematerializzazione anche delle ricette mediche c.d. bianche, prevedendone pure qui la disponibilità del promemoria nel fascicolo sanitario elettronico. V. CARULLO, *Dematerializzazione delle ricette mediche "bianche": dubbi sulla competenza del Ministero dell'economia*, in www.irpa.eu, *Osservatorio sullo Stato digitale*, 23 febbraio 2021

dati personali nel contesto emergenziale"[503]. Il comma 1° dell'art. 17 *bis*, ha sancito, infatti, che un gruppo di soggetti, più o meno direttamente riferibili a funzioni sanitarie[504] potessero effettuare trattamenti dei dati personali che risultassero necessari all'espletamento delle funzioni attribuite nell'ambito emergenziale. La disposizione non ha specificato quali trattamenti né quali dati, anzi il testo dell'articolo ha incluso espressamente la comunicazione dei dati tra detti soggetti e il trattamento dei dati di cui agli artt. 9 e 10 del Regolamento, senza escludere alcunché. Come unica limitazione per la comunicazione dei dati personali a soggetti pubblici e privati, diversi da quelli di cui al comma 1, nonché la diffusione dei dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento, il comma 2° apporta il requisito dell'indispensabilità ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto. Al comma 3° si è prevista l'adozione di misure appropriate a tutela dei diritti e delle libertà degli interessati, senza però enunciare alcuna misura in particolare.

L'attribuzione di questo potere è stata disposta – come si legge al comma 1° – «per motivi di interesse pubblico nel settore della sanità pubblica e, in particolare, per garantire la protezione dall'emergenza sanitaria a carattere transfrontaliero determinata dalla diffusione del Covid-19 mediante adeguate misure di profilassi, nonché per assicurare la diagnosi e l'assistenza sanitaria dei contagiati ovvero la gestione emergenziale del Servizio sanitario nazionale»[505].

Si può cogliere, nel complesso, la difficoltà a ritenere «che l'art. 17 *bis* costituisca un fondamento legale idoneo a soddisfare il vincolo di compatibilità con il diritto

[503] V. al riguardo le considerazioni svolte da PERRONE, *Questioni di conformità del diritto alla privacy dell'emergenza con il diritto dell'Unione europea*, in *Dir. rel. ind*., 2020, 581 ss.

[504] Trattasi dei «soggetti operanti nel Servizio nazionale della protezione civile, di cui agli articoli 4 e 13 del codice di cui al decreto legislativo 2 gennaio 2018, n. 1, e i soggetti attuatori di cui all'articolo 1 dell'ordinanza del Capo del Dipartimento della protezione civile n. 630 del 3 febbraio 2020, nonché gli uffici del Ministero della salute e dell'Istituto superiore di sanità, le strutture pubbliche e private che operano nell'ambito del Servizio sanitario nazionale e i soggetti deputati a monitorare e a garantire l'esecuzione delle misure disposte ai sensi dell'articolo 2 del decreto-legge 25 marzo 2020, n. 19»

[505] «La compresenza di esigenze connesse alla sanità pubblica e alla protezione dei dati personali rappresenta proprio un esempio di quel necessario contemperamento di interessi contrapposti che il legislatore italiano ha dovuto affrontare durante questo periodo di emergenza sanitaria. Un esempio è l'art. 17-bis del d.l. 17 marzo 2020, n. 18 che ha dettato disposizioni particolari sul trattamento dei dati personali nel contesto emergenziale, sancendo in particolare la legittimità della comunicazione dei dati, anche sanitari, tra determinati soggetti al fine di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali necessari all'espletamento delle funzioni ad essi attribuite nell'ambito dell'emergenza determinata dalla diffusione del Covid-19. In presenza di tali norme derogatorie rispetto al regime normativo ordinario, occorrerà senz'altro porre cautela a ricondurre, una volta terminato il periodo emergenziale, i trattamenti di dati personali effettuati all'ambito delle ordinarie competenze e delle regole dettate in materia di protezione dei dati personali». Così Giusella Finocchiaro, nell'intervista di BOTTOS, *op. cit.*, 108.

dell'Unione»[506], alla luce di quanto effettivamente stabilito dall'art. 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea e dall'art. 23 del Regolamento.

L'effetto della disposizione, per come espressamente sancito, è durato fino al termine dello stato di emergenza, che, con le proroghe intervenute, si è avuto il 31 dicembre 2022. La ricerca di regole utili per rispondere alle necessità dell'emergenza, evidentemente, non è stata un'opera semplice e priva di disordine e talvolta ha prodotto formulazioni normative alquanto frettolose e forse infelici o quantomeno bisognose di un'interpretazione che, in un certo qual modo, riportasse la trama giuridica nazionale a conformità con il quadro del sistema eurounitario.

In questo contesto si è inserito il d.l. 19 maggio 2020, n. 34, recante "Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19" (c.d. Decreto rilancio), che ha previsto sostanziali modifiche alla disciplina del fascicolo sanitario elettronico.

Quella del Covid-19 è stata una parentesi normativa, un periodo transitorio in cui si è cercato di far fronte all'imprevisto e all'imprevedibile con gli strumenti che si sono apprestati al momento, un "laboratorio" di soluzioni giuridiche nuove, che hanno attinto agli schemi della sorveglianza[507]. L'uso dei dati attraverso la tecnologia è stato fondamentale, anche se forse, talvolta, le scelte avrebbero potuto essere più misurate[508].

---

[506]PERRONE, *op. cit.*, 585.

[507]E. ORRÙ, *Verso un nuovo Panottico? La sorveglianza digitale*, in CASADEI e PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano, Wolters Kluwer, 2021, 203 ss

[508] Si v. il menzionato report delle Nazioni Unite sulla gestione della crisi pandemica (A/76/220): *«"Surveillance" is a term of art used for epidemiological study and containment of disease. It is also used to refer to security activities linked, for example, to intelligence gathering and law enforcement purposes. Both uses, i.e., medical and security, must be necessary and proportionate.* […] *The Special Rapporteur finds that a significant amount of personal data collection in the name of combating the COVID-19 pandemic was, for certain periods of time, especially during the period from January to June 2020, neither necessary nor proportionate*. […] *From a right to privacy perspective, the pandemic has enabled more intrusion by Governments and corporations into people's lives, infringing their right to privacy. While some infringements can be expected to arise during a pandemic, for public health purposes, it has, to date, proven to be impossible to gauge to what extent these have been necessary and proportional.* […] *Unfortunately, many States have framed privacy protection as opposed to necessary measures for saving lives. It is a simplistic view that ignores the importance that people attach to their privacy and to limiting unwarranted incursions by government and the commercial sector into their lives. The result is resistance to government's pandemic management efforts.* […] *If a State decides that technological surveillance is necessary as a response to the global COVID-19 pandemic, it must prove both the necessity and proportionality of the specific measure and establish a law that explicitly provides for such surveillance measures containing mandatory explicit and specific safeguards*» (punti 24, 53, 87, 88 e 114). V. anche il report sull'attuazione dei principi di limitazione delle finalità, cancellazione dei dati e responsabilità nel trattamento dei dati personali raccolti da enti pubblici nel contesto della pandemia (A/HRC/52/37), consultabile in *www.undocs.org*.

Ma non è mai stata una parentesi dei diritti fondamentali, compreso quello alla protezione dei dati personali, la cui tutela non ha mai smesso di essere garantita dall'ordinamento.

7. *Il fascicolo sanitario elettronico (FSE)*

Dei tanti strumenti della sanità digitale, il fascicolo sanitario elettronico (FSE) rappresenta, nell'ordinamento italiano, una figura centrale per l'ammodernamento tecnologico dei servizi sanitari e, forse, una delle maggiori sfide per la regolamentazione del trattamento dei dati relativi alla salute e l'implicito bilanciamento di diritti[509].

Definito in dottrina come «un supporto informatico contenente dati personali di natura amministrativa, sociale e sanitaria che riflettono un'immagine passata, presente e futura dello stato di salute di una persona al fine di facilitarne l'accesso e l'utilizzo da parte dei terzi autorizzati»[510] – con la precisazione che, a differenza del tradizionale fascicolo cartaceo conservato dalla struttura o dal professionista stesso e funzionalmente limitato ad alcuni dati, esso intende raccogliere ogni informazione attinente alla salute di un paziente e condividerla fra più soggetti per via elettronica – il FSE costituisce «una nuova forma di comunicazione e gestione dei dati del paziente, che permette di far confluire in un unico documento informatizzato tutti i dati sanitari di quest'ultimo, in modo da facilitare l'accesso e l'utilizzo degli stessi da parte dei terzi autorizzati al momento del bisogno»[511].

Nelle linee guida del 16 luglio 2009, il Garante per la protezione dei dati personali lo qualificava come «condivisione informatica, da parte di distinti organismi o professionisti, di dati e documenti sanitari che vengono formati, integrati e aggiornati nel tempo da più soggetti, al fine di documentare in modo unitario e in termini il più possibile completi un'intera gamma di diversi eventi sanitari riguardanti un medesimo individuo e, in prospettiva, l'intera sua storia clinica», puntualizzando di riferirsi «all'insieme dei diversi eventi clinici occorsi ad un individuo, messo in condivisione logica dai professionisti o organismi sanitari che assistono l'interessato, al fine di offrirgli un migliore processo di

[509] Cfr. CAPILLI, *Diritto privato sanitario. Fondamenti*, cit., 5 ss.; L. FERRARO, *Il Regolamento UE 2016/679 tra Fascicolo Sanitario Elettronico e Cartella Clinica Elettronica: il trattamento dei dati di salute e l'autodeterminazione informativa della persona*, in *BioLaw Journal - Rivista di BioDiritto*, 2021

[510] V. PEIGNÉ, *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, cit.,

[511] COMANDÉ, NOCCO e PEIGNÉ, *Il fascicolo sanitario elettronico: uno studio multidisciplinare*, in *Riv. it. med. leg.*, 2012, 105 s.

cura»[512]. Nel sito istituzionale dell'Agenzia per l'Italia Digitale (AgID) dedicato al FSE, si può leggere che esso «è lo strumento attraverso il quale il cittadino può tracciare e consultare tutta la storia della propria vita sanitaria, condividendola con i professionisti sanitari per garantire un servizio più efficace ed efficiente»[513].

La definizione che ne diede il legislatore all'art. 12, comma 1°, d.l. 18 ottobre 2012, n. 179, fu: «l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito». Il d.l. n. 34 del 2020 è intervenuto a modificare questa definizione, estendendola con l'aggiunta del riferimento «anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale».

Il FSE, sul quale tanto investe il PNRR, come anticipato, nella Missione 6 'Salute', non è una novità nell'esperienza italiana, essendo stato ufficialmente istituito, appunto, con il d.l. n. 179/2012 (c.d. Decreto crescita 2.0)[514].

Ma già prima di allora diverse iniziative[515] locali, pubbliche e private, avevano promosso l'apertura di analoghi fascicoli elettronici, tanto che, per preservare la privacy degli individui nell'impiego della nuova tecnologia, che di lì a poco sarebbe stata istituita formalmente, furono approvate le menzionate linee guida del Garante, del 2009, cui seguirono, dopo un anno, quelle del Ministero della salute[516]. Si optò, quindi, per un modello di FSE caratterizzato da un'infrastruttura basata su una rete nazionale di architetture regionali[517].

---

[512] "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di *dossier* sanitario" del Garante per la protezione dei dati personali del 16 luglio 2009, del. n. 25, consultabili all'indirizzo: *www.garanteprivacy.it.*

[513] È la definizione presente in *www.fascicolosanitario.gov*.

[514] Con il d.l. n. 179/2012 non si realizzò solamente il FSE, ma anche il fascicolo elettronico dello studente (art. 10, d.l. n. 179/2012) e una – per certi versi simile – digitalizzazione nel settore della giustizia (v. la sez. VI del d.l. n. 179/2012, "Giustizia digitale", in particolare l'art. 16 *bis*). Vi era, alla base, l'idea di costruire banche dati digitali, che fossero consultabili agevolmente dagli interessati.

[515] l'iniziativa regionale sul tema risponde alla suddivisione delle competenze fra Stato e Regioni, di cui all'art. 117 Cost., per cui in relazione alla tutela della salute le Regioni hanno una competenza legislativa concorrente con lo Stato. PEIGNÉ, *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, cit., 1522.

[516] Ministero della salute, *Il Fascicolo Sanitario Elettronico. Linee guida nazionali*, in *www.salute.gov.it*, 11 novembre 2010.

[517] PEIGNÉ, *Verso il Fascicolo Sanitario Elettronico: presentazione della riforma francese*, in *Dir. Internet*, 2007, 626 ss. Recentemente si è posto il problema dell'interoperabilità dei fascicoli. In relazione alla progettazione, contemplata in seguito all'art. 12, comma 15 *ter*, d.l. 179/2012, da parte dell'Agenzia per l'Italia Digitale (AgID), in accordo con il Ministero della salute, il Ministero dell'economia e delle finanze e le Regioni, di una infrastruttura nazionale necessaria a garantire l'interoperabilità dei FSE (cfr. l'art. 25 d.P.C.m. n. 178/2015), la cui realizzazione è curata dal Ministero dell'economia e delle finanze attraverso l'utilizzo del Sistema Tessera Sanitaria – delineato in attuazione dell'art. 50 del d.l. n. 269/2003 – l'AgID stessa ha emanato una circolare, la n. 4 del 1° agosto 2017: "Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici (art. 12 - comma 15 *ter* – D.L. 179/2012)". Secondo le modifiche apportate all'art. 12, nel 2022, tale progettazione è affidata all'AGENAS, anziché all'Agenzia per

L'esigenza da cui prese avvio la creazione del FSE era un bisogno da tempo avvertito non solo a livello nazionale, italiano e straniero, ma anche sovranazionale[518] e internazionale, percepito sia dagli operatori sanitari sia dagli utenti del sistema sanitario, e cioè una più agevole accessibilità ai dati relativi alla salute del paziente, per il miglior perseguimento dello scopo di cura[519].

Nacque quindi come strumento per la persona[520] e alla volontà di questa subordinato[521].

Apparve subito chiaro, tuttavia, che con questo strumento si potevano raggiungere più obiettivi. Al fine primario di cura, così, si aggiunsero le finalità di ricerca e di governo, essendo già allora note le potenzialità del trattamento dei dati sanitari.

Il FSE ha dunque acquisito, da un lato, la finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico, e, dall'altro, quella di programmazione sanitaria, verifica della qualità delle cure e valutazione dell'assistenza sanitaria. Si è cioè riconosciuto, accanto allo scopo principale, ossia l'agevolazione dell'assistenza del paziente, quello di fornire una base informativa consistente per il complessivo miglioramento della qualità dei servizi, compresi appunto quelli inerenti a ricerca e governo[522].

Inoltre, attraverso il FSE sarebbe possibile – almeno in teoria – soddisfare un'esigenza di tipo 'economico': la maggior efficienza perseguita con l'utilizzo di tale strumento, infatti,

---

l'Italia digitale, ma, nella fase di attuazione del PNRR e fino al 31 dicembre 2026, è curata dalla struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale in raccordo con il Ministero della salute e il Ministero dell'economia e delle finanze (comma 15 ter.1). Questa infrastruttura nazionale ha il compito di garantire, tra l'altro, anche l'identificazione dell'assistito attraverso l'allineamento con l'Anagrafe Nazionale degli Assistiti (ANA). Con d.P.C.m. 1° giugno 2022 (in Gazz. Uff., 13 ottobre 2022, n. 240) è avvenuta l'istituzione effettiva dell'ANA, ma il processo è stato seguito anche dal Garante per la protezione dei dati personali. Cfr. S. CORSO, *Il sì del Garante allo schema di d.P.C.m. sull'Anagrafe nazionale degli assistiti*, in *www.rivistaresponsabilitamedica.it*, 6 aprile 2022.

[518] G. THIENE (a cura di), *op. cit.*

[519] GUARDA, *Fascicolo Sanitario Elettronico e protezione dei dati personali*, Trento, 2011

[520] PIOGGIA, *Il Fascicolo sanitario elettronico: opportunità e rischi dell'interoperabilità dei dati sanitari*, in CAVALLO PERIN (a cura di), *op. cit.*, 215 ss.

[521] FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, cit., 305: «Molte sarebbero state le scelte possibili nel delineare l'architettura giuridica del fascicolo sanitario elettronico, come pure del dossier sanitario: lo si sarebbe potuto incentrare sul medico, garantendo la completezza delle informazioni, o sulla struttura sanitaria, conferendo maggiore rilevanza agli aspetti amministrativi. Si è scelto, invece, di incentrarlo sull'individuo e di garantire l'autodeterminazione del medesimo. Il fascicolo sanitario elettronico, in questa concezione, è dell'individuo e questi ne gestisce le informazioni. Può decidere, quindi, non solo se costituirlo o meno, ma anche quali eventi sanitari rendere visibili, quali oscurare e quali deoscurare. Il principio di autodeterminazione prevale quindi su altre diverse esigenze, quali appunto quella già citata della completezza delle informazioni contenute nel fascicolo».

[522] Art. 12, comma 2°, d.l n. 179/2012. V. Garante per la protezione dei dati personali, *Fascicolo sanitario elettronico - Domande più frequenti*, consultabile all'indirizzo www.garanteprivacy.it; Agenzia per l'Italia Digitale, *Fascicolo Sanitario Elettronico. Cos'è. Il Fascicolo Sanitario Elettronico (FSE)*, in *www.fascicolosanitario.gov.it*.

potrebbe consentire una riduzione degli errori medici e la correlativa diminuzione dei costi. La conservazione degli esiti e la loro non dispersione permetterebbero poi di evitare la ripetizione di accertamenti già svolti e l'esecuzione di esami inutili, conseguentemente con minori tempi e costi delle cure[523].

Il FSE si trova quindi regolato principalmente dal menzionato art. 12 d.l. n. 179/2012 e dal d.P.C.m. 29 settembre 2015, n. 178, recante "Regolamento in materia di fascicolo sanitario elettronico"[524].

Va detto, peraltro, che l'art. 12 è stato sin da subito oggetto di plurimi interventi modificativi.

Dopo le modifiche dettate dall'art. 1, comma 1°, l. 17 dicembre 2012, n. 221, in sede di conversione, l'articolo è stato ritoccato dall'art. 17, comma 1°, lett. *a*, d.l. 21 giugno 2013, n. 69, convertito, con modificazioni, dalla l. 9 agosto 2013 n. 98. A queste hanno fatto seguito quelle di cui all'art. 1, l. 11 dicembre 2016, n. 232; art. 1, comma 558, l. 30 dicembre 2018, n. 145; art. 3, l. 22 marzo 2019, n. 29; art. 11, d.l. 19 maggio 2020, n. 34, convertito, con modificazioni, dalla l. 17 luglio 2020, n. 77[525]; art. 21, d.l. 27 gennaio 2022, n. 4, convertito, con modificazioni, dalla l. 28 marzo 2022 n. 25.

L'art. 12 d.l. n. 179/2012 risulta quindi ritoccato dal legislatore per ben nove volte, finora. I continui interventi del legislatore, susseguitisi in un breve arco di tempo, fanno immediatamente intuire la delicatezza così come la problematicità del tema che affronta. La cospicua attività dell'Autorità garante, non solo di monitoraggio e sanzionatoria, ma anche consultiva, ne conferma la complessità[526].

7.1 Aspetti essenziali della disciplina

Il FSE è un 'contenitore' di dati personali e, come tale, di dati personali è alimentato. Ad alimentarlo sono i dati degli eventi clinici presenti e trascorsi riguardanti l'assistito, inerenti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale, in maniera

[523] PEIGNÉ, *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, cit.
[524] In Gazz. Uff., 11 novembre 2015, n. 263
[525] Illustra le intenzioni sottese alle singole modifiche apportate dall'art. 11, d.l. n. 34 del 2020, il Dossier del 9 luglio 2020, approvato dalla Camera dei Deputati e relativo appunto al c.d. "Decreto Rilancio", vol. I, p. 102 ss., consultabile all'indirizzo *www.documenti.camera.it.*
[526] ad esempio, il provvedimento del Garante per la protezione dei dati personali del 26 luglio 2017, n. 339, "Parere su uno schema di decreto del MEF di concerto con il Ministero della salute, concernente le modalità tecniche e i servizi telematici resi disponibili all'infrastruttura nazionale per l'interoperabilità dei FSE", e il provvedimento del Garante per la protezione dei dati personali del 27 settembre 2018, n. 456, "Parere su uno schema di decreto in tema di interoperabilità del Fascicolo Sanitario Elettronico (FSE) - 27 settembre 2018", entrambi consultabili all'indirizzo: *www.garanteprivacy.it.*

continuativa e tempestiva dai soggetti e dagli esercenti le professioni sanitarie che hanno in cura l'assistito stesso nonché, su iniziativa di quest'ultimo, con i dati medici in suo possesso[527].

Come previsto dalla modifica apportata nel 2022, «ogni prestazione sanitaria erogata da operatori pubblici, privati accreditati e privati autorizzati è inserita, entro cinque giorni dalla prestazione medesima, nel FSE»[528]. La regola, strettamente connessa al radicale intervento di natura sostanziale sul consenso, operato dal d.l. n. 34/2020, di cui si dirà, sancisce un termine, ma non comporta per i sanitari un obbligo di caricamento dei dati e così neppure una responsabilità in caso di mancato inserimento, come del resto già rilevato dal Garante per la protezione dei dati personali[529].

I contenuti del FSE si dividono in un "nucleo minimo" di dati e documenti e in dati e documenti integrativi[530].

Tra i contenuti, una particolare considerazione è riservata a dati e documenti "soggetti a maggiore tutela dell'anonimato", di cui all'art. 5 d.P.C.m. n. 178/2015.

È questa una disposizione di grande rilievo e, forse, si potrebbe dire di portata sistematica, nell'ottica della tutela della persona con riferimento al trattamento di dati relativi alla salute. Non solo nel contesto del trattamento operato mediante il FSE, ma in relazione alla disciplina del trattamento di dati sanitari nel suo complesso. E ciò per via dei principi e dei

---

[527] V. art. 12, commi 1° e 3°, d.l. n. 179/2012. Una parte specifica del FSE è il *dossier* farmaceutico (art. 12, comma 2 *bis*), finalizzato a favorire qualità, monitoraggio e appropriatezza nella dispensazione dei medicinali e aderenza alla terapia per la sicurezza del paziente e aggiornato a cura della farmacia che effettua la dispensazione.

[528] La modifica, operata con l. n. 25/2022, è all'art. 12, comma 1°, d.l. n. 179/2012.

[529] Provvedimento del 22 agosto 2022, n. 294, "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, sul Fascicolo Sanitario Elettronico (FSE)", in *www.garante- privacy.it.* L'Autorità ha rilevato, del resto, come l'assenza di un quadro giuridico che definisca le responsabilità degli operatori per il caricamento, l'aggiornamento o la correzione di eventuali errori possa incidere sul rispetto dei principi di completezza, esattezza, aggiornamento e sicurezza previsti dal Regolamento (art. 5).

[530] Art. 2, d.P.C.m. n. 178/2015. Il nucleo minimo si compone di: dati identificativi e amministrativi dell'assistito (art. 21, d.P.C.m. n. 178/2015), referti, verbali pronto soccorso, lettere di dimissione, profilo sanitario sintetico (art. 3, d.P.C.m. n. 178/2015), dossier farmaceutico, consenso o diniego alla donazione degli organi e tessuti. I dati e documenti integrativi comprendono invece: prescrizioni, prenotazioni, cartelle cliniche, bilanci di salute, assistenza domiciliare, piani diagnostico-terapeutici, assistenza residenziale e semiresidenziale, erogazione farmaci, vaccinazioni, prestazioni di assistenza specialistica, prestazioni di emergenza urgenza, prestazioni di assistenza ospedaliera in regime di ricovero, certificati medici, taccuino personale dell'assistito (art. 4, d.P.C.m. n. 178/2015), relazioni relative alle prestazioni erogate dal servizio di continuità assistenziale, autocertificazioni, partecipazione a sperimentazioni cliniche, esenzioni, prestazioni di assistenza protesica, dati a supporto delle attività di telemonitoraggio, dati a supporto delle attività di gestione integrata dei percorsi diagnostico-terapeutici (a questi si aggiungono gli altri documenti di cui all'art. 2, comma 3, lett. *aa*, d.P.C.m. n. 178/2015)

valori costituzionali, ma anche eurounitari, di cui si fa veicolo, su tutti la dignità della persona.

Riprendendo la riflessione già condotta su questa norma, si rammenta che essa subordina al previo *esplicito consenso* dell'assistito[531] – la cui acquisizione spetta ai sanitari – la visibilità di un insieme di dati connotato da estrema sensibilità, forse il *gradiente* più alto di sensibilità di dati relativi alla salute.

Si tratta di dati e documenti relativi alle condizioni delle persone sieropositive, delle donne che si sottopongono a interruzione volontaria di gravidanza, delle vittime di atti di violenza sessuale o di pedofilia, delle persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, delle donne che decidono di partorire in anonimato, nonché i dati e i documenti riferiti ai servizi offerti dai consultori familiari. Queste tipologie di dati vengono dunque oscurate di *default*, se caricate nel FSE. I dati e i documenti caricati nel FSE possono in ogni caso essere oscurati dall'assistito. L'art. 8 d.P.C.m. n. 178/2015, infatti, riconosce il diritto all'oscuramento. La richiesta di oscuramento dei dati e dei documenti può essere avanzata sia prima che dopo l'alimentazione del fascicolo, permettendo la loro consultabilità esclusivamente all'assistito e ai titolari che li hanno generati. La modalità con cui è realizzato l'oscuramento – che è sempre revocabile – impedisce che i soggetti abilitati all'accesso per finalità di cura vengano automaticamente a conoscenza dell'avvenuto oscuramento stesso e dell'esistenza dei dati oscurati: è il c.d. 'oscuramento dell'oscuramento'[532].

L'accesso al proprio FSE avviene in forma protetta e riservata, con gli strumenti previsti dal d.lgs. 7 marzo 2005, n. 82, c.d. Codice dell'amministrazione digitale. I Capi II, III e IV del "Regolamento in materia di fascicolo sanitario elettronico" sono dedicati ai trattamenti rispettivamente per finalità di cura, di ricerca e di governo. Le finalità di cura sono perseguite dai soggetti del Servizio sanitario nazionale e dei servizi socio-sanitari regionali e da tutti gli esercenti le professioni sanitarie secondo le rispettive modalità di accesso e nel

[531] Fermo restando che, qualora egli scelga di ricorrere alle prestazioni in anonimato, è vietata l'alimentazione del fascicolo da parte dei soggetti che erogano le prestazioni.

[532] Si è pure sottolineato come il fatto di riconoscere all'individuo il potere di oscurare i dati confluiti nel fascicolo e di limitare l'accesso si possa considerare in funzione di una maggiore adesione all'uso di questo strumento, legata a minori timori e disapprovazioni. PEIGNÉ, *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, cit., 1536 ss., la quale sottolinea che si può immaginare come l'esercizio di questo potere da parte del paziente possa reputarsi raro. L'assistito può comunque ottenere l'integrazione, la rettifica e l'aggiornamento dei propri dati contenuti nel FSE attraverso un apposito servizio di supporto, come previsto dal comma 3° dell'art. 8, e in conformità ai diritti sanciti dal Reg. Ue n. 679/2016.

rispetto delle misure di sicurezza[533].

L'alimentazione del FSE può avvenire da parte di molti soggetti, espressamente menzionati, nello svolgimento della loro attività professionale nell'ambito di un processo di cura.

I dati e i documenti presenti nel FSE possono essere consultati, per le medesime finalità di cura, solo con il consenso dell'assistito e sempre nel rispetto del segreto professionale, salvo i casi di emergenza sanitaria secondo apposite modalità. Il mancato consenso non pregiudica mai il diritto all'erogazione della prestazione sanitaria.

Le finalità di ricerca, da una parte, e quelle di governo, dall'altra, sono invece perseguite dalle Regioni e dalle Province autonome, oltreché dal Ministero del lavoro e delle politiche sociali e dal Ministero della salute nei limiti delle rispettive competenze attribuite dalla legge, senza l'utilizzo dei dati identificativi degli assistiti presenti nel fascicolo, secondo livelli di accesso, modalità e logiche di organizzazione ed elaborazione dei dati definiti conformemente ai principi di proporzionalità, necessità e indispensabilità nel trattamento dei dati personali.

In ogni caso, un generalizzato accesso dei terzi al FSE è vietato, così come è vietata la diffusione dei dati relativi alla salute, ai sensi dell'art. 2 *septies*, comma 8°, del Codice della privacy.

Attraverso l'Ecosistema Dati Sanitari (EDS), dovrà essere assicurata l'adeguatezza delle infrastrutture tecnologiche e la sicurezza cibernetica in raccordo con l'Agenzia per la cybersicurezza nazionale. Tale ecosistema è alimentato dai dati trasmessi dalle strutture sanitarie e socio-sanitarie, dagli enti del Servizio sanitario nazionale e da quelli resi disponibili tramite il sistema Tessera Sanitaria. Titolare del trattamento dei dati raccolti e generati dall'EDS è il Ministero della salute e la gestione operativa dell'EDS è affidata all'Agenzia nazionale per i servizi sanitari regionali (AGENAS), responsabile del trattamento. I contenuti dell'EDS, le modalità di alimentazione dell'EDS, nonché i soggetti che hanno accesso all'EDS, le operazioni eseguibili e le misure di sicurezza per assicurare i diritti degli interessati sono individuati con decreto del Ministro della salute. Il sistema del FSE, ai sensi del comma 3° dell'art. 12, viene ad alimentare l'EDS. Come evidenziato – pure in senso critico – dal Garante per la protezione dei dati personali, «l'EDS e la nuova architettura del FSE delineata dai recenti interventi normativi sono dunque fondati sull'elaborazione di dati e documenti sanitari originariamente generati per finalità di cura. In

[533] Art. 12, comma 4°, d.l. n. 179/2012.

particolare, l'EDS comporta una duplicazione dei dati e dei documenti generati per finalità di cura, costituendo una banca dati ("data repository centrale") che "acquisisce, memorizza e gestisce i dati", poi elaborati per offrire servizi agli esercenti le professioni sanitarie, al Ministero della salute, alle regioni/province autonome e allo stesso interessato. Il modello previsto determina quindi la costituzione della più grande banca di dati sulla salute del nostro Paese, raccogliendo, senza applicare alcuna tecnica di pseudonimizzazione, i dati e i documenti sanitari relativi alle prestazioni socio sanitarie erogate sul territorio nazionale di tutti gli assistiti»[534].

La disciplina del FSE, nel complesso, lascia aperto un problema 'operativo' di non poco momento, ossia che il fascicolo resta una raccolta di dati incompleta. Nel FSE, infatti, possono mancare alcune informazioni e il vuoto può essere reale, se i documenti non vengono caricati – e questo può accadere perché l'alimentazione, anche se non dipende dal consenso del paziente, non è obbligatoria – oppure virtuale, qualora il paziente abbia esercitato il suo diritto all'oscuramento. Dunque il professionista sanitario dev'essere consapevole del fatto che il FSE può sempre dare una visione solo parziale della storia clinica del paziente. L'eventuale non esaustività della raccolta visibile e consultabile di dati effettuata per mezzo di questo strumento comporta perciò anche la sua potenziale incompletezza. Il medico, allora, non può permettersi di fare totale affidamento sul FSE, poiché potrebbe rivelarsi dannoso per il paziente stesso, potendosi prendere decisioni inerenti alla sua salute sulla base di un compendio di informazioni parziale e, complessivamente, inesatto[535]. A ciò si deve aggiungere che il professionista non può sapere quali soggetti hanno conoscenza delle informazioni inserite nel fascicolo, dal momento che il paziente può limitare gli accessi al suo contenuto, pertanto non può contare su una conoscenza dei dati relativi alla salute del paziente condivisa con altri professionisti sanitari. L'incompletezza attuale del FSE è stata ribadita dal Garante per la protezione dei dati personali nel provvedimento n. 294 del 2022, il quale pure ha rilevato che nemmeno esiste un obbligo di consultazione del FSE[536].

È fuori discussione l'importanza, nel percorso terapeutico, del dialogo fra medico e paziente, l'anamnesi e il colloquio, l'interazione personale, che l'uso del FSE non può

[534] Provvedimento del 22 agosto 2022, n. 295, "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)" in *www.garanteprivacy.it*.
[535] PEIGNÉ, *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, cit., 1535 ss.
[536] Il Garante per la protezione dei dati personali ha, peraltro, ribadito che, secondo la normativa vigente, l'interessato ha «il diritto di non acconsentire all'utilizzo del FSE per finalità di cura, prevenzione e profilassi internazionale».

sostituire. «Il tempo della comunicazione tra medico e paziente costituisce tempo di cura»[1084].

7.2 L'eliminazione del consenso all'alimentazione del FSE. Profili critici e prospettive possibili

Fondamentale, il tema del consenso all'alimentazione del FSE rappresenta l'emblema dell'approccio dell'ordinamento italiano verso il trattamento dei dati relativi alla salute e la sua regolamentazione. Esso viene a integrarsi in un sistema contemporaneo del diritto – privato e pubblico – in cui la fonte nazionale norma solo una parte di questa realtà, ossia ciò per cui non dispone già la fonte sovranazionale. Questa non solo la affianca, ma anche, avendo acquistato nel tempo maggiore spazio e maggiore peso, la condiziona, conformandola ai suoi schemi e ai suoi modelli nuovi.

«Il FSE può essere alimentato esclusivamente sulla base del consenso libero e informato da parte dell'assistito, il quale può decidere se e quali dati relativi alla propria salute non devono essere inseriti nel fascicolo medesimo»[537]. Così recitava l'art. 12, d.l. n. 179/2012, al comma 3 *bis*[538]. Tale comma è stato abrogato dal menzionato d.l. n. 34/2020[539]. Anche alla luce del richiamato Decreto del Ministero della salute del 18 maggio 2022, non è più da ritenere applicabile l'art. 7 del d.P.C.m. n. 178/2015, che ancora contempla il consenso dell'assistito all'alimentazione del FSE.

La scheda sintetica aggiornata rinvenibile nel sito istituzionale dell'Autorità garante, finalizzata a riassumere le novità normative, riferisce, in ordine al consenso, che, «con i recenti interventi di semplificazione, il FSE viene automaticamente alimentato»[540].

La scelta di procedere all'abrogazione cancellando il requisito del consenso, è in linea con le affermazioni del Garante per la protezione dei dati personali, che nel provvedimento del 7 marzo 2019, n. 55 – come anticipato – ammetteva, forse incautamente, la possibile eliminazione della necessità di acquisire il consenso dell'interessato all'alimentazione del

---

[537] V. BOLOGNA *et al*., *Electronic Health Record in Italy and Personal Data Protection*, in *European Journal of Health Law*, n. 23, 2016, 265 ss.

[538] Introdotto dall'art. 1, comma 1°, l. 17 dicembre 2012, n. 221, in sede di conversione

[539] GAMBINO, MAGGIO e OCCORSIO, *La riforma del fascicolo sanitario elettronico*, in *Diritto mercato tecnologia*, *www.dimt.it*, 22 luglio 2020. Cfr. POSTERARO e CAVALCANTI, *Sanità digitale in Italia: il Fascicolo Sanitario Elettronico (FSE) dopo le modifiche introdotte dal decreto Rilancio*, in *www.irpa.eu*, *Osservatorio sullo Stato digitale*, 25 marzo 2021.

[540] «In modo che – aggiunge – lo stesso assistito possa facilmente consultare i propri documenti sociosanitari, anche se generati da strutture sanitarie situate al di fuori della Regione di appartenenza, grazie all'interoperabilità assicurata dal Sistema Tessera Sanitaria». Trattasi dell'infografica del 19 giugno 2020, *Le novità sul FSE*, consultabile all'indirizzo *www.garanteprivacy.it*.

fascicolo.

La posizione del Garante si basava sul quadro normativo rinnovato, a seguito dell'entrata in vigore del Regolamento generale sulla protezione dei dati e del d.lgs. n. 101/2018, di adeguamento delle disposizioni contenute nel Codice della privacy.

Già si è detto che l'art. 9 del Regolamento permette di eccepire al divieto di trattamento di dati relativi alla salute anche in assenza del consenso dell'interessato.

L'art. 75 del Codice della privacy, riformato dal d.lgs. n. 101/2018, come si è visto, rimanda all'art. 9 del Regolamento e all'art. 2 *septies* del Codice stesso, per le misure di garanzia.

L'art. 2 *sexies*, nella versione modificata nel 2021 contempla ora espressamente il trattamento di dati sanitari, privi di elementi identificativi diretti, da parte di soggetti istituzionali, per motivi di interesse pubblico rilevante, compresi i dati del FSE.

Del ruolo del consenso, così come emergeva dalle disposizioni in materia di protezione dei dati relativi alla salute e privacy in sanità, sembrano oggi perse le tracce.

Gli interventi del legislatore, soprattutto i più recenti, pare abbiano optato per un impianto tutt'altro che consensocentrico, un impianto imperniato invece su un paradigma pubblicistico – o forse solidaristico – della protezione dei dati personali, inclusi quelli sanitari.

Per quanto riguarda il FSE, sembra definitivamente sancito il passaggio ermeneutico di questa figura da strumento *principalmente per la persona* e la tutela dei suoi diritti fondamentali, primo fra tutti quello alla sua salute, a strumento *primariamente per la pubblica amministrazione* e la garanzia di maggiore efficienza, nel contesto del funzionamento del Servizio sanitario nazionale[541].

Dall'analisi di queste disposizioni di dettaglio si può notare come la previsione dell'interesse pubblico rilevante, così come l'interesse pubblico nel settore della sanità pubblica, tra le eccezioni al divieto di trattamento di dati sanitari, possa tradursi in una valvola di apertura – attesa anche l'ampiezza dell'elenco delle materie in cui si intende rilevante l'interesse pubblico di cui al comma 2°, dell'art. 2 *sexies* – quasi una clausola generale, che determina il superamento del divieto, al ricorrere del generale elemento pubblicistico.

La protezione dei dati personali – e specialmente relativi alla salute – si connota, quindi, sempre più come materia di diritto pubblico e amministrativo, perdendo rilievo la

[541] S. CORSO, *Sanità digitale e riservatezza. Interpretazioni sul fascicolo sanitario elettronico*, cit., 115

connotazione privatistica che la descriveva sostanzialmente come un semplice diritto dei singoli, come una questione di riserbo o un affare tra privati.

La tutela della persona – e lo si può intendere anche dall'evoluzione normativa del FSE – è affidata, dunque, al piano della sicurezza, che concretamente andrà garantita e implementata dai titolari del trattamento.

Questa impostazione potrebbe comunque comportare delle problematiche.

La creazione di un fascicolo sanitario determina, sin dal principio, una maggiore sfuggevolezza e incontrollabilità dei dati sanitari, giacché praticamente qualsiasi strumento elettronico può risultare, prima o poi, fallibile. Si può certo dire che la sicurezza del FSE debba essere massima, ma nessuno è in grado di assicurare un livello perfetto di tutela informatica[542]. Continua ad essere essenziale, su questo versante, il ruolo delle Autorità garanti nazionali e gli organi internazionali[543].

Alcuni profili critici, per quanto attiene al trattamento dei dati sanitari operato mediante il FSE, emergono, a nostro avviso, anche a monte, per così dire, sul piano interpretativo[544].

Un primo profilo attiene alla formulazione dell'art. 9 del Regolamento. Messo da parte il consenso esplicito dell'interessato, le ipotesi eccezionali di cui al par. 2, che derogano al divieto del par. 1 e che rilevano per il trattamento dei dati relativi alla salute tramite FSE, sono costruite – come si è detto – in termini di trattamento 'necessario'.

Il principio di necessità, che senz'altro vale anche per il trattamento dei dati c.d. neutri o comuni, come espresso dall'art. 6 del Regolamento, a maggior ragione trova applicazione, con riferimento al trattamento dei dati sensibili. Possiamo avere dei dubbi su come come vada inteso l'aggettivo 'necessario'. Si potrebbe pensare che 'necessario' voglia dire 'utile' o 'funzionale': quando il trattamento di dati sensibili è utile nei casi elencati nel par. 2 dell'art. 9, allora non è vietato. Oppure si potrebbe ritenere che 'necessario' stia per 'indispensabile', cioè il trattamento di dati sensibili non è vietato quando è indispensabile per lo scopo enunciato nelle ipotesi del par. 2 e non si può fare altrimenti. Tuttavia, delle due interpretazioni, forse la seconda è più convincente, poiché la prima priverebbe di qualsiasi significato effettivo il divieto di cui al par. 1: infatti, quale trattamento di dati personali non

[542] A. THIENE, *Salute, riserbo e rimedio risarcitorio*, cit., 1419 ss., che già evidenziava il fatto che «questo sistema, nell'agevolare l'accesso e la circolazione dei dati, espone a non pochi rischi il riserbo, l'identità, la libertà e la dignità della persona, amplificando problemi che si erano già posti in tema di cartella clinica. Lo testimoniano, anche in questo caso, la serie impressionante di pareri del Garante e la sua incessante attività ispettiva e sanzionatoria, svolta in un clima di costante attenzione nei confronti di problematiche legate alla realizzazione a livello nazionale del FSE».

[543] PEIGNÉ, *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, cit., 1543 s.

[544] S. CORSO, *Sanità digitale e riservatezza. Interpretazioni sul fascicolo sanitario elettronico*, cit., 119 ss

appare utile, quale non risulta necessario per meglio raggiungere uno di quegli obiettivi? L'eccezione diventerebbe la regola.

Seguendo la seconda interpretazione, ossia a quella per cui il divieto è derogato solo quando il trattamento di dati è indispensabile – in questo senso necessario – si può però sostenere che il trattamento di dati sanitari operato con il FSE sia l'unico modo possibile per rispondere agli interessi pubblici nel settore della sanità, indicati dalla legge? Se si risponde affermativamente, si deve accettare che la scelta di questo strumento, con l'esclusione di altri, renda il FSE qualcosa di molto diverso da un vero e proprio fascicolo di documenti del paziente, qualcosa di più simile a una banca dati della pubblica amministrazione attraverso cui andranno svolte funzioni pubbliche e di 'governo'[545].

Un secondo profilo critico si può ricavare esaminando la normativa nazionale. Si è detto che il consenso all'alimentazione del FSE è stato eliminato. Tuttavia, una cosa è il consenso all'alimentazione e altra cosa è il consenso all'attivazione del FSE, se non altro perché alimentazione e attivazione sono operazioni di trattamento di dati personali distinte.

Da quel che emerge leggendo il numero di fascicoli attivati nel sito istituzionale dedicato, si ricava comunque che non solo l'alimentazione, ma anche l'attivazione del FSE è già avvenuta e senza il consenso degli interessati[546].

La possibilità di attivare automaticamente il FSE di ciascun singolo si è dedotta interpretativamente dall'eliminazione del necessario consenso per l'alimentazione del FSE, che ora avviene in automatico È però un ulteriore trattamento di dati, che a sua volta deve rispettare quanto disposto dal Regolamento, compresa la copertura di una delle fattispecie eccezionali *ex* art. 9, par. 2.

Si potrebbe sostenere che l'attivazione del FSE non comporti già un trattamento di dati appartenenti alle particolari categorie di cui all'art. 9, ma questa interpretazione si scontrerebbe con la stretta prodromicità di questo trattamento con quelli di dati sanitari che andranno a svolgersi con l'alimentazione, con l'ampia definizione di dati relativi alla salute e con la struttura del fascicolo stesso.

La scelta legislativa di eliminare il consenso all'alimentazione del FSE, applicando altre ipotesi di deroga ai sensi dell'art. 9, par. 2, non è priva, quindi, di aspetti problematici inerenti

[545] In ogni caso, con riguardo al requisito della necessità, si fatica a comprendere come possano essere indispensabili due 'contenitori' digitali di dati relativi alla salute, visto che il FSE sarà affiancato dall'EDS, che pure alimenterà, con rischio di duplicazioni di dati, come riferito dal Garante per la protezione dei dati personali, nel provvedimento citato n. 295 del 2022.

[546] CONTALDO e CREA, *Il fascicolo sanitario elettronico con le puntualizzazioni operative delle fonti secondarie*, in *Diritto di Internet*, 2021,.

alla legittimazione stessa dei trattamenti di dati sanitari operati con questo strumento[547].

Quale sia, sul versante pratico, il portato di tale innovazione normativa si può cogliere immaginando la situazione concreta. Qualora un soggetto si rechi presso una struttura o da un professionista sanitario per una visita o una prestazione sanitaria, il referto o la documentazione relativa potranno essere caricati nel FSE dello stesso a prescindere da una sua qualsivoglia manifestazione di volontà.

Eliminare i dati o i file caricati nel FSE non risulta possibile, visto pure quali sono i confini del diritto di cancellazione intrinseci alla disciplina del Regolamento.

Ciò potrebbe addirittura scoraggiare il soggetto dal richiedere la prestazione sanitaria, sapendo che l'informazione sensibile relativa alla sua condizione di salute potrà essere consegnata al sistema informatico e immessa in rete[548].

Il consenso dell'interessato, con tutti i limiti evidenziati[549], non è più, quindi, l'istituto principale che fonda la legittimità del trattamento dei dati. Ciò non significa, però, che alla volontà dell'individuo non possa riconoscersi ancora un ruolo – anche con riferimento al FSE – e già diverse sono le disposizioni che tuttora rimandano al consenso, nella sua multiforme natura[550].

È forse superfluo sottolineare le grandi potenzialità del FSE, nel panorama della digitalizzazione della sanità, e i numerosi benefici che possono derivare alle persone dalla condivisione dei dati sanitari[551].

Ripristinare la regola del generalizzato previo consenso all'alimentazione del FSE non

---

[547] Il riferimento è almeno alle criticità osservate in relazione all'eliminazione del consenso all'operazione di alimentazione, che si replicherebbero ora in relazione all'eliminazione anche del consenso all'operazione di attivazione del FSE.

[548] «Non può non evidenziarsi un ideale contrasto tra la l. 219/2017 e l'eliminazione del consenso ai fini del FSE. Il legislatore ha, riguardo a quest'ultimo, valorizzato l'esigenza pubblicistica di un monitoraggio della situazione sanitaria di ciascun consociato, anche alla luce dell'emergenza sanitaria legata al Covid- 19, a discapito del diritto individuale di non consentire trattamenti terapeutici. In questo modo, viene definitivamente sancita la separazione tra il rapporto di cura e il rapporto 'informativo' – riguardante, da un lato, il consenso ex ante al trattamento e, dall'altro, il consenso ex post all'alimentazione del FSE. Quasi a voler dire che, una volta consentito il trattamento, le informazioni sanitarie ad esso relative non possono essere 'cancellate' per volontà del paziente. Ciò, probabilmente, potrebbe comportare una indiretta influenza in chi preferisca non far risultare alcuni trattamenti sanitari – riguardanti ad esempio la sfera sessuale – dovendo questi decidere se effettuarli e doverne dare atto nel FSE, o non effettuarli del tutto». GAMBINO, MAGGIO e OCCORSIO, *op. cit*., 8 s.

[549] Cfr. la riflessione del Comitato nazionale per la bioetica, *"Mobile-health" e applicazioni per la salute: aspetti bioetici*, cit., al punto 5.3.

[550] Ad esempio, il comma 6° dell'art. 2 *septies* del Codice della privacy che – per i dati genetici – riserva al Garante la possibilità di richiedere, quale ulteriore misura di protezione dei diritti dell'interessato, in caso di particolare ed elevato livello di rischio, il consenso per il trattamento

[551] FINOCCHIARO - POLLICINO, *Perché condividere i dati sanitari aiuta a tutelare i cittadini. Il nuovo regolamento europeo*, in *Il Sole 24 Ore* e in www.digitalmedialaws.com, 20 ottobre 2022

sarebbe forse la cosa più auspicabile.

Ci si chiede, tuttavia, se non possa essere opportuno una reintroduzione del consenso – o forse, meglio, della volontà del soggetto – in chiave di dissenso, cioè una regola che consenta di rimuovere dati o documenti presenti nel FSE o parti di essi, anche contestualmente al caricamento, o persino di chiudere un FSE, come avviene in altre esperienze giuridiche europee. È lo schema del c.d. *opt-out*. Certo questo meccanismo può sacrificare alcuni interessi. Potrebbe limitare la disponibilità di dati utili per gli studi e la ricerca scientifica, aumentare il rischio di eliminazioni accidentali compromettendo l'esattezza e l'integrità dei dati, creare confusione nella comunicazione tra medici e pazienti, richiedere aggiornamenti dell'infrastruttura tecnica e una gestione onerosa dei consensi.

Considerando però i vantaggi per i diritti del soggetto, alla protezione dei dati personali, alla privacy e a tutti gli altri diritti fondamentali connessi, si può immaginare di accompagnare a questo modello un correttivo, ossia circoscrivere la possibilità di esercitare il dissenso in ipotesi delimitate.

Questa delimitazione potrebbe seguire il livello o il "diverso gradiente di sensibilità" dei dati relativi alla salute, riservando l'operatività di tale consenso – non più base per la legittimazione del trattamento, ma esercizio di un diritto di 'uscita'[552] – ai dati più sensibili fra i dati sensibili, come sono quelli enunciati all'art. 5 d.P.C.m. n. 178/2015[553].

Un modello di *opt-out* limitato ai soli dati di questo tipo ridurrebbe i sacrifici altrimenti imposti agli altri interessi in gioco, nel trattamento di dati operato mediante FSE, e allo stesso tempo consentirebbe una forma di controllo sulle informazioni più intime dell'individuo, con una partecipazione attiva del paziente.

L'idea di un diverso rilievo della volontà del soggetto a seconda della sensibilità del dato personale – relativo alla salute – trattato, potrebbe trovare proprio in tale contesto applicazione concreta.

Una regola vecchia, quella del consenso come manifestazione della volontà, in una veste

[552] Cfr. PUNZI, *La persona nei dati. Ragioni e modelli di una regolamentazione*, cit., 773, riferisce di un diritto di uscita. V. anche ALÙ, *Il doppio volto di Internet tra l'accesso e l'uscita e il paradosso della "trappola" digitale*, in *Dir. fam. e pers*., 2023, 626 ss.

[553] «Pensando alla rilevanza che il sistema italiano – abbiamo visto – assegna al diritto alla riservatezza, ed alla riservatezza dei dati sensibili in particolare (secondo il circuito riservatezza-dignità-autodeterminazione), si deve considerare come un suo superamento ad opera di altri interessi possa essere ragionevole, e legittimo, solo in caso di estrema e reale necessità (in applicazione del criterio dell'«*indispensabilità*» del trattamento e della diffusione dei dati del sieropositivo, sopra menzionato)». CASONATO, Privacy *e AIDS. Il punto di vista giuridico*, cit

nuova, come nuova considerazione della tutela della personalità[554].

8. *L'Intelligenza Artificiale in Sanità*

L'utilizzo di sistemi di intelligenza artificiale in sanità trova oggi i suoi perimetro in varie e nuove discipline: il Reg.Ue 2024/1689 (AI ACT) che riguarda in particolare i prodotti (sistemi di AI), nel nuovo Disegno di legge sulla intelligenza artificiale (Atto Camera 2316) trasmesso dal Senato alla Camera il 20 marzo U.S.; da ultimo non meno importante il GDPR e, nello specifico, il Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale (pubblicato in ottobre 2023).

Nel disegno di legge italiano sull'intelligenza artificiale l'articolo 7, titolato (Uso dell'intelligenza artificiale in ambito sanitario e di disabilità) rappresenta la prima norma nazionale che affronta in modo organico l'impiego dell'IA nei settori della sanità e della disabilità, fissando principi generali e obiettivi strategici.

L'art. 7 del DDL intelligenza artificiale non introduce nuove regole relative al trattamento dei dati (come invece avviene all'art. 8 sulla ricerca per lo sviluppo della AI e art. 9 sulla ricerca attraverso strumenti di AI).

Ciò non toglie che erogare una prestazione sanitaria attraverso un sistema di AI significa trattare i dati dei pazienti in maniera diversa rispetto al trattamento che avviene attraverso altre tipologie di software.

Solo a titolo di esempio molti algoritmi operano attraverso "black box", rendendo opaca la logica decisionale e rendendo quindi complesso il rispetto degli articoli dal 13-14 del GDPR (nonché gli obblighi di spiegabilità di cui all'art. art. 13 GDPR), i rischi legati agli algoritmi di AI sono più alti richiedendo quindi una DPIA, l'utilizzo di un sofwtare di AI in sanità può configurare una profilazione ex art. 22 GDPR ecc.

L' 7 articolo infatti non detta regole tecniche, ma introduce una cornice valoriale: etica, trasparenza, non discriminazione e centralità della persona diventano criteri guida per lo sviluppo e l'uso di tecnologie che, per definizione, incidono su diritti fondamentali.

Il primo obiettivo della norma è chiaramente dichiarato: promuovere un impiego etico e responsabile dell'intelligenza artificiale, finalizzato al miglioramento della prevenzione, diagnosi, cura e qualità della vita. L'innovazione tecnologica è quindi vista come una leva di miglioramento del sistema sanitario, ma da impiegare nel rispetto del diritto alla salute, della

[554] ZATTI, *Il diritto all'identità e l'«applicazione diretta» dell'art. 2 Cost.*, cit

dignità del paziente e della libertà di scelta.

La norma sceglie un approccio "antropocentrico" ai sistemi di IA che, viene precisato, possono supportare, ma non sostituire, le decisioni del medico. È una scelta normativa chiara, in linea con i principi dell'AI Act europeo, che sancisce il primato del controllo umano sui sistemi ad alto rischio. Nel contesto sanitario, questo principio assume una valenza particolare: la responsabilità clinica resta sempre in capo al professionista, che deve saper utilizzare lo strumento tecnologico senza esserne vincolato. Di conseguenza, si impone anche una riflessione sulla formazione continua dei professionisti sanitari (chiamati a comprendere – oltre che usare – l'IA nei percorsi diagnostici e terapeutici) che si sposa perfettamente con gli obblighi di AI Literacy di cui all'art. 4 dell'AI ACT

L'articolo 7 introduce anche un'altra disposizione, tanto essenziale quanto necessaria: nessun sistema automatizzato può limitare l'accesso alle prestazioni sanitarie. È un principio che deve valere sia per la programmazione pubblica che per la gestione clinica, e che impedisce l'utilizzo dell'IA come strumento selettivo o escludente.

In altre parole, l'adozione di soluzioni tecnologiche non può creare barriere implicite – ad esempio legate al profilo socioeconomico, alla residenza, o al livello di digital literacy – nell'accesso al diritto alla salute.

Un altro aspetto di rilievo riguarda la trasparenza dell'impiego dell'IA nei percorsi clinici. L'art. 7 comma 3 stabilisce infatti che: "L'interessato ha diritto di essere informato sull'impiego di tecnologie di intelligenza artificiale." Questo è senza dubbio un aspetto che merita una particolare riflessione.

Come noto infatti nel nostro ordinamento l'art. 1 comma 1 Legge 22 dicembre 2017, n. 219 "Norme in materia di consenso informato e di disposizioni anticipate di trattamento" legge stabilisce che: «Nessun trattamento sanitario può essere iniziato o proseguito se privo del consenso libero e informato della persona interessata, tranne che nei casi espressamente previsti dalla legge».

La combinazione delle due norme comporta che il paziente dovrà essere informato non solo degli aspetti clinici ma anche di quelli tecnologici (uso della AI), potendo a quel punto esprimere il proprio consenso o rifiutare le cure.

Si tratta di un cambio di paradigma: il paziente diventa anche interlocutore consapevole rispetto agli strumenti che orientano il proprio percorso di cura.

Infine, la norma stabilisce l'obbligo di verifica e aggiornamento periodico dei sistemi di IA, nonché dei dati utilizzati per alimentarli.

Più esattamente sancisce che " I sistemi di intelligenza artificiale utilizzati in ambito sanitario e i relativi dati impiegati devono essere affidabili, periodicamente verificati e aggiornati al fine di minimizzare il rischio di errori e migliorare la sicurezza dei pazienti."

La norma non stabilisce esattamente chi deve essere il responsabile di tali controlli, ma se combiniamo tale obbligo con quelli di cui al Cap IX dell'AI ACT relativi alla sorveglianza post commercializzazione ed alla vigilanza sui sistemi di AI ad alto rischio in capo al fornitore del sistema AI, capiamo bene come la governance interna della struttura sanitaria ed le procedure post commercializzazione del fornitore di AI dovranno fortemente interconnettersi.

Se da un alto l'introduzione della tecnologia e dell'Intelligenza Artificaile in sanità è, da un lato un fenomeno inevitabile e, dall'altro un innegabile vantaggio in termini di prestazioni rese all'utente, non dobbiamo dimenticare "l'altra faccia della medaglia" di questo percorso di progressiva digitalizzazione che, inevitabilmente comporterà l'insorgenza di rischi molto rilevanti.

Le principali criticità da affrontare saranno le seguenti:

Potenziale discriminazione: I sistemi di IA potrebbero essere predisposti a discriminare determinati gruppi di persone, ad esempio sulla base della razza, dell'etnia, del sesso o dello stato socioeconomico. ***Occorrerà ancora una volta fare leva sulla tecnologia***, realizzando un sistema personalizzato all'utente, predisponendo gli strumenti tecnologici adeguati, elaborando altresì linee guida per il corretto utilizzo. Bisognerà inoltre rafforzare le c***ompetenze tecnologiche degli esseri umani:*** è necessario, infatti, garantire un alto livello di competenza e formazione dei professionisti e degli utenti al fine di assicurare un uso appropriato dell'IA. A tale sfida, occorrerà prepararsi formando in modo adeguato il personale, creando basi sufficientemente solide affinché venga garantite una corretta gestione dei sistemi intelligenti.

Mancanza di trasparenza: I sistemi di IA possono risultare complessi da "capire" e poco trasparenti, rendendo difficile comprendere in che modo vengano prese le decisioni. Questo può portare a una mancanza di fiducia da parte dei pazienti e dei professionisti sanitari stessi che utilizzano tale tecnologia. È essenziale che il personale sanitario comprenda come funzionano questi sistemi per poterli utilizzare correttamente e con fiducia. ***Una possibile soluzione potrebbe essere quella di rafforzare il contesto legale ad oggi inadeguato a regolamentare la materia***: occorre individuare una metodologia unitaria e conforme al nostro ordinamento che permetta di motivare ogni provvedimento elaborato dall'IA.

Perdita di posti di lavoro: Uno dei pensieri ricorrenti quando si parla di IA è che l'automazione di compiti sanitari da parte dell'IA potrebbe portare alla perdita di posti di lavoro per i professionisti sanitari. Occorre comprendere come l'utilizzo dell'IA comporti una necessaria riorganizzazione dei processi lavorativi. ***Bisognerà "accompagnare la trasformazione" creando nuovi posti di lavoro che sfruttino l'AI*** : è necessario, da una parte, creare una cultura interna che riesca ad implementare le capacità dei dipendenti e, dall'altra parte, favorire l'accettazione delle tecnologie da parte dell'utente tramite l'implementazione dell'uso delle piattaforme IA.

Problemi di privacy e sicurezza: I sistemi di IA raccolgono e archiviano grandi quantità di dati sanitari sensibili, che devono essere protetti da accessi non autorizzati e violazioni dei dati. ***Bisognerà pertanto tracciare nitidamante il ruolo dei dati***: è necessario creare le condizioni che consentano all'AI di utilizzare una rete di dati coretti ed intellegibila. Al fine di raggiungere gli obiettivi programmati, occorre disporre di dati veritieri e completi, regolamentare in maniera corretta l'utilizzo delle informazioni raccolte e supervisionare la qualità dei dati. Bisognerà, infine, tracciare molto bene i princi etici e di **responsabilità nel campo della tecnologia ed i loro confini**: Chi è responsabile in caso di errore commesso da un sistema di IA? È necessario stabilire linee guida chiare per attribuire responsabilità legali ed etiche. Occorrerà quindi rinforzare il framework etico in materia di protezione dei dati raccolti: i sistemi intelligenti necessitano di dati appuntati da esseri umani e, pertanto, nell'ambito sanitario è d'uopo che il personale sanitario inserisca in maniera corretta le informazioni contenute nelle prescrizioni mediche, evitando errori di comprensione o scrittura del testo. Il funzionamento della digitalizzazione richiede altresì un sistema trasparente al fine di evitare discriminazioni, garantendo al cittadino la comprensione delle decisioni elaborate dal personale e tutelando i propri dati personali.

Il sitema sociale, per non implodere, dovrebbe quindi mentenersi sempre "antropocentrico": l ***'essere umano*** è colui che "rischia" di più rispetto all'IA che con la sua forza innovativa ed inarrestabile potrebbe travolgerlo. L'IA coinvolgerà, infatti, gli aspetti esistenziali e psicologici più intrinseci dell'uomo. Il cittadini hanno perciò la necessità di sviluppare una visione coerente con la digitalizzazione tecnologie.

Dunque, la digitalizzazione e l'IA sebbene abbiano creato una nuova realtà contraddistinta da innumerevoli vantaggi, rappresenta ancora oggi un'area pervasa da zone grigie: un ulteriore limite è rappresentato dalla qualità dei dati che, soltanto se puri e senza errori, garantiranno il corretto il funzionamento dell'intelligenza.

Conclusioni

Il diritto alla protezione dei dati personali ha acquisito una importanza sistematica all'interno degli ordinamenti nazionali, incluso quello italiano, a fronte di tutte le sfide della contemporaneità, specialmente l'innovazione digitale e il progresso tecnologico, cha attraversano ogni aspetto della società.

È un diritto fondamentale che si inserisce e si integra nel novero dei diritti della persona e che necessita di un'attenzione particolare, per adeguare le forme di tutela della personalità proprie delle categorie tradizionali alle nuove esigenze del mondo che evolve. Tale diritto assume una veste significativa e peculiare in relazione al trattamento di dati sensibili, tra cui rientrano i dati relativi alla salute. Essi, infatti, presentano uno stretto legame con l'identità e l'intimità della vita di ciascuno, sostanziando – per usare una felice espressione della dottrina civilistica – *situazioni giuridiche esistenziali* della persona. La protezione dei dati personali assume varie declinazioni fra le quali assume una peculiare rilevanza quella che investe i profili particolari del trattamento di dati relativi alla salute, principalmente in ambito sanitario. Il consenso dell'individuo, quale strumento per garantirne l'autodeterminazione e, pertanto, per tutelare la persona - assume un ruolo centrale.

La problematica dei rischi connessi al trattamento dei dati sulla salute è particolarmente sentita, non solo ai fini della tutela della riservatezza della persona, ma anche per la salvaguardia dei suoi diritti e delle sue libertà fondamentali.

Si tratta di questioni che si ponevano già quando ancora si usava solo il supporto cartaceo, ma che si pongono in misura maggiore con l'utilizzo dei mezzi informatici e dell'AI.

Oggi abbiamo acquisito la piena consapevolezza della vulnerabilità della persona ed abbiamo compreso la delicatezza e la rilevanza della condizione del soggetto i cui dati più sensibili siano oggetto di trattamento; ciò ha portato ad elaborare un nuovo quadro giuridico che garantisca la tutela più idonea. Distinguere fra dati comuni e dati sensibili permette di assoggettare il trattamento di questi ultimi a regole differenti, per una migliore protezione della persona.

La giurisprudenza – nell'esperienza giuridica italiana – individua, a partire dall'assetto normativo, dati supersensibili o sensibilissimi, quali i dati sull'orientamento sessuale, la vita sessuale, i dati genetici e biometrici e i dati relativi alla salute.

Regole più stringenti per il trattamento di dati sensibili garantiscono un livello più

elevato di tutela della riservatezza. Esse, però, si concepiscono non tanto per motivi di privacy, quanto perché sono in gioco le libertà e i diritti fondamentali della persona.

Tutta la disciplina della protezione dei dati personali si fonda sulla necessità di bilanciare vari interessi e diritti. Operare un bilanciamento richiede però di considerare anche il rilievo pubblicistico dei dati: gli interessi sottesi tanto alla circolazione dei dati quanto alla difesa dell'individuo hanno anche una "dimensione pubblica e collettiva" che ci impedisce di considerare la questione come collegata solo ad una riflessione sul diritto dei privati.

Perciò il divieto di trattamento di cui all'art. 9, par. 1, non è assoluto, ma trova molte deroghe al par. 2 dello stesso articolo. Si tratta di fattispecie eccezionali che possono spiegarsi come cause di giustificazione. Fra queste, il consenso esplicito dell'interessato è solo una delle varie ipotesi che caratterizza le operazioni di trattamento di dati sensibili.

Dalla frequenza e dall'estensione della formulazione di queste deroghe non deriva, però, l'inversione del rapporto regola-eccezione che pervade l'art. 9 e che riflette la preminenza del principio personalistico rispetto agli altri principi da cui derivano le eccezioni al divieto.

Sono state esaminate, nel dettaglio, le caratteristiche dei dati relativi alla salute. Partendo dalla definizione dell'espressione – per la cui relativa nozione è stata essenziale l'interpretazione della Corte di giustizia dell'Unione europea – si è ragionato sul concetto di sensibilità di questa particolare categoria di dati personali.

I dati relativi alla salute possono quindi contenere informazioni di diverso tipo, il trattamento delle quali, conseguentemente, non rappresenta un medesimo rischio per i diritti della persona. Dei dati sanitari esiste quindi un diverso "*gradiente* di sensibilità"che, a sua volta, giustifica misure eccezionali a difesa della persona e della sua dignità.

Nell'ordinamento interno, una norma che rispecchia l'assunto è l'art. 5 D.P.C.M. n.178/2015, relativo al trattamento di dati operato mediante fascicolo sanitario elettronico.

Una serie di dati estremamente sensibili, come quelli sulla condizione del paziente sieropositivo all'HIV o sulla donna che abbia effettuato una interruzione di gravidanza, è soggetta a oscuramento di *default* all'interno del fascicolo stesso. Particolare cautela e rigore nei confronti di informazioni di questo genere – su tutte, quella del paziente affetto da HIV – sono mostrati anche dalla giurisprudenza della Corte europea dei diritti dell'uomo.

Le disposizioni che regolano il trattamento di dati relativi alla salute sono distribuite su più piani, secondo l'insieme di fonti multilivello proprio della materia. Dal diritto internazionale, al diritto sovranazionale – eurounitario – fino al diritto nazionale e, nel diritto interno, seguendo la gerarchia delle fonti.

Nel sistema giuridico italiano, l'entrata in vigore del Regolamento ha portato a un rilevante mutamento dell'orizzonte normativo sulla protezione dei dati sanitari. E ciò non tanto per una novità delle disposizioni del Regolamento, che spesso ricalcano quelle della Direttiva n. 46 del 1995, ma per la loro diretta applicabilità. L'ampia discrezionalità che la Direttiva lasciava agli Stati nel darvi attuazione ha determinato scelte "interne" in cui il sistema di tutela si basava sul consenso dell'interessato, unitamente alle autorizzazioni dell'Autorità garante.

Le disposizioni del Regolamento, direttamente applicabili, hanno prodotto invece un modello di protezione dei dati relativi alla salute che si contraddistingue per la pluralità di possibili basi giuridiche del trattamento e di fattispecie di deroga, in cui il consenso non è più centrale, e in questo modo, hanno valorizzato anche esigenze diverse da quelle del singolo.

Il settore in cui maggiormente vengono in rilievo i trattamenti di dati relativi alla salute è quello sanitario, in cui rilevano non solo le operazioni di trattamento dei dati finalizzate all'erogazione dei servizi assistenziali e di cura, ma anche quelle che hanno fini di ricerca e di gestione della sanità.

Per l'interpretazione delle disposizioni sul trattamento di dati relativi alla salute in ambito sanitario, è stata ed è tuttora fondamentale l'attività del Garante per la protezione dei dati personali. Particolarmente incisivi sono stati i chiarimenti che fornì con il provvedimento n. 55 del 2019, in cui dava atto del rinnovamento del quadro giuridico, a seguito dell'applicabilità del Regolamento e dell'emanazione del d.lgs. n. 101 del 2018, di adeguamento del Codice della privacy, e della possibilità di riconsiderare la posizione del consenso dell'assistito in relazione ai trattamenti svolti mediante il fascicolo sanitario elettronico.

Il Regolamento, in ogni caso, non elimina del tutto la discrezionalità degli Stati membri nell'adeguare la normativa interna e, come disposto dell'art. 9, par. 4, permette a questi ultimi di prevedere condizioni ulteriori, incluse limitazioni, per il trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Dai dati relativi alla salute vanno concettualmente tenuti distinti i dati genetici e i dati biometrici, pur considerando che talvolta, in concreto, può essere molto difficile separare le nozioni e identificare univocamente un dato personale come dato genetico o biometrico o relativo alla salute, per via delle sovrapposizioni definitorie che originano dalla lettera del Regolamento.

È stato evidenziato quanto il ruolo del consenso dell'interessato sia cruciale per la tutela della persona, in relazione al trattamento dei dati personali, dal momento che "storicamente" ha connotato il modo di concepire la protezione dei dati, come strumento di controllo sulla circolazione delle informazioni inerenti al soggetto ed espressione del diritto all'autodeterminazione informativa.

Ragionando sull'autodeterminazione informativa in ambito sanitario, si può osservare, peraltro, il parallelismo con l'autodeterminazione terapeutica – *habeas data, habeas corpus* – e la convergenza fra i due diversi tipi di autodeterminazione, in termini di consensualità, laddove si facciano più sensibili i dati relativi alla salute trattati.

Il solo consenso dell'interessato spesso però non è sufficiente a tutelare la persona dai pregiudizi derivanti dal trattamento di dati personali o a garantire un controllo effettivo sulla circolazione delle informazioni. La tutela della personalità viene dunque affidata ad altri strumenti, altri principi e altre regole, che possono ricondursi, semplificando, all'idea di sicurezza. Si pensi al principio di accountability, alle nozioni di privacy by design e privacy by default, alle procedure di pseudonimizzazione e ai meccanismi di valutazione del rischio.

Avendo riguardo al contesto sanitario, in cui il titolare del trattamento è, spesso, un soggetto pubblico, possiamo cogliere il superamento della regola di diritto privato da parte di quella di diritto pubblico o forse, meglio, amministrativo, in una amministrativizzazione della protezione dei dati personali.

Da un alto il concetto di autodeterminazione come prerogativa affidata al consenso dell'interessato al trattamento dei dati personali risulta superato ma, d'altro canto, il potenziale della volontà della persona non può certo considerarsi esaurito. Il consenso, infatti, può essere concepito anche in altro modo rispetto a quello di base giuridica del trattamento e ciò può valere specialmente per il trattamento di dati relativi alla salute. Il consenso può essere inteso allora come assenso o accettazione oppure come dissenso o rifiuto e può modellarsi attraverso schemi di opt-in e opt-out, secondo diversi gradi di esercizio dell'autodeterminazione, al variare del diverso livello di sensibilità dei dati stessi.

Si sono presi in esame, infine, il contesto dello sviluppo tecnologico e le sfide che pone per la tutela della persona, con riferimento alla protezione dei dati personali e al trattamento di dati relativi alla salute. La digitalizzazione della sanità apre nuovi scenari, in cui gli utenti del servizio sanitario e la collettività tutta possono beneficiare di maggiori vantaggi e possibilità, ma allo stesso tempo si aggiungono rischi, che mettono a repentaglio le libertà e i diritti dei singoli.

Questo processo di ammodernamento della tecnologia è guidato dalle Istituzioni dell'Unione europea alla luce del principio personalista e dei valori democratici propri dell'Unione. Un grande impulso è dato, in questa direzione, dall'attività normativa dell'Unione, dagli atti di diritto derivato, già posti o solo proposti, che mirano a regolare le nuove realtà tecnologiche. La creazione dello Spazio europeo dei dati sanitari, è destinata ad avere un grande impatto nell'utilizzo dei dati relativi alla salute, non solo per scopi legati all'assistenza sanitaria, ma anche per le finalità proprie dell'uso secondario di questi dati.

Tra le più promettenti delle tecnologie emergenti, l'Intelligenza Artificiale è oggetto di attenzione particolare da parte del diritto, soprattutto per la sua portata trasversale all'interno della società e la potenziale incidenza sui diritti delle persone. I sistemi di intelligenza artificiale già trovano impiego in ambito sanitario, non solo per finalità di cura, ma anche di gestione della sanità, e operano anche mediante il trattamento di dati relativi alla salute.

Il Regolamento generale sulla protezione dei dati regola, all'art. 22, la fattispecie della c.d. decisione automatizzata, che è esito del trattamento algoritmico di dati. Anche in questo caso, quando il trattamento automatizzato abbia ad oggetto dati sensibili, la disciplina si fa più rigorosa, ed è riservato un ruolo al consenso dell'individuo, che può permettere l'assunzione della decisione che lo riguarda.

Il bilanciamento fra diversi interessi è compiuto dal Regolamento senza distinguere il diverso livello di sensibilità che si può riscontrare per i dati relativi alla salute. Potrebbe forse essere, invece, più consono al personalismo che è proprio della digitalizzazione europea, prevedere una disciplina differenziata a seconda del tipo di dato sanitario trattato, anche qui valorizzando il consenso del soggetto, o meglio la funzione della volontà in chiave di rimedio.

Agli sviluppi della tecnologia è stata impressa una maggiore accelerazione anche per via delle esigenze che si sono riscontrate durante la crisi per la pandemia di Covid-19. La sanità digitale si è mostrata una risorsa per far fronte ai bisogni nel tempo dell'emergenza sanitaria e gli ordinamenti hanno dettato apposite regole – anche se non sempre felici – per gestire l'impiego della tecnica al servizio delle persone.

Garantire l'effettiva protezione dei dati personali in questo frangente non è semplice, ma il riconoscimento di questo diritto, come diritto fondamentale della persona, non è mai venuto meno.

In questa fase di contingenza, il legislatore italiano ha deciso di eliminare la regola che richiedeva la necessaria acquisizione del consenso dell'assistito per l'alimentazione del

fascicolo sanitario elettronico, mediante i suoi dati personali.

Il fascicolo sanitario elettronico – la cui disciplina rappresenta forse uno degli aspetti salienti della regolamentazione del trattamento di dati relativi alla salute – è quindi passato ad essere da dispositivo principalmente per la persona a strumento primariamente per la pubblica amministrazione. Attraverso il fascicolo sanitario elettronico possono sì perseguirsi fini di cura, in termini di migliore assistenza del paziente, ma soprattutto possono conseguirsi obiettivi di efficienza, sul piano economico e gestionale, e di utilità per la ricerca, specialmente in ambito medico.

Il singolo non può impedire che sia attivato il suo fascicolo e che vi siano caricati dati e documenti sanitari inerenti alla sua condizione così come non può ottenere che quei dati e documenti vengano eliminati dal fascicolo.

Proprio questo potrebbe essere il contesto per un'applicazione concreta dell'idea di un diverso rilievo della volontà dell'individuo a seconda della sensibilità del dato trattato. Una disposizione che prevedesse un meccanismo di *opt-out*, di rimozione del dato, o eventualmente di chiusura del fascicolo stesso, quando ad essere trattati fossero dati estremamente sensibili, e ciò potesse risultare opportuno per il soggetto, potrebbe essere una forma di tutela della personalità idonea, a fronte dei rischi insiti nel trattamento di questi dati per il paziente, e tale da garantire il rispetto della sua dignità.

Ritornare all'assoggettamento di ogni trattamento di dati relativi alla salute al previo consenso dell'interessato non sarebbe la soluzione più idonea per una tutela della persona che tenga conto anche delle esigenze della collettività. Il ruolo del consenso dell'interessato è destinato via via a diminuire di importanza fino, probabilmente, a una sua consegna alla storia, almeno per così come lo si è conosciuto. Ciò non significa però che non possa continuare ad avere un ruolo la volontà della persona, in chiave di autodeterminazione. Questa invece sembra poter dispiegare le sue potenzialità quando ad essere trattati siano dati personali di sensibilità estrema, come lo sono certe tipologie di dati relativi alla salute.

Una volontà che agisca per quelle informazioni più delicate, e non necessariamente per ogni dato relativo alla salute, se, da un lato, inevitabilmente sacrifica una parte degli interessi attuali e potenziali sottesi al trattamento di dati, dall'altro, può avere il pregio di contribuire all'*empowerment* del paziente e, di converso, favorire una circolazione più libera dei dati personali che non presentino questa caratteristica di massima sensibilità.

Recuperare la volontà non significa, in ogni caso, accedere a un altro consenso di stampo modulistico, che solo aggraverebbe la condizione del sistema sanitario aumentandone

la burocrazia, ma solo adeguare la tecnologia alla condizione dell'essere umano.

Non significa nemmeno contrapporre la persona alla tecnologia. Pensare una tutela della personalità in questa chiave rimediale non significa concepire persona e tecnologia in una logica di contrapposizione, ma piuttosto di integrazione, conferendo alla tecnologia un limite, che ne funga anche da indirizzo per l'evoluzione futura.

Conclusivamente, e in sintesi, si può sostenere che:

- se dei dati relativi alla salute – che sono dati di particolari categorie – esiste un diverso gradiente di sensibilità, per cui il trattamento di alcune tipologie di dati sanitari può ledere in misura minore i diritti dell'interessato e il trattamento di altre può farlo molto di più, così che possono immaginarsi diversi regimi di tutela a seconda del livello di sensibilità dei dati stessi; e se è possibile che a livello nazionale siano contemplate ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati relativi alla salute;
- se il consenso dell'interessato ha natura multiforme e, anche se non è più la condizione di liceità del trattamento di dati personali per eccellenza, riveste ancora un ruolo nell'ambito della disciplina della protezione dei dati; e se, più in generale, il consenso della persona – quindi la sua volontà – può astrattamente declinarsi in forme di autodeterminazione diverse dal consenso dell'interessato come base giuridica per la legittimità del trattamento, come può immaginarsi per la manifestazione di un dissenso o un meccanismo di *opt-out* rispetto al trattamento di dati;
- se l'avvento delle tecnologie più nuove e della digitalizzazione implica operazioni di trattamento di dati più numerose e con modalità differenti che mettono a repentaglio in misura maggiore rispetto al passato i diritti e le libertà dei soggetti e insieme pure apportano grandi vantaggi per la collettività; e se gli strumenti di tutela forniti dalla tecnologia stessa, l'implementazione di misure di sicurezza e l'attività delle Autorità amministrative – così come le misure sanzionatorie o gli istituti della responsabilità – rappresentano certo il futuro della protezione dei dati, in un paradigma non più consensocentrico e strettamente privatistico, ma solidaristico e più pubblicistico, senza tuttavia neutralizzare ogni possibile rischio legato alla circolazione dei dati, specialmente quelli sensibili;
- allora si può pensare al consenso della persona – o meglio la sua volontà – come a una nuova considerazione della tutela della personalità, un rimedio, inteso in termini negativi di dissenso, per realizzare l'autodeterminazione della persona, sempre tenendo a mente il necessario bilanciamento dei diritti e degli interessi sottesi al trattamento di dati personali.

Tale potrebbe essere un modello di *opt-out* applicato al fascicolo sanitario elettronico, soltanto per i dati più sensibili. In questo senso, una soluzione per garantire al soggetto una tutela adeguata sarebbe l'assoggettamento alla sua volontà della sola circolazione delle informazioni più sensibili, come sono i dati relativi alla salute con il più elevato gradiente di sensibilità, permettendo, a contrario, una circolazione più libera e slegata dalla volontà del soggetto dei dati sanitari non così sensibili, in modo che sia garantito l'*empowerment* del paziente e allo stesso tempo la realizzazione di finalità di interesse pubblico, come la ricerca o la programmazione sanitaria.

Come autorevolmente affermato dal Presidente dell'Autorità garante per la protezione dei dati personali, Pasquale Stanzione, con nota del 27/01/2023 "«Il dato sanitario è un valore fondamentale» perché è un valore fondamentale ciò che quell'informazione intimamente riguarda: la persona.

BIBLIOGRAFIA

Acciai, R. (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Santarcangelo di Romagna, Maggioli, 2004;

Acciai, R., *I trattamenti in ambito sanitario*, in Acciai, R. (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Santarcangelo di Romagna, Maggioli, 2004, 486 ss.;

Addante, A., *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*, in *Giust. civ.*, 2020, 889 ss.;

Adinolfi, A., e Simoncini, A. (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, Edizioni Scientifiche Italiane, 2022;

Agostinelli, B., *Informazione e minori: una lettura integrata per una tutela uniforme*, in *Jus civile*, 2022, 334 ss.;

Agrifoglio, G., *Risarcimento e quantificazione del danno da lesione della privacy: dal danno alla persona al danno alla personalità*, in *Eur. e dir. priv.*, 2017, 1265 ss.;

Aiello, G.F., *La protezione dei dati personali dopo il Trattato di Lisbona. Natura e limiti di un diritto fondamentale «disomogeneo» alla luce della nuova proposta di General Data Protection Regulation*, in *Osservatorio dir. civ. e comm.*, 2015, 421 ss.;

Ainis, M., *Circolazione dei dati personali e disciplina del mercato*, in Morace Pinelli, A. (a cura di), *La circolazione dei dati personali.*
Persona, contratto e mercato, Pisa, Pacini, 2023, 53 ss.;

Al Mureden, E., *Tutela della persona e limitazione dell'errore umano tra Advanced Driver Assistance Systems e guida automatizzata di livello 3*, in Garaci, I., e Montinaro, R. (a cura di), *La sostenibilità dell'innovazione digitale*, Napoli, Unior press, 2023, 299 ss.;

Alagna, I.M., Big data *e* People Analytics*: nuove sfide e opportunità per liberare valore*, in *Ciberspazio e diritto*, 2018, 339 ss.;

Albergo, F. (a cura di), Health Activity Based Costing. *L'analisi economica delle prestazioni sanitarie*, t. I, Milano, Giuffrè, 2020;

Albrecht, J.P., *Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung. Überblick und Hintergründe zum finalen Textfür die Datenschutz-Grundverordnung derEU nach der Einigung im Trilog*, in *Computer und Recht*, 2016, vol. 32, n. 2, 88 ss.;

Alovisio, M., *et al.*, *Videosorveglianza e privacy*, Forlì, Experta, 2011;

Alovisio, M., *Primi chiarimenti del Garante privacy sul trattamento dei dati in ambito sanitario*, in *www.dirittoegiustizia.it*, 21 marzo 2019;

Alovisio, M. (a cura di), *Videosorveglianza e GDPR. Profili di compliance nelle imprese e nelle pubbliche amministrazioni*, Milano, Giuffrè, 2021;

Alovisio, M., *L'impatto della legge di conversione del decreto capienze sulla privacy nel settore pubblico e sanitario*, in *www.diritt- toegiustizia.it*, 13 dicembre 2021;

Alovisio, M., *I nuovi poteri sanzionatori dell'Agenzia per la Cybersicurezza Nazionale in materia di certificazioni*, in *www.dirittoe- giustizia.it*, 24 agosto 2022;

Alpa G., e Bessone, M. (a cura di), *Banche dati, telematica e diritti della persona*, Padova, CEDAM, 1984; Alpa, G., voce

«Salute (diritto alla)», in *Noviss. Digesto it*., app. VI, Torino, Utet, 1986, 913 ss.;

Alpa, G., *Privacy e statuto dell'informazione (Il* privacy act*, 1974 e la* loi relative à l'informatique, aux fichiers et aux libertés n. 78- 17 del 1978*)*, in Bessone, M., e Giacobbe, G. (a cura di), *Il diritto alla riservatezza in Italia ed in Francia. Due esperienze a confronto*, Padova, CEDAM, 1988, 263 ss.;

Alpa, G., *Diritti della personalità emergenti: profili costituzionali e tutela giurisdizionale. Il diritto all'identità personale*, in *Giur. merito*, 1989, 464 ss.;

Alpa, G., e Resta, G., *Le persone e la famiglia*, I, *Le persone fisiche e i diritti della personalità*, nel *Trattato di diritto civile*, diretto da Sacco, 2a ed., Torino, Utet, 2019;

Alpa, G., *La "proprietà" dei dati personali*, in Zorzi Galgano, N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, CEDAM, 2019, 11 ss.;

Alpa, G. (a cura di), *Diritto e intelligenza artificiale*, Pisa, Pacini, 2020;

Alpa, G., *Prefazione*, in Alpa, G. (a cura di), *Diritto e intelligenza artificiale*, Pisa, Pacini, 2020, 13 s.;

Alpa, G., *Introduzione*, in Alpa, G. (a cura di), *I diritti della persona*, numero speciale di *Nuova giur. civ. comm*., 2020, 1 ss.;

Alpa, G., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 1, d.lgs. 30 giugno 2003, n. 196, 995 ss.;

Alpa, G., *Il mercato unico digitale*, in *Contr. e impr. Eur*., 2021, 1 ss.;

Alpa, G., *Quale modello normativo europeo per l'intelligenza artificiale?*, in Aa.Vv., *Per i cento anni dalla nascita di Renato Scognamiglio*, Napoli, Jovene, 2022, 21 ss.;

Alpa, G., *La "proprietà" dei dati personali*, in D'Auria, M. (a cura di), *I problemi dell'informazione nel diritto civile, oggi. Studi in*
onore di Vincenzo Cuffaro, Roma Tre-press, 2022, 21 ss.;

Alpa, G., *Salute e medicina*, in Alpa, G. (a cura di), *La responsabilità sanitaria. Commento alla l. 8 marzo 2017, n. 24*, 2a ed., Pisa, Pacini, 2022, 89 ss.;

Alpa, G., *Solidarietà. Un principio normativo*, Bologna, il Mulino, 2022;

Alpini, A., *Sull'approccio umano-centrico all'intelligenza artificiale. Riflessioni a margine del "Progetto europeo di orientamenti etici per una IA affidabile"*, in *www.comparazionedirittocivile.it*, aprile 2019;

Alpini, A., *Identità, creatività e condizione umana nell'era digitale*, in *Tecnologie e diritto*, 2020, 4 ss.;

Alpini, A., *La trasformazione digitale nella formazione del civilista*, in *Tecnologie e diritto*, 2021, fasc. 2, 1 ss.;

Alvisi, C., *Dati personali e diritti dei consumatori*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 669 ss.;

Alwan, A., *et al*., *Strengthening national health information systems: challenges and response*, in *Eastern Mediterranean Health Journal*, 2016, vol. 22, n. 11, 840 ss.;

Amato, G., *Democrazia e potere dei dati. A proposito di un recente libro del garante per la protezione dei dati personali*, in *Diritto di Internet*, 2019, 615 ss.;

Amato, S., *Caratteri del biodiritto*, in *Riv. fil. dir*., 2013, fasc. 1, 31 ss.;

Amato, S., *Abbandono terapeutico, ostinazione irragionevole e sedazione profonda*, in *Nuove leggi civ. comm*., 2019, 176 ss.; Amato, S., *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Torino, Giappichelli, 2020;

Amidei, A., *La proposta di Regolamento UE per un* Artificial Intelligence Act*: prime riflessioni sulle ricadute in tema di responsa- bilità da Intelligenza Artificiale*, in *Tecnologie e diritto*, 2022, 1 ss.;

Amore, G., Covid-19 *e Protezione dei dati personali*, in *Studium iuris*, 2020, 1159 ss.; Amore, G., *Digitalizzazione, protezione dei dati e terzo settore*, in *Jus civile*, 2022, 863 ss.;

Amoroso, A., e Roccetti, M., *Alcune considerazioni sociotecnologiche sul Fascicolo Sanitario Elettronico, con riferimento a quello della Regione Emilia-Romagna*, in *Salute e società*, 2017, fasc. 2, 97 ss.;

Amram, D., e Comandé, G., *Sul non facile coordinamento degli obblighi imposti dal Regolamento europeo sulla protezione dei dati personali UE/679/2016 e dalla legge n. 24/2017*, in *Riv. it. med. leg*., 2018, 1 ss.;

Amram, D., *Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health- data research: Comparative remarks*, in *Computer Law & Security Review*, vol. 37, 2020;

Angiolini, C., *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Torino, Giappichelli, 2020;

Angiolini, C., *Health and Data Protection*, in Iamiceli, P., Cafaggi, F., e Angiolini, C. (a cura di), *Casebook Judicial Protection of Health as a Fundamental Right*, Roma, Scuola Superiore della Magistratura, 2022, 126 ss.;

Annoni, A., e Thiene, A. (a cura di), *Minori e privacy. La tutela dei bambini e degli adolescenti alla luce del Regolamento (UE) 2016/679*, Napoli, Jovene, 2019;

Antoniazzi, S., *Le sanzioni amministrative*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1093 ss.;

Aperio Bella, F., *New health technologies and professional's liability. How public law can prevent "remote defensive medicine"?*, in Sandulli, M.A., e Aperio Bella, F. (a cura di), *Shaping the Future of Health Law: Challenges for Public Law*, in *www.fed- eralismi.it*, 17 novembre 2021, 5 ss.;

Aperio Bella, F., *The Role of Law in Preventing "Remote" Defensive Medicine: Challenges and Perspectives in the Use of Telemedcine*, in *Federalismi*, n. 1, 2023, *www.federalismi.it*, 11 gennaio 2023, 305 ss.;

Arcangeli, F., e Corsanego, P., *Le sanzioni amministrative*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 723 ss.;

Archer, N., *et al*., *Personal health records: a scoping review*, in *Journal of the American Medical Informatics Association*, 2011, vol. 18, n. 4, 515 ss.;

Ardissone, A., *La relazione medico-paziente nella sanità digitale. Possibili impatti sul professionalismo medico*, in *Rassegna italiana di sociologia*, 2018, fasc. 1, 77 ss.;

Arganelli, P., *App, Privacy e minori. La tutela dei minori in internet tra autodeterminazione informativa e fruizione dei contenuti digitali*, in *De Iustitia*, 2021, fasc. 2, 81 ss.;

Arzt, C., *Dal 1970 al 2007: tutela della* privacy *e protezione dei dati personali nella esperienza tedesca*, in Ferrari, G.F. (a cura di), *La legge sulla privacy dieci anni dopo*, Milano, EGEA, 2008, 125 ss.;

Astone, A., *Il trattamento dei dati personali dei minori nell'Unione europea: dai codici di condotta al Regolamento 2016/679*, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 441 ss.;

Astone, A., *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, Milano, Giuffrè, 2019;

Astone, A., *L'accesso dei minori d'età ai servizi della c.d. società dell'informazione: l'art. 8 del Reg. (UE) 2016/679 e i suoi riflessi sul codice per la protezione dei dati personali*, in *Contr e impr*., 2019, 614 ss.;

Astone, A., *Capitalism of digital surveillance and digital disintermediation in the era of the pandemic*, in *European Journal of Privacy Law & Technologies*, 2020, fasc. 2, 165 ss.;

Astone, A., *Autodeterminazione nei dati e sistemi A.I.*, in *Contr. e impr*., 2022, 429 ss.;

Astone, A. *Consenso ed intelligenza artificiale: limiti e prospettive*, in Garaci, I., e Montinaro, R. (a cura di), *La sostenibilità dell'innovazione digitale*, Napoli, Unior press, 2023, 187 ss.;

Astone, M.A., Digital Services Act *e nuovo quadro di esenzione dalla responsabilità dei prestatori di servizi intermediari: quali prospettive?*, in *Contr. e impr*., 2022, 1050 ss.;

Auletta, T., *Riservatezza e tutela della personalità*, Milano, Giuffrè, 1978;

Aulino, L., *Consenso al trattamento dei dati e carenza di consapevolezza: il* legal design *come un rimedio* ex ante, in *Dir. inf*., 2020, 303 ss.;

Auricchio, A., voce «Autorizzazione (dir. priv.)», in *Enc. del dir*., IV, Milano, Giuffrè, 1959, 502 ss.;

Aurucci, P., e Pinto, P., *DNA e anonimizzazione: i possibili effetti negativi di un intervento legislativo sulla Ricerca medica*, in *Ciber- spazio e diritto*, 2018, 159 ss.;

Aurucci, P., *Protezione e libera circolazione dei dati personali nel contesto della ricerca medica in Italia. Risposte istituzionali ad un necessario nuovo bilanciamento*, in *Queste istituzioni*, 2022, fasc. 4, 174 ss.;

Autero, E., e Castelli, A., *Intelligenza Artificiale e procedimento amministrativo: paura di cadere o voglia di volare?*, in *Ciberspazio e diritto*, 2020, 399 ss.;

Avdeeva, O., e Elias, M. (a cura di), *Bulgaria: Health system review. Health Systems in Transition*, in *www.euro.who.int*, 2007;

Avitabile, A., *Il* data protection officer, in Finocchiaro, G. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 331 ss.;

Balducci Romano, F., *La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo*, in *Riv. it. dir. pubbl. com.*, 2015, 1619 ss.;

Balducci Romano, F., *I trasferimenti di dati personali*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 949 ss.;

Balducci Romano, F., *Il diritto di proporre reclamo: aspetti sostanziali e procedurali di uno strumento di tutela multilivello*, in D'Au- ria, M. (a cura di), *I problemi dell'informazione nel diritto civile, oggi. Studi in onore di Vincenzo Cuffaro*, Roma Tre- press, 2022, 489 ss.;

Balducci Romano, F., *Le tutele dinanzi al Garante della privacy. Reclami, segnalazioni e sanzioni*, Pisa, Pacini, 2022;

Balduzzi, R., *Ci voleva l'emergenza Covid-19 per scoprire che cos'è il Servizio sanitario nazionale? (con un approfondimento su un ente poco conosciuto, l'INMP)*, in *Corti supreme e salute*, 2020, fasc. 1, 67 ss.;

Balduzzi, R., *et al*., *Come il diritto sanitario può aiutare oggi e nel dopo-pandemia. Lo chiediamo a non giuristi*, in *Corti supreme e salute*, 2020, fasc. 3, 715 ss.;

Balsamo, F., *La protezione dei dati personali di natura religiosa*, Cosenza, Luigi Pellegrini Editore, 2021;

Barba, A., *Le modalità del trattamento*, in Cuffaro, V., e Ricciuto, V. (a cura di), *La disciplina del trattamento dei dati personali*, Torino, Giappichelli, 1997, 127 ss.;

Barba, A., e Pagliantini, S. (a cura di), *Delle persone. Leggi collegate*, II, nel *Commentario del Codice civile*, diretto da Enrico Ga- brielli, Torino, Utet, 2019;

Barbareschi, S., e Giubilei, A., *L'equilibrio tra la tutela dei dati personali e la manifestazione del pensiero*, in Cuffaro, V., D'Orazio,
R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 453 ss.;

Barbarossa, M., *et al*., *La responsabilità civile e danno da trattamento illecito dei dati alla luce del Regolamento UE 2016/679*, in Cassano, G., *et al.* (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018, n. 101*, Milano, Giuffrè, 2018, 359 ss.;

Barbierato, D., *Osservazioni sul diritto all'oblio e la (mancata) novità del Regolamento UE 2016/679 sulla protezione dei dati personali*, in *Resp. civ. e prev.*, 2017, 2100 ss.;

Barbierato, D., *Trattamento dei dati personali e «nuova» responsabilità civile*, in *Resp. civ. e prev*., 2019, 2151 ss.;

Barfield, W., e Pagallo U., *Advanced Introduction to Law and Artificial Intelligence*, Cheltenham, Elgar, 2020;

Bardari, U., *Sicurezza dei dati e valutazione dei rischi*, in Cassano, G., *et al.* (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018, n. 101*, Milano, Giuffrè, 2018, 155 ss.;

Bargelli, E., in Bianca, C.M., e Busnelli, F.D. (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196, Codice della privacy*, Padova, CEDAM, 2007, *sub* art. 7, 130 ss.;

Bargelli, E., in Bianca, C.M., e Busnelli, F.D. (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196, Codice della privacy*, Padova, CEDAM, 2007, *sub* art. 15, comma 2°, 410 ss.;

Barilà, E., e Caputo, C., *Problemi applicativi della legge sulla privacy: il caso delle cartelle cliniche*, in *Pol dir*., 1998, 275
ss.;

Barraco, E., e Sitzia, A., *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, Milano, Ipsoa, 2016;

Basilica, F., *Il difficile percorso della formalizzazione giuridica dei diritti della personalità c.d. atipici*, in *Riv. dir. civ*., 2005, 677 ss.;

Bassini, M., *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quaderni costituzionali*, 2016, 587 ss.;

Bassini, M., *Il diritto costituzionale alla* privacy *nel prisma dell'evoluzione tecnologica*, in *Dir. cost*., 2023, fasc. 1, 83 ss.;

Bassini, S., *L'Italia nella corsa globale per il supercalcolo*, in *Pandora Rivista*, 2021, fasc. 1 *Frontiere*, 104 ss.;

Basunti, C., *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. e impr*., 2020, 860 ss.;

Battaini, F., *La tutela della privacy nelle strutture sanitarie*, in *Nuova rass.*, 1998, 609 ss.;

Battelli, E., Insurtech *ed evoluzione dell'offerta di polizze sanitarie: tra innovazione tecnologica e nuovi servizi assicurativi in campo medico*, in *Contr. e impr*., 2022, 52 ss.;

Battelli, E., *Commercializzazione dei dati e consenso digitale*, in Battelli, E. (a cura di), *Diritto privato digitale*, Torino, Giappichelli, 2022, 113 ss.;

Bellabarba, M., *Il trasferimento all'estero dei dati personali*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. II, Milano, Giuffrè, 2006, 1707 ss.;

Bellavista, A., *Società della sorveglianza e protezione dei dati personali*, in *Contr. impr*., 1996, 63 ss.; Bellavista, A., *Il trattamento dei dati sensibili nei rapporti di lavoro*, in *Dir. e prat. lav.*, 1998, 23 ss.; Bellavista, A., *Le autorizzazioni n. 2 e 5 al trattamento dei dati sensibili*, in *Dir. e prat. lav*., 1998, 475 ss.; Bellavista, A., *Le autorizzazioni nn. 3, 4 e 6 al trattamento dei dati sensibili*, in *Dir. e prat. lav*., 1998, 550 ss.;

Bellavista, A., *La tutela dei dati personali nel rapporto di lavoro*, in Cardarelli, F., Sica, S., e Zeno-Zencovich, V. (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, Giuffrè, 2004, 397 ss.;

Bellavista, A., *Il futuro della protezione dei dati personali dei lavoratori*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. II, Milano, Giuffrè, 2006, 1685 ss.;

Bellezit, J., *Dignité humaine et protection contre les discriminations en droit francais*, in De Carli, P. (a cura di), *Europa dei valori.*
Primo rapporto ACEV, Padova, CEDAM, 2022, 50 ss.;

Bellisario, E., *Il pacchetto europeo sulla responsabilità per danni da prodotti e da intelligenza artificiale. Prime riflessioni sulle Proposte della Commissione*, in *Danno e resp*., 2023, 153 ss.;

Bellomo, G.A.M., *"There ain't no such thing as a free lunch". Una riflessione sui meccanismi di mercato dell'economia digitale e sull'effettività delle tutele esistenti*, in *Concorrenza e mercato*, 2016, 205 ss.;

Belov, M., *The impact of EU Regulation 2016/679 on the Bulgarian Health System*, in Fares, G. (a cura di), *The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis*, Torino, Giappichelli, 2021, 101 ss.;

Beltrán Aguirre, J.L., *Reglamento general de protección de datos: novedades. Adaptación de la normativa española: el proyecto de LOPD*, in *Derecho y Salud*, Vol. 28, Extraordinario XXVII Congreso, 2018, 74 ss.;

Benciolini, P., *Obiezione di coscienza alle DAT? Ordinamento deontologico e ordinamento statuale*, in *Nuove leggi civ. comm*., 2019, 153 ss.;

Benedetti, A.M., *Contratto, algoritmi e diritto civile transnazionale: cinque questioni e due scenari*, in *Riv. dir. civ*., 2021, 411 ss.; Bergé, J.-S., Grumbach, S., e Zeno-Zencovich, V., *The 'Datasphere', Data Flows Beyond Control, and the Challenges for Law and*
Governance, in *European Journal of Comparative Law and Governance*, vol. 5, n. 2, 2018;

Bernardini, M.G., e Giolo, O., *L'algoritmo alla prova del caso concreto: stereotipi, serializzazione, discriminazione*, in Giolo, O. (a cura di), *L'algoritmo alla prova del caso concreto: stereotipi, serializzazione, discriminazione*, in *GenIUS*, 2022, fasc. 1, 6 ss.;

Bernes, A., *La protezione dei dati personali nell'attività di ricerca scientifica*, in *Nuove leggi civ. comm.*, 2020, 175 ss.;

Bernes, A., *Regolare la tecnologia di digital contact tracing alla luce della protezione dei dati personali*, in *Jus civile*, 2020, 1279 ss.;

Bernes, A., *Dati e ricerca genetica. Dalla tutela individuale alla gestione procedurale*, in *BioLaw Journal - Rivista di BioDiritto, Special issue* 1, 2022, 67 ss.;

Bernes, A., Privacy Enhancing Technologies, *trasparenza e tutela della persona nell'ambiente digitale*, in Orlando, S., e Capaldo, G. (a cura di), *Annuario 2022 Osservatorio Giuridico sulla Innovazione Digitale*, Roma, sapienza Università Editrice, 2022, 23 ss.;

Berti Suman, A., *Intelligenza artificiale e soggettività giuridica: quali diritti (e doveri) dei robot?*, in Alpa, G. (a cura di), *Diritto e intelligenza artificiale*, Pisa, Pacini, 2020, 251 ss.;

Bennett, C.J, *Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?*, in *International Data Privacy Law*, vol. 6, n. 4, 2016, 261 ss.;

Beyleveld, D., *et al.* (a cura di), *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*, Farnham, Ashgate, 2004;

Beyleveld, D., e Brownsword, R., *Consent in the Law*, Londra, Bloomsbury Publishing PLC, 2007;

Biagi, M., e Salomone, R., *L'Europa sociale e il diritto al lavoro: il ruolo della "*European Social Charter*"*, in *Lav. nella giur*., 2000, 414 ss.;

Bianca, C.M., e Busnelli, F.D. (a cura di), *Tutela dei dati personali. Commentario alla l. 31 dicembre 1996, n. 675*, Padova, CEDAM, 1999;

Bianca, C.M., e Busnelli, F.D. (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196, Codice della privacy*, Padova, CEDAM, 2007;

Bianca, M., *Il minore e i nuovi* media, in Senigaglia, R. (a cura di), *Autodeterminazione e minore età. Itinerari di diritto minorile*, Pisa, Pacini, 2019, 145 ss.;

Bianca, M., *La* filter bubble *e il problema dell'identità digitale*, in *MediaLaws*, 2019, fasc. 2, 39 ss.;

Biancardo, A., *Problematiche etico giuridiche relative all'utilizzo dell'intelligenza artificiale in ambito sanitario*, in *Jus. Vita e pen- siero*, 2021, fasc. 3, 102 ss.;

Bianchedi, G., *Il consenso dei minori per i servizi della società dell'informazione sotto il profilo giuridico e informatico*, in *Ciber- spazio e diritto*, 2019, 389 ss.;

Bieresborn, D., *Sozialdatenschutz nach Inkrafttreten der EU-Datenschutzgrundverordnung – Anpassungen des nationalen Sozialda- tenschutzes an das europäische Recht*, in *Neue Zeitschrift für Sozialrecht*, 2017, 887 ss.;

Bieresborn, D., *Sozialdatenschutz nach Inkrafttreten der EU-Datenschutzgrundverordnung – Verarbeiten von Sozialdaten, Reich- weite von Einwilligungen, grenzüberschreitende Datenübermittlung und Auftragsverarbeitung*, in *Neue Zeitschrift für So- zialrecht*, 2017, 926 ss.;

Biferali, G., *Big data e valutazione del merito creditizio per l'accesso al peer to peer lending*, in *Dir. inf.*, 2018, 487 ss.;

Bifulco, R., *Codici di condotta e regole deontologiche, dopo il d.lgs. n. 101/2018*, in Pizzetti, F. (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, Giappichelli, 2021, 337 ss.;

Bilotta, F., *L'emersione del diritto alla privacy*, in Clemente, A. (a cura di), *Privacy*, Padova, CEDAM, 1999, 21 ss.;

Bilotta, F., e Liberati, A., *Diritto di accesso ai documenti amministrativi e trattamento dei dati personali*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. II, Milano, Giuffrè, 2006, 2145 ss.;

Bilotta, F., *La responsabilità civile nel trattamento dei dati personali*, in Panetta, R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, Milano, Giuffrè, 2019, 445 ss.;

Bilotti, E., *L'accrescimento ereditario secondo Renato Scognamiglio. Ritorno al futuro*, in *Riv. dir. civ.*, 2022, 629 ss.; Bin,

M., *Privacy e trattamento dei dati personali: entriamo in Europa*, in *Contr. e impr. Eur.*, 1997, 459 ss.;

Bincoletto, G., mHealth app *per la televisita e il telemonitoraggio. Le nuove frontiere della telemedicina tra disciplina sui dispositivi medici e protezione dei dati personali*, in *BioLaw Journal - Rivista di BioDiritto*, 2021, 381 ss.;

Blasimme, A., e Vayena, E., *The Ethics of AI in Biomedical Research, Patient Care, and Public Health*, in Dubber, M.D., Pasquale,F. e Das, S. (a cura di), *The Oxford Handbook of Ethics of AI*, Oxford University Press, 2020, 703 ss.;

Blume, P., *Will it be a better world? The proposed EU Data Protection Regulation*, in *International Data Privacy Law*, vol. 2, n. 3, 2012, 130 ss.;

Bocchini, F., *Le cartelle cliniche. Funzioni, documento, prova*, in *Riv. it. med. leg.*, 2018, 35 ss.;

Bocciolesi, E., e de Lucia, A. (a cura di), *Proposte interdisciplinari come contributi per ripartire nella società post-Covid-19*, Napoli, Edizioni Scientifiche Italiane, 2023;

Bodei, R., *Dominio e sottomissione. Schiavi, animali, macchine, Intelligenza Artificiale*, Bologna, il Mulino, 2019;

Bologna, S., *et al*., *Electronic Health Record in Italy and Personal Data Protection*, in *European Journal of Health Law*, n. 23, 2016, 265 ss.;

Bonavita, S., e Pardolesi, R., *GDPR e diritto alla cancellazione (oblio)*, in *Danno e resp.*, 2018, 269 ss.;

Bonetti, S., *La protezione dei dati personali del defunto: il nuovo art. 2-terdecies del Codice della* privacy *al vaglio delle Corti*, in Troiano, S. (a cura di), *Diritto privato e nuove tecnologie. Riflessioni incrociate tra esperienze giuridiche a confronto*, Napoli, Edizioni Scientifiche Italiane, 2022, 115 ss.;

Bonfanti, A., *La protezione dei dati personali nell'era digitale: considerazioni alla luce del quadro giuridico internazionale in materia di business e diritti umani*, in *Ciberspazio e diritto*, 2017, 477 ss.;

Bonifazi, F., *et al*., *Machine Learning Systems Applied to Health Data and System*, in *European Journal of Health Law*, vol. 27, n. 3, 2020, 242 ss.;

Boniolo, G., *The problematic side of precision medicine. A short voyage through some questions*, in Barilan, Y.M., *et al.* (a cura di),
Can precision medicine be personal; Can personalized medicine be precise?, Oxford University Press, 2022; Bonomi,

M.S., Privacy *e dati sanitari: le principali novità introdotte dal GDPR*, in *www.federalismi.it*, 17 ottobre 2018;

Bonsignori, R., *AIDS e contagio sessuale: profili penali e civili*, nel *Trattato della responsabilità civile e penale in famiglia*, diretto da Cendon, vol. I, Padova, CEDAM, 2011, 905 ss.;

Bontempi, V., Mocavini, G., e Tatì, E., *L'attività normativa del governo nel periodo 2020-2021*, in *Riv. trim. dir. pubbl*., 2022, 467 ss.;

Bonzagni, G., *Le comunicazioni elettroniche*, in Finocchiaro, G. (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 972 ss.;

Borgia, F., *Profili critici in materia di trasferimento dei dati personali verso i Paesi extra-europei*, in Cuffaro, V., D'Orazio, R., e
Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 961 ss.;

Borsellino, P., *"Biotestamento": i confini della relazione terapeutica e il mandato di cura*, in *Fam. e dir*., 2018, 789 ss.;

Botrugno, C., *La diffusione dei modelli di cura a distanza: verso un "diritto alla telesalute"?*, in *BioLaw Journal - Rivista di BioDi- ritto*, 2014, 161 ss.;

Botrugno, C., *Un diritto per la telemedicina: analisi di un complesso normativo in formazione*, in *Pol. dir*., 2014, 639 ss.;

Botrugno, C., *Telemedicina e trasformazione dei sistemi sanitari. Un'indagine di bioetica*, Roma, Aracne, 2018;

Botrugno, C., *Telemedicina ed emergenza sanitaria: un grande rimpianto per il nostro Paese*, in *BioLaw Journal - Rivista di BioDi- ritto*, *Special Issue* 1, 2020, 691 ss.;

Botrugno, C., *Telemedicina e diritto alla salute in carcere: stato dell'arte, rischi e opportunità*, in *BioLaw Journal - Rivista di Bio- Diritto*, 2021, 401 ss.;

Bossi Malafosse, J., *Introductory Report for updating Recommendation R (97) 5 of the Council of Europe on the Protection of medical Data*, Strasburgo, 15 giugno 2015, consultabile in *www.coe.int*;

Botta, C., *La tutela dei dati genetici tra innovazione tecnologica e diritti fondamentali della persona*, in *De Iustitia*, 2021, fasc. 2, 56 ss.;

Bottari, C., *L'inquadramento costituzionale del Fascicolo Sanitario Elettronico*, in *Salute e società*, 2017, fasc. 2, 65 ss.;

Bottos, G., *Il diritto di fronte alla tecnologia. Intervista a Giusella Finocchiaro*, in *Pandora Rivista*, 2020, fasc. 3 *Piattaforme*, 106 ss.;

Bovero, M., *Diritti deboli, democrazie fragili. Sullo spirito del nostro tempo*, in *Diritto e questioni pubbliche*, 2016, fasc. 2, 11 ss.;

Bozzi, L., *I soggetti coinvolti nell'attività di trattamento*, in Cuffaro, V., e Ricciuto, V. (a cura di), *La disciplina del trattamento dei dati personali*, Torino, Giappichelli, 1997, 97 ss.;

Bozzi, L., *Il diritto di conoscere le proprie origini*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1323 ss.;

Bozzi, L., *I dati del minore tra protezione e circolazione: per una lettura non retorica del fenomeno*, in *Eur. e dir. priv.*, 2020, 251 ss.;

Bravo, F., *Le condizioni di liceità del trattamento di dati personali*, in Finocchiaro, G. (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 110 ss.;

Bravo, F., *Data Management Tools and Privacy by Design and by Default*, in Senigaglia, R., Irti, C., e Bernes, A. (a cura di), *Privacy and Data Protection in Software Services*, Berlino, Springer, 2022, 85 ss.;

Bregolat y Obiols, E., *China y la revolución digital*, in *Revista de privacidad y derecho digital*, vol. 3, n. 11, 2018, 25 ss.;

Bregolat y Obiols, E., *Carta de China: Los cambios que exige la pandemia*, in *Política exterior*, vol. 34, n. 197, 2020, 40 ss.;

Brighi, R., Cybersecurity. *Dimensione pubblica e privata della sicurezza dei dati*, in Casadei, T., e Pietropaoli, S. (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano, Wolters Kluwer, 2021, 135 ss.;

Brighi, R., e Chiara, P.G., *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi*, n. 21, 2021, 18 ss., in *www.federalismi.it*, 8 settembre 2021; Brizzi, F., *Dati sanitari, GDPR, e Covid-19. Il caso della ricerca: tra scienza e diritto*, Milano, Key editore, 2021;
Brkan, M., *The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core*, in *European Constitutional Law Review*, vol. 14, n. 2, 2018, 332 ss.;

Brkan, M., *Privacy, data protection and the role of European Courts: Towards judicialisation and constitutionalisation of European privacy and data protection framework*, in González Fuster, G., Van Brakel, R., e De Hert, P. (a cura di), *Research Hand- book on Privacy and Data Protection Law. Values, Norms and Global Politics*, Cheltenham, Elgar, 2022, 274 ss.;

Brown, P., *On vulnerability. A critical introduction*, Londra, Routledge, 2021;

Brownsword, R., *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality*, in Gutwirth, S., *et al.* (a cura di), *Reinventing Data Protection?*, Berlino, Springer, 2009, 83 ss.;

Brownsword, R., *Law, Technology and Society. Reimagining the Regulatory Environment*, Londra, Routledge, 2019;

Brownsword, R., *Law, Technology, and Society: in a State of Delicate Tension*, in *Notizie di Politeia*, 2020, n. 137, 26 ss. ;

Brunetti-Pons, C., *La primauté de la personne et de la dignité humaine en droit francais*, in De Carli, P. (a cura di), *Europa dei valori.*
Primo rapporto ACEV, Padova, CEDAM, 2022, 22 ss.;

Brutti, N., *Intelligenza artificiale e responsabilità in ambito medico: la prospettiva statunitense*, in *Resp. med*., 2018, 473 ss.;

Brutti, N., *Le figure soggettive delineate dal GDPR: la novità del* data protection officer, in Tosi, E. (a cura di), *Privacy Digitale.*
Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy, Milano, Giuffrè, 2019, 115 ss.; Brutti, N.,

Le regole dell'informazione ambientale, tra pubblico e privato, in *Dir. inf*., 2022, 617 ss.;

Buccelli, C., e Casella, C. (a cura di), *Ricerche di Biodiritto*, di Carmine Dionisi, Napoli, Edizioni Scientifiche Italiane, 2020; Bugetti, M.N., *La disciplina del consenso informato nella legge 219/2017*, in *Riv. dir. civ*., 2019, 106 ss.;

Busacca, A., *Le "categorie particolari di dati" ex art. 9 GDPR. Divieti, eccezioni e limiti alle attività di trattamento*, in *Ordine internazionale e diritti umani*, 2018, 36 ss.;

Busca, N., *Chiarimenti sull'applicazione della disciplina di protezione dei dati in ambito sanitario*, in *www.rivistaresponsabilitame- dica.it*, 8 aprile 2019;

Busca, N., *Il trattamento dei dati sanitari nell'ambito della ricerca e della sperimentazione clinica*, in *www.rivistaresponsabilitame- dica.it*, 26 settembre 2020;

Busca, N., *GDPR e ricerca scientifica: i requisiti al trattamento dei dati sanitari nel pubblico interesse*, in *Resp. med*., 2020, 417 ss.; Busia, G., *I codici di deontologia e di buona condotta*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*,. I, Milano, Giuffrè, 2006, 201 ss.;

Busia, G., *Il ruolo dell'autorità indipendente per la protezione dei dati personali*, in Zorzi Galgano, N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, CEDAM, 2019, 293 ss.;

Buttarelli, G., *The geostrategic importance of data protection: an abstract of the edps 2018 annual report*, in Tosi, E. (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019, 677 ss.;

Buzzacchi, C., *La politica europea per i big data e la logica del Single market: prospettive di maggiore concorrenza?*, in *Concorrenza e mercato*, 2016, 153 ss.;

Buzzelli, D., e Palazzo, M. (a cura di), *Intelligenza artificiale e diritti della persona*, Pisa, Pacini, 2022;

Bygrave, L.A., *Data Privacy Law: An International Perspective*, Oxford University Press, 2014;

Bygrave, L.A., e Tosoni, L., in Kuner, C., Bygrave, L.A., e Docksey, C. (a cura di), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020, *sub* art. 4(1), 103 ss.;

Bygrave, L.A., e Tosoni, L., in Kuner, C., Bygrave, L.A., e Docksey, C. (a cura di), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020, *sub* art. 4(11), 174 ss.;

Bygrave, L.A., e Tosoni, L., in Kuner, C., Bygrave, L.A., e Docksey, C. (a cura di), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020, *sub* art. 4(13), 196 ss.;

Bygrave, L.A., e Tosoni, L., in Kuner, C., Bygrave, L.A., e Docksey, C. (a cura di), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020, *sub* art. 4(14), 207 ss.;

Bygrave, L.A., in Kuner, C., Bygrave, L.A., e Docksey, C. (a cura di), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020, *sub* art. 22, 522 ss.;

Cabazzi, R., *Utilizzo dei* cookie *e (nuova) tutela dell'utente interessato: la presa di posizione della Corte di Giustizia nel caso* Pla- net49, in *MediaLaws*, 2020, fasc. 2, 316 ss.;

Cacace, S., *Autodeterminazione in salute*, Torino, Giappichelli, 2017;

Cacace, S., *La nuova legge in materia di consenso informato e DAT: a proposito di volontà e di cura, di fiducia e di comunicazione*, in *Riv. it. med. leg*., 2018, 935 ss.;

Cacciari, S., *Scenari. Etica, antropologia, intelligenza artificiale*, in *Dir. inf*., 2019, 1175 ss.;

Caggia, F., *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, in Cuffaro, V., D'Orazio, R., e Ric-
ciuto, V. (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 405 ss.;

Caggia, F., *Libertà ed espressione del consenso*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 249 ss.;

Caggia, F., *Il consenso al trattamento dei dati personali nel diritto europeo*, in *Riv. dir. comm*., 2019, 405 ss.;

Caggia, F., *Cessione di dati personali per accedere al servizio digitale gratuito: il modello del "consenso rafforzato"*, in D'Auria, M. (a cura di), *I problemi dell'informazione nel diritto civile, oggi. Studi in onore di Vincenzo Cuffaro*, Roma Tre-press, 2022, 417 ss.;

Caggia, F., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e data protection*, Milano, Giuffrè, 2021, *sub* art. 7, reg. Ue n. 679/2016, 205 ss.;

Caggiano, I.A., *Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*, in *Familia*, 2018, 3 ss.;

Caggiano, I.A., *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamen- tali*, in *Osservatorio dir. civ. e comm.*, 2018, 67 ss.;

Cai, P., e Chen, L., *Demystifying data law in China: a unified regime of tomorrow*, in *International Data Privacy Law*, vol. 12, n. 2, 2022, 75 ss.;

Cal Purriños, N., *Inteligencia artificial. El uso de los datos de los pacientes*, in *Derecho y Salud*, vol. 31, Extraordinario,

2021, 86 ss.; Calabresi, G., e Bobbit, P., *Scelte tragiche*, Milano, Giuffrè, 1986 ;

Calzolaio, S., Privacy by design. *Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *www.federalismi.it*, 20 dicembre 2017;

Camardi, C., *Mercato delle informazioni e privacy. Riflessioni generali sulla l. n. 675/1996*, in *Eur. e dir. priv*., 1998, 1049 ss.; Camardi, C., *Certezza e incertezza nel diritto privato contemporaneo*, Torino, Giappichelli, 2017;

Camardi, C., *Relazione di filiazione e privacy. Brevi note sull'autodeterminazione del minore*, in *Jus civile*, 2018, 831 ss.;

Camardi, C., *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ*., 2019, 499 ss.;

Camardi, C., *Minore e privacy nel contesto delle relazioni familiari*, in Senigaglia, R. (a cura di), *Autodeterminazione e minore età.*
Itinerari di diritto minorile, Pisa, Pacini, 2019, 117 ss.;

Camardi, C., e Tabarrini, C., *Contact tracing ed emergenza sanitaria. "Ordinario" e "straordinario" nella disciplina del diritto al*
controllo dei dati personali, in *Nuova. giur. civ. comm*., 2020, suppl., 32 ss.;

Camardi, C., *Liability and Accountability in the 'Digital' Relationships*, in Senigaglia, R., Irti, C., e Bernes, A. (a cura di), *Privacy and Data Protection in Software Services*, Berlino, Springer, 2022, 25 ss.;

Camardi, C. (a cura di), *La via europea per l'intelligenza artificiale. Atti del convegno del progetto dottorale di alta formazione in scienze giuridiche, Ca' Foscari Venezia, 25-26 novembre 2021*, Padova, CEDAM, 2022;

Camardi, C., *Pluralismo e statuti giuridici delle persone*, in *Jus civile*, 2023, 64 ss.;

Camardi, C., *Sulla Governance digitale europea: una proposta di confronto*, in *Accademia*, 2023, 7 ss.;

Campagna, M., *Linee guida per la Telemedicina: considerazioni alla luce dell'emergenza Covid-19*, in *Corti supreme e salute*, 2020, fasc. 3, 599 ss.;

Candini, A., *Gli strumenti di tutela*, in Finocchiaro, G. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 569 ss.;

Candini, A., *Tutela amministrativa e giurisdizionale*, in Finocchiaro, G. (a cura di), *La protezione dei dati personali in Italia. Rego- lamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 742 ss.;

Canepa, C., *L'Italia e l'occasione persa del Fascicolo Sanitario Elettronico*, in *www.repubblica.it*, 27 luglio 2021;

Canestrari, S., *Consenso informato e disposizioni anticipate di trattamento: una "buona legge buona"*, in *Corr. giur*., 2018, 301 ss.;

Capilli, G., *La tutela dei dati personali dei minori*, in Panetta, R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, Milano, Giuffrè, 2019, 247 ss.;

Capilli, G., *I criteri di interpretazione delle responsabilità*, in Alpa, G. (a cura di), *Diritto e intelligenza artificiale*, Pisa, Pacini, 2020, 457 ss.;

Capilli, G., *Diritto privato sanitario. Fondamenti*, Pisa, Pacini, 2022;

Capogna, S., *Sanità digitale tra organizzazione e innovazione. Un caso di studio*, in *Salute e società*, 2017, fasc. 2, 35 ss.;

Caporale, M., *Aspetti particolari del trattamento dei dati personali in ambito pubblico: accesso ai documenti amministrativi e sistemi di identificazione personale*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 495 ss.;

Caporale, M., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 45 *bis*, d.lgs. 30 giugno 2003, n. 196, 1172 ss.;

Cappuccini, C., *La dimensione europea del diritto alla salute*, in Alpa, G. (a cura di), *La responsabilità sanitaria. Commento alla L.8 marzo 2017, n. 24*, Pisa, Pacini, 2017, 55 ss.;

Caravà, E., in Sciaudone, R., e Caravà, E. (a cura di), *Il codice della privacy. Commento al D.Lgs. 30 giugno 2003, n. 196 e al D.Lgs. 10 agosto 2018, n. 101 alla luce del Regolamento (UE) 2016/679 (GDPR)*, Pisa, Pacini, 2019, *sub* art. 2-*septies*, 85 ss.;

Carotti, B., *Pandemia e panopticon*, in *www.irpa.eu*, *Osservatorio sullo Stato digitale*, 23 aprile 2020;

Casonato, C., e Marchetti, B., *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, 2021, fasc. 3, 415 ss.;

Casonato, C., e Penasa, S., *Intelligenza artificiale e medicina del domani*, in Ferrari, G.F. (a cura di), *Le smart cities al tempo della resilienza*, Milano, Mimesis, 2021, 553 ss.;

Casonato, C., Fasan, M., e Penasa, S. (a cura di), *Diritto e intelligenza artificiale*, sezione monografica in *DPCE online*, 2022, fasc.
1, 155 ss.;

Cassano, G., *et al.* (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018, n. 101*, Milano, Giuffrè, 2018;

Cassano, G., Iaselli, M., e Spangher, G., *Cybersecurity: contesto normativo di riferimento a livello nazionale ed europeo*, in *Diritto di Internet*, 2022, 637 ss.;

Cassese, S., *Diritto privato/diritto pubblico: tradizione, mito o realtà?*, in Conte, G., *et al.* (a cura di), *Dialoghi con Guido Alpa. Un volume offerto in occasione del suo LXXI compleanno*, Roma Tre-Press, 2018, 51 ss.;

Castellaneta, M., *L'incidenza del regolamento GDPR sul quadro normativo esistente*, in *Notariato*, 2018, 259 ss.;

Castellaneta, M., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 8, CEDU, 3 ss.;

Castronovo, C., *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in Cuffaro, V., Ricciuto, V., e Zeno- Zencovich, V. (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffrè, 1999, 189 ss.;

Castronovo, C., e Mazzamuto, S. (a cura di), *Manuale di diritto privato europeo*, vol. I, *Fonti, persone e famiglia*, Milano, Giuffrè, 2007;

Catalano, R., e Venditti, C., *Questioni di biodiritto nella filmografia cyberpunk*, Napoli, Editoriale scientifica, 2017;

Catalano, R., *Biotecnologie e tutela giuridica dei diritti fondamentali della persona*, in Catalano, R., e Venditti, C., *Questioni di biodiritto nella filmografia cyberpunk*, Napoli, Editoriale scientifica, 2017, 7 ss.;

Catalano, F., *Il diritto alla portabilità dei dati tra interessi individuali e prospettiva concorrenziale*, in *Eur. e dir. priv*., 2019, 833 ss.;

Cataleta, A., *Categorie particolari di dati: le regole generali e i trattamenti specifici*, in Finocchiaro, G. (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 204 ss.;

Catallozzi, M., *I provvedimenti del Garante per la protezione dei dati personali*, in *Nuova giur. civ. comm*., 1998, II, 436

ss.; Cataudella, A., *La tutela civile della vita privata*, Milano, Giuffrè, 1974;

Caterina, R., *Novità e continuità nel Regolamento generale sulla protezione dei dati*, in Caterina, R. (a cura di), *GDPR tra novità e discontinuità*, in *Giur. it*., 2019, 2777;

Caterina, R., e Thobani, S., *Il diritto al risarcimento dei danni*, in Caterina, R. (a cura di), *GDPR tra novità e discontinuità*, in *Giur. it*., 2019, 2805 ss.;

Caterini, E., Artificial Intelligence, *persona e soggetto*, in *Tecnologie e diritto*, 2022, 207 ss.;

Caterini, E., Artificial Intelligence, *persona e soggetto*, in Garaci, I., e Montinaro, R. (a cura di), *La sostenibilità dell'innovazione*
digitale, Napoli, Unior press, 2023, 23 ss.;

Causarano, M.C., *GDPR e forme di autoregolamentazione privata: continuità e discontinuità nella disciplina dei codici di condotta*, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 247 ss.;

Colussi, I A., *Dai vichinghi agli oroscopi genetici: saghe islandesi passate e future*, in Casonato, C., Piciocchi, C., e Veronesi, P. (a cura di), *La disciplina delle biobanche a fini terapeutici e di ricerca*, Università degli Studi di Trento, 2012, 249 ss.;

Comandé, G., in Giannantonio, E., Losano, M.G., e Zeno-Zencovich, V. (a cura di), *La tutela dei dati personali. Commentario alla l.*
675/1996, Padova, CEDAM, 1997, *sub* artt. 11 e 12, 98 ss.;

Comandé, G., *Privacy informatica: prospettive e problemi*, in *Danno e resp*., 1997, 140 ss.;

Comandé, G., in Bianca, C.M., e Busnelli, F.D. (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003,*
n. 196, Codice della privacy, Padova, CEDAM, 2007, *sub* art. 15, comma 1°, 362 ss.;

Comandé, G., *Circolazione elettronica dei dati sanitari e regolazione settoriale: spunti ricostruttivi su «interferenze sistematiche»*, in Ruscello, F. (a cura di), *Studi in onore di Davide Messinetti*, I, Napoli, Edizioni Scientifiche Italiane, 2008, 279 ss.;

Comandé, G., Nocco, L., e Peigné, V., *Il fascicolo sanitario elettronico: uno studio multidisciplinare*, in *Riv. it. med. leg*., 2012, 105 ss.;

Comandé, G., *Ricerca in sanità e data protection un puzzle... risolvibile*, in *Riv. it. med. leg*., 2019, 187 ss.;

Comandé, G., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e data protection*, Milano, Giuffrè, 2021, *sub* art. 21, reg. Ue n. 679/2016, 366 ss.;

Comella, C., *Privacy e nuove tecnologie*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. II, Milano, Giuffrè, 2006, 1245 ss.;

Comunello, F., *Oltre le filter bubbles. Una riflessione sulla controversia vaccinale nei social media*, in *Riv. it. med. leg*., 2018, 311 ss.;

Contaldo, A., e Crea, G., *Il fascicolo sanitario elettronico con le puntualizzazioni operative delle fonti secondarie*, in *Diritto di Inter- net*, 2021, 423 ss.;

Conte, G., *Diritti dell'interessato e obblighi di sicurezza*, in Cuffaro, V., e Ricciuto, V. (a cura di), *La disciplina del trattamento dei dati personali*, Torino, Giappichelli, 1997, 225 ss.;

Conte, L., *La reazione allo stato di emergenza* Covid *nella prospettiva del sistema delle fonti*, in *Studium iuris*, 2020, 991 ss.;

Conti, S., e Peruginelli, G., *L'impatto del Regolamento europeo in materia di protezione dei dati personali sull'attività giurisdizionale*, in *Ciberspazio e diritto*, 2018, 123 ss.;

Corasaniti, G., *La sicurezza dei dati personali*, in Cardarelli, F., Sica, S., e Zeno-Zencovich, V. (a cura di), *Il codice dei dati personali.*
Temi e problemi, Milano, Giuffrè, 2004, 111 ss.;

Cordeiro, J.L., e Wood, D., *La muerte de la muerte. La posibilidad científica de la inmortalidad física y su defensa moral*, Zalla, Deusto, 2018;

Cordiano, A., *Identità della persona e disposizione del corpo. La tutela della salute nelle nuove scienze*, Roma, Aracne,

2011; Cordiano, A., *Biobanche di ricerca e modelli regolativi*, in *www.comparazionedirittocivile.it*, febbraio 2018;

Corrias, P. (a cura di), *I soggetti vulnerabili nella disciplina comune e nei mercati regolamentati*, Napoli, Edizioni Scientifiche Ita- liane, 2022;

Corso, G., *Diritto pubblico e diritto privato: il confine è mobile, ma esiste*, in Nivarra, L., e Plaia, A. (a cura di), *I mobili confini del diritto privato*, Torino, Giappichelli, 2018, 45 ss.;

Corso, L., *Vulnerabilità, giudizio di costituzionalità e sentimentalismo*, in *Ars interpretandi*, 2018, 57 ss.

Corso, S., *Salute e riserbo del paziente: questioni aperte in tema di cartella clinica*, in *Resp. med.*, 2017, 395 ss.;

Corso, S., *Brevi riflessioni sulla dimensione europea del diritto alla salute*, in *www.rivistaresponsabilitamedica.it*, 3 ottobre 2018;

Corso, S., *Il parere favorevole, ma non incondizionato, del Garante privacy sul d.P.C.m. di attuazione della piattaforma per il Green Pass*, in *www.rivistaresponsabilitamedica.it*, 18 giugno 2021;

Corso, S., *Modifiche alla disciplina sul trattamento dei dati relativi alla salute*, in *www.rivistaresponsabilitamedica.it*, 29 gennaio 2022;

Corso, S., *Il sì del Garante allo schema di d.P.C.m. sull'Anagrafe nazionale degli assistiti*, in *www.rivistaresponsabilitamedica.it*, 6 aprile 2022;

Corso, S., *Fascicolo sanitario elettronico, ecosistema dati sanitari, Agenzia nazionale per la sanità digitale: il governo della sanità digitale*, in *www.rivistaresponsabilitamedica.it*, 11 aprile 2022;

Corso, S., European Health Data Space. *La Commissione europea presenta la proposta di Regolamento sullo spazio europeo dei dati sanitari*, in *www.rivistaresponsabilitamedica.it*, 13 giugno 2022;

Corso, S., *Le Linee guida di attuazione del fascicolo sanitario elettronico*, in *www.rivistaresponsabilitamedica.it*, 31 luglio 2022; Corso, S., *Lo spazio europeo dei dati sanitari: la Commissione Europea presenta la proposta di regolamento*, in *www.federalismi.it*,
10 agosto 2022;

Corso, S., *Il parere congiunto del Comitato europeo per la protezione dei dati e del Garante europeo della protezione dei dati in merito alla proposta di Regolamento sullo spazio europeo dei dati sanitari*, in *www.rivistaresponsabilitamedica.it*, 5 set- tembre 2022;

Corso, S., *Fascicolo sanitario elettronico ed ecosistema dati sanitari. I pareri critici del Garante per la protezione dei dati personali al Ministero della salute*, in *www.rivistaresponsabilitamedica.it*, 22 settembre 2022;

Corso, S., *Sanità digitale e riservatezza. Interpretazioni sul fascicolo sanitario elettronico*, in Thiene, A., e Corso, S. (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza*, Napoli, Jovene, 2023, 91 ss.;

Corso, S., *Trasformazione digitale, digitalizzazione della sanità e intelligenza artificiale. La Dichiarazione europea sui diritti e i principi digitali e il programma strategico per il decennio digitale 2030*, in *federalismi.it, Osservatorio di diritto sanitario*, maggio 2023;

Corso, S., *Il trattamento dei dati relativi alla salute e la dignità della persona. La nota del Garante per la protezione dei dati personali*, in *federalismi.it, Osservatorio di diritto sanitario*, maggio 2023;

Corso, S., *Sulla* female technology *o* Femtech. *Intelligenza artificiale, salute della donna e volontà della persona*. in *BioLaw Journal*
- *Rivista di BioDiritto*, n. 3/2023;

Cortese, B., *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Dir. un. eur.*, 2013, 313 ss.;

Cortese, F., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 2 *sexies*, d.lgs. 30 giugno 2003, n. 196, 1044 ss.;

Costantino, F., *Lampi. Nuove frontiere delle decisioni amministrative tra open e big data*, in *Dir. amm.*, 2017, 799 ss.;

Costanza, M., *Brevi osservazioni sulla legge 31 dicembre 1996 n. 675. Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, in *Resp. comun. e impr*., 1997, 309 ss.;

Cottu, E., *L'impatto del Regolamento generale sulla protezione dei dati sul sistema punitivo a livello eurounitario e sovranazionale*, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 263 ss.;

Covino, F., *Uso della tecnologia e protezione dei dati personali sulla salute tra pandemia e normalità*, in *Federalismi*, fasc. 5, 2021,
42 ss., consultabile all'indirizzo *www.federalismi.it*, 12 febbraio 2021;

Cremona, E., Laviola, F., e Paganelli, V. (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Torino, Giappichelli, 2022;

Cremona, E., *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Napoli, Edizioni Scientifiche Italiane, 2023;

Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007;

Cuffaro, V., *Il diritto europeo sulla protezione dei dati personali e la sua applicazione in Italia: spunti per un bilancio*, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 23 ss.;

Cuffaro, V., *Il diritto europeo sul trattamento dei dati personali*, in *Contr. e impr.*, 2018, 1098 ss.;

Cuffaro, V., *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, in *Corr. giur.*, 2018, 1181 ss.;

Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019;

Cuffaro, V., *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 3 ss.;

Cuffaro, V., *Cancellare i dati personali. Dalla* damnatio memoriae *al diritto all'oblio*, in Zorzi Galgano, N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, CEDAM, 2019, 219 ss.;

Cuffaro, V., e D'Orazio, R., *La protezione dei dati personali ai tempi dell'epidemia*, in *Corr. giur.*, 2020, 729 ss.;

Cuocci, V.V., Lops, F.P., e Motti, C. (a cura di), *La responsabilità civile nell'era digitale. Atti della Summer school 2021*, Bari, Cacucci, 2022;

Cuttaia, F.G., *Il recupero della centralità del diritto alla salute. Prospettive di riforma del Servizio Sanitario Nazionale*, Torino, Giappichelli, 2022;

Cuttaia, F.G., *La dimensione europea del diritto alla salute e i suoi riflessi sull'ordinamento italiano*, in Alpa, G. (a cura di), *La responsabilità sanitaria. Commento alla l. 8 marzo 2017, n. 24*, 2a ed., Pisa, Pacini, 2022, 153 ss.;

Cupelli, C., e Fico, F., *I riflessi penalistici del Regolamento UE 2016/679 e le nuove fattispecie di reato previste nel Codice* privacy *dal d.lgs. n. 101/2018*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1107 ss.;

Cuttaia, F.G., *The impact of EU Regulation 2016/679 on the Italian health system*, in Fares, G. (a cura di), *The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis*, Torino, Giappichelli, 2021, 195 ss.;

D'Acquisto, G., e Naldi, M., Big data *e* privacy by design. *Anonimizzazione pseudonimizzazione, sicurezza*, Torino, Giappichelli, 2017;

D'Acquisto, G., *L'agenda digitale della protezione dei dati personali*, in Pizzetti, F. (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, Giappichelli, 2021, 299 ss.;

D'Agata, C., *Il legittimo interesse del titolare o di un terzo nel quadro dei diversi presupposti di legittimità del trattamento*, in Panetta,
R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, Milano, Giuffrè, 2019, 81 ss.;

D'Agnino, E., *La tutela della privacy ai tempi del coronavirus: profili giuslavoristici*, in *www.giustisizacivile.com*, 17 marzo 2020;

d'Agostino Panebianco, M., *Il trattamento dei dati nel Sistema Sanitario Nazionale italiano alla luce del Provvedimento del Garante del 7 marzo 2019*, in *Ciberspazio e diritto*, 2019, 241 ss.:

d'Agostino Panebianco, M., *Lineamenti di responsabilità derivanti dalla violazione al trattamento dati*, in *Eur. e dir. priv.*, 2020, 237 ss.;

D'Aloia, A., *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal - Rivista di BioDiritto*, 2019, fasc. 1, 3 ss.;

D'Aloia, A. (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, FrancoAngeli, 2021;

D'Aloia, A., *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in D'Aloia, A. (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, FrancoAngeli, 2021, 7 ss.;

D'Aloia, A., *Il diritto e l'incerto mestiere del vivere. Ricerche di biodiritto*, Padova, CEDAM, 2021;

D'Alterio, E., *Protezione dei dati personali e accesso amministrativo: alla ricerca dell'"ordine segreto"*, in *Giornale di diritto am- ministrativo*, 2019, 9 ss.;

De Cupis, A., *I diritti della personalità*, nel *Trattato Cicu-Messineo*, IV, 2a ed., Milano, Giuffrè, 1982;

De Felice, A., *Intelligenza artificiale e processi decisionali automatizzati: GDPR ed* ethics by design *come avamposto per la tutela dei diritti umani*, in D'Aloia, A. (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, FrancoAngeli, 2021, 415 ss.;

De Franceschi, A., *European Contract Law and the Digital Single Market: Current Issues and New Perspectives*, in De Franceschi,
A. (a cura di), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*, Cambridge, Intersentia, 2016, 1 ss.;

De Franceschi, A., *La circolazione dei dati personali tra* privacy *e contratto*, Napoli, Edizioni Scientifiche Italiane, 2017;

De Franceschi, A., *La circolazione dei dati personali nella proposta di Direttiva UE sulla fornitura dei contenuti digitali*, in Mante- lero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 203 ss.;

De Franceschi, A., *Il «pagamento» mediante dati personali*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1381 ss.;

De Franceschi, A., *La vendita di beni con elementi digitali*, Napoli, Edizioni Scientifiche Italiane, 2019;

De Franceschi, A., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 4, reg. Ue n. 679/2016, 156 ss.;

De Franceschi, A., *Personal Data as a Counter-Performance*, in Senigaglia, R., Irti, C., e Bernes, A. (a cura di), *Privacy and Data Protection in Software Services*, Berlino, Springer, 2022, 59 ss.;

De Francesco, F., *La successione* mortis causa *nei rapporti contrattuali: spunti interpretativi sull'art. 2*-terdecies *codice* privacy *e*
sull'eredità "digitale", in *Contr. e impr*., 2022, 640 ss.;

De Giacomo, C., *Diritto, libertà e privacy nel mondo della comunicazione globale*, Milano, Giuffrè, 1999;

De Gregorio, G., e Torino, R., *Privacy, protezione dei dati personali e big data*, in Tosi, E. (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019, 447 ss.;

De Hert, P., e Gutwirth, S., *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, in Gut- wirth, S., *et al.* (a cura di), *Reinventing Data Protection?*, Berlino, Springer, 2009, 3 ss.;

De Meo, R., *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Dir. inf*., 2013, 587 ss.;

De Meo, R., *La profilazione dei dati personali: il problema e gli orientamenti del Garante della privacy*, in *www.giustiziacivile.com*, 16 marzo 2015;

De Minico, G., *Electronic health record: political issues and privacy*, in *www.apertacontrada.it*, 18 dicembre 2015; De

Rold, C., *Sotto controllo. La salute ai tempi dell'e-health*, Roma, Il Pensiero Scientifico, 2015;

de Terwagne, C., *Is a Global Data Protection Regulatory Model Possible?*, in Gutwirth, S., *et al.* (a cura di), *Reinventing Data Protection?*, Berlino, Springer, 2009, 175 ss.;

de Terwagne, C., in Kuner, C., Bygrave, L.A., e Docksey, C. (a cura di), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020, *sub* art. 5, 309 ss.;

de Terwagne, C., *Privacy and data protection in Europe: Council of Europe's Convention 108+ and the European Union's GDPR*, in González Fuster, G., Van Brakel, R., e De Hert, P. (a cura di), *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics*, Cheltenham, Elgar, 2022, 10 ss.;

de Tura, A., *Le regole ulteriori per i soggetti pubblici*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 163 ss.;

De Vecchi Lajolo, V., *Il ritratto tra GDPR e legge sul diritto d'autore*, in *Dir. ind*., 2018, 532 ss.;

Del Conte, M., *Le regole della* privacy *nel rapporto di lavoro*, in Ferrari, G.F. (a cura di), *La legge sulla privacy dieci anni dopo*, Milano, EGEA, 2008, 201 ss.;

del Federico, C., e Popoli, A.R., *Disposizioni generali*, in Finocchiaro, G. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 57 ss.;

Di Marzio, F., Hybris, vanitas, jus. *Rifare l'umano*, in *Giust. civ*., 2018, 99 ss.;

Di Masi, M., *La specialità della relazione di cura e la responsabilità medica. Un itinerario dal paternalismo al "consenso biogra- fico"*, in Foglia, M. (a cura di), *La relazione di cura dopo la legge 219/2017. Una prospettiva interdisciplinare*, Pisa, Pacini, 2019, 15 ss.;

Di Masi, M., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 75, d.lgs. 30 giugno 2003, n. 196, 1233 ss.;

Di Masi, M., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), Codice della privacy e data protection, Milano, Giuffrè, 2021, sub art. 77, d.lgs. 30 giugno 2003, n. 196, 1243 ss.;

Di Masi, M., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 78, d.lgs. 30 giugno 2003, n. 196, 1252 ss.;

Di Masi, M., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 79, d.lgs. 30 giugno 2003, n. 196, 1262 ss.;

Di Pentima, M.G., *La cartella clinica: compilazione, profili di danno e criticità*, Milano, Giuffrè, 2023;

Di Porto, F. (a cura di), *Big data e concorrenza*, numero speciale di Concorrenza e mercato, Milano, Giuffrè, 2016; Di Porto, F., *La rivoluzione* big data. *Un'introduzione*, in *Concorrenza e mercato*, 2016, 5 ss.;

Di Porto, F., *La regolazione degli obblighi informativi. La sfida delle scienze cognitive e dei* big data, Napoli, Editoriale Scientifica, 2017;

Di Resta, F., *La nuova "privacy europea". I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Torino, Giap- pichelli, 2018;

Di Rosa, G., *Biodiritto. Itinerari di ricerca*, 2a ed., Torino, Giappichelli, 2010;

Di Rosa, G., *Dai principi alle regole. Appunti di Biodiritto*, Torino, Giappichelli, 2013;

Di Rosa, G., *La relazione di cura e di fiducia tra medico e paziente*, in *Nuove leggi civ. comm.*, 2019, 26 ss.; Di Rosa, G., *Profili giuridici dell'esistenza*, Torino, Giappichelli, 2022;

Di Rosa, G., *Soggettività giuridica e responsabilità robotica*, in Cuocci, V.V., Lops, F.P., e Motti, C. (a cura di), *La responsabilità civile nell'era digitale. Atti della Summer school 2021*, Bari, Cacucci, 2022, 163 ss.;

Di Tano, F., *Protezione dei dati personali e ricerca scientifica: un rapporto controverso ma necessario*, in *BioLaw Journal - Rivista di BioDiritto*, 2022, 71 ss.;

Diker Vanberg, A., e Maunick, M., *Data protection in the UK post-Brexit: the only certainty is uncertainty*, in *International Review of Law, Computers & Technology*, 2018, 190 ss.;

Dinant, J.-M., *The Concepts of Identity and Identifiablity: Legal and Technical Deadlocks for Protecting Human Beings in the Information Society?*, in Gutwirth, S., *et al.* (a cura di), *Reinventing Data Protection?*, Berlino, Springer, 2009, 111 ss.;

Diurni, A., *Gli stati di giustificazione nella responsabilità civile*, Torino, Giappichelli, 2003; Diurni, A., *I diritti collettivi dei pazienti nel panorama europeo*, in *Riv. dir. priv*., 2017, 349 ss.;

Ducato, R., *I dati biometrici*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1285 ss.;

Durante, V., *Dimensioni della salute: dalla definizione dell'OMS al diritto attuale*, in *Nuova giur. civ. comm.*, 2001, II, 132 ss.;

Durmuş, V., e Uydaci, M., *A Legal Framework for Healthcare: Personal Data Protection for Health Law in Turkey*, in Gupta, B.B., e Srinivasagopalan, S. (a cura di), *Handbook of Research on Intrusion Detection Systems*, 2021, Hershey, IGI Global, 219 ss.;

Durst, L., *Oggetto e finalità: un nuovo statuto giuridico dei dati personali*, in Panetta, R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, Milano, Giuffrè, 2019, 41 ss.;

Evans, R.S., *Electronic Health Records: Then, Now, and in the Future*, in *Yearbook of Medical Informatics*, 2016, *Special 25th Anni- versary Edition*, 48 ss.;

Everett, M., *The "I" in the gene: Divided property, fragmented personhood, and the making of a genetic privacy law*, in *American Ethnologist*, vol. 34, n. 2, 2007, 375 ss.;

Eysenbach, G., *What's e-Health*, in *J Med Internet Res.*, vol. 3, n. 2, 2001;

Fabbri, A., *I dati personali di natura religiosa, tra scelte individuali e trattamento confessionale collettivo*, in Califano, L., e Colapie- tro, C. (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regola- mento UE 2016/679*, Napoli, Editoriale Scientifica, 2017, 539 ss.;

Faccioli, E., e Cassaro, M., *Il "GDPR" e la normativa di armonizzazione nazionale alla luce dei principi:* accountability *e* privacy by design, in *Dir. ind.*, 2018, 561 ss.;

Faccioli, M., *Covid-19, linee guida e (difetto di) organizzazione delle strutture sanitarie*, in *Corti supreme e salute*, 2020, fasc. 3, 661 ss.;

Faccioli, M., *Telemedicina e responsabilità civile degli operatori e delle strutture sanitarie*, in Troiano, S. (a cura di), *Diritto privato e nuove tecnologie. Riflessioni incrociate tra esperienze giuridiche a confronto*, Napoli, Edizioni Scientifiche Italiane, 2022, 293 ss.;

Faccioli, M. (a cura di), *Profili giuridici dell'utilizzo della robotica e dell'intelligenza artificiale in medicina*, Napoli, Edizioni Scien- tifiche Italiane, 2022;

Faillace, S., *La natura e la disciplina delle obbligazioni di cui all'art. 25 del GDPR, espressione dei principi di* privacy by design *e di* privacy by default, in *Contr. e impr.*, 2022, 1123 ss.;

Faini, F., Big data *e* Internet of Things*:* data protection *e* data governance *alla luce del regolamento europeo*, in Cassano, G., *et al.* (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018, n. 101*, Milano, Giuffrè, 2018, 259 ss.;

Faini, F., *Dati, algoritmi e Regolamento europeo 2016/679*, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg.*
UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna, Pisa University Press, 2018, 333 ss.; Faini,

F., *La* governance *dell'intelligenza artificiale tra etica e diritto*, in *Notizie di Politeia*, 2020, n. 137, 59 ss.;

Faini, F., *Intelligenza artificiale, diritto e pubblica amministrazione*, in D'Aloia, A. (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, FrancoAngeli, 2021, 385 ss.;

Faini, F., *Società tecnologica, amministrazione pubblica e diritti digitali*, in Casadei, T., e Pietropaoli, S. (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano, Wolters Kluwer, 2021, 17 ss.;

Faini, F., *Intelligenza artificiale e regolazione giuridica: il ruolo del diritto nel rapporto tra uomo e macchina*, in *Federalismi*, n. 2, 2023, 1 ss., in *www.federalismi.it*, 25 gennaio 2023;

Falce, V., *L'"insostenibile leggerezza" delle regole sulle banche dati nell'unione dell'innovazione*, in *Riv. dir. ind.*, 2018,

377 ss.; Falcon, G., *Viaggio al centro del PNRR*, in *Le Regioni*, 2021, 715 ss.;

Falcone, M., *Big data e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica*, in *Rivista trimestrale di diritto pubblico*, 2017, 601 ss.;

Falletti, E., *Discriminazione algoritmica. Una prospettiva comparata*, Torino, Giappichelli, 2022;

Farace, D., *Il titolare e il responsabile del trattamento*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 731 ss.;

Farace, D., *Privacy by design e privacy by default*, in Tosi, E. (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019, 485 ss.;

Faralli, C., *Il diritto alla* privacy. *Profili storico-filosofici*, in Zorzi Galgano, N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, CEDAM, 2019, 1 ss.;

Faralli, C. (a cura di), *Vulnerabilità e nuove tecnologie*, in *Notizie di Politeia*, 2019, n. 136, 5 ss.;

Finocchiaro, G., *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in Finocchiaro, G. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 1 ss.;

Finocchiaro, G., *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 1 ss.;

Finocchiaro, G., *Corpo digitale e informazioni nella sanità elettronica*, in *Salute e società*, 2017, fasc. 2, 32 ss.;

Finocchiaro, G., *Intelligenza Artificiale e protezione dei dati personali*, in Gabrielli, E., e Ruffolo, U. (a cura di), *Intelligenza Artifi- ciale e diritto*, in *Giur. it.*, 2019, 1670 ss.;

Finocchiaro, G., *Il principio di* accountability, in Caterina, R. (a cura di), *GDPR tra novità e discontinuità*, in *Giur. it.*, 2019, 2778 ss.;

Finocchiaro, G. (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019;

Finocchiaro, G., *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in Finocchiaro, G. (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 1 ss.;

Finocchiaro, G., *Intelligenza artificiale e responsabilità*, in *Contr. e impr.*, 2020, 713 ss.;

Finocchiaro, G., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 17, reg. Ue n. 679/2016, 326 ss.;

Finocchiaro, G., *La proposta di Regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. inf.*, 2022, 303 ss.;

Finocchiaro, G., *La proposta di Regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in Camardi, C. (a cura di), *La via europea per l'intelligenza artificiale. Atti del convegno del progetto dottorale di alta for- mazione in scienze giuridiche, Ca' Foscari Venezia, 25-26 novembre 2021*, Padova, CEDAM, 2022, 215 ss.;

Finocchiaro, G., *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in Salanitro, U. (a cura di), *SMART la persona e l'infosfera*, Pisa, Pacini, 2022, 49 ss.;

Finocchiaro, G., e Pollicino, O., *Perché condividere i dati sanitari aiuta a tutelare i cittadini. Il nuovo regolamento europeo*, in *Il Sole 24 Ore* e in *www.digitalmedialaws.com*, 20 ottobre 2022;

Fiorentini, A., Machine learning *e dispositivi medici: riflessioni in materia di responsabilità civile*, in *Corr. giur.*, 2021, 1258 ss.; Fiorentino, L., *Il trattamento dei dati personali: l'impatto sulle amministrazioni pubbliche*, in *Giornale di diritto amministrativo*, 2018, 690 ss.;

Fioriglio, G., *Informatica medica e diritto. Un'introduzione*, Modena, Mucchi, 2020;

Fioriglio, G., eHealth*: tecnologie, diritto e salute*, in Casadei, T., e Pietropaoli, S. (a cura di), *Diritto e tecnologie informatiche.*
Questioni di informatica giuridica, prospettive istituzionali e sfide sociali, Milano, Wolters Kluwer, 2021, 45 ss.;

Fioriglio, G., *La protezione dei dati sanitari nella Società algoritmica. Profili informatico-giuridici*, in *Journal of Ethics and Legal Technologies*, vol. 3, n. 2, 2021, 79 ss.;

Fioriglio, G., *Intelligenza artificiale e medicina: alcune riflessioni sui profili giuridici ed etici*, in *Notizie di Politeia*, 2021, n. 143, 162 ss.;

Fiorillo, C., *La protezione dei dati personali nel diritto UE di fronte all'emergenza del COVID-19*, in *L'emergenza sanitaria Covid- 19 e il diritto dell'Unione europea. La crisi, la cura, le prospettive*, numero speciale di Eurojus, 2020;

Flick, G.M., *Dalla Leopolda alla Leopoldina. Un passo indietro o un ritorno al futuro?*, in *Cass. pen.*, 2015, 2526 ss.;

Florena, M., e Di Napoli, N., *Nuove declinazioni del diritto all'oblio nell'era digitale*, in *Tecnologie e diritto*, 2022, 313 ss.;

Floridi, L., *Metaverse: a matter of eXperience*, in *Philosophy & Technology*, 27 maggio 2022;

Floridi, L., *The European Legislation on AI: A Brief Analysis of Its Philosophical Approach*, in Mökander, J., e Ziosi, M. (a cura di),
The 2021 Yearbook of the Digital Ethics Lab, 2022, 1 ss.;

Floridi, L., *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, Raffaello Cortina Editore, 2022;

Foglia, C., *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione nel GDPR*, in Panetta, R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, Milano, Giuffrè, 2019, 309 ss.;

Foglia, M., *Autodeterminazione terapeutica e poteri della persona nella relazione di cura*, in Sirena, P., e Zoppini, A. (a cura di), *I poteri privati e il diritto della regolazione. A quarant'anni da «Le autorità private» di C.M. Bianca*, RomaTre-Press, 2018, 245 ss.;

Foglia, M. (a cura di), *La relazione di cura dopo la legge 219/2017. Una prospettiva interdisciplinare*, Pisa, Pacini, 2019;

Foglia, M., Sharenting *e riservatezza del minore in rete*, in *Actualidad Jurídica Iberoamericana*, 2022, n. 16 *bis*, 3550 ss.;

Fonderico, G., *La regolazione amministrativa del trattamento dei dati personali*, in *Giornale di diritto amministrativo*, 2018, 415 ss.;

Fontanarosa, F., *L'attuazione del Regolamento europeo in tema di protezione dei dati personali alla luce della dicotomia* civil law/common law, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 189 ss.;

Forgó, N., *My health data—your research: some preliminary thoughts on different values in the General Data Protection Regulation*, in *International Data Privacy Law*, vol. 5, n. 1, 2015, 54 ss.;

Fosch-Villaronga, E., *Robots, Healthcare, and the Law: Regulating Automation in Personal Care*, Londra, Routledge, 2019; Fosch-Villaronga, E., e Drukarch, H., *AI for Healthcare Robotics*, Londra, Routledge, 2022;

Francario, F., *Disposizioni "urgenti" in materia di protezione dei dati personali. Brevi note sul trattamento dati per finalità di pub- blico interesse*, in *www.giustiziainsieme.it*, 26 ottobre 2021;

Francario, F., *Protezione dei dati personali e pubblica amministrazione*, in Pisani, C., Proia, G., e Topo, A. (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Milano, Giuffrè, 2022, 679 ss.;

Franco, G., *L'evoluzione del trattamento dei dati religiosi: dalla legge 675/1996 al Regolamento (UE) 2016/679*, in *Ciberspazio e diritto*, 2019, 177 ss.;

Franceschelli, V. (a cura di), *La tutela della privacy informatica. Problemi e prospettive*, Milano, Giuffrè, 1998; Franzoni, M., *La nuova responsabilità in ambito sanitario*, in *Resp. med*., 2017, 5 ss.;

Franzoni, M., *Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale*, in *Jus civile*, 2021, 4 ss.;

Frattallone, S., *Principi generali del trattamento nel processo penale*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. II, Milano, Giuffrè, 2006, 1311 ss.;

Frattallone, S., *Il trattamento dei dati personali nelle investigazioni difensive*, in Panetta, R. (a cura di), *Libera circolazione e prote- zione dei dati personali*, t. II, Milano, Giuffrè, 2006, 1391 ss.;

Frau, R., *Il trattamento dei dati personali nell'attività bancaria*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 627 ss.;

Frè, F., *La cartella clinica nel sistema sanitario italiano*, in *Ragiusan*, 2008, 352 ss.; Freeman, M. (a cura di), *Law and Popular Culture*, Oxford University Press, 2005;

Frosini, J.O., Privacy *nel Regno Unito e l'impatto dello* Human Rights Act *del 1998*, in Ferrari, G.F. (a cura di), *La legge sulla privacy dieci anni dopo*, Milano, EGEA, 2008, 105 ss.;

Frosini, T.E., *La tutela dei dati e il diritto all'oblio*, in Scaffardi, L. (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, Torino, Giappichelli, 2018, 89 ss.;

Frosini, T.E., *L'orizzonte giuridico dell'intelligenza artificiale*, in *Dir. inf*., 2022, 5 ss.;

Frosini, T.E., *L'orizzonte giuridico dell'intelligenza artificiale*, in Camardi, C. (a cura di), *La via europea per l'intelligenza artificiale. Atti del convegno del progetto dottorale di alta formazione in scienze giuridiche, Ca' Foscari Venezia, 25-26 novembre 2021*, Padova, CEDAM, 2022, 7 ss.;

Frosini, V., *Cibernetica diritto e società*, Milano, Edizioni comunità, 1968;

Gallo, P., *Diritti della personalità e interessi non patrimoniali*, nel *Digesto online*, agg. 2022, in *OneLegale*;

Gallo, P., Big data *e diritto allo sfruttamento economico dei dati personali*, in D'Auria, M. (a cura di), *I problemi dell'informazione nel diritto civile, oggi. Studi in onore di Vincenzo Cuffaro*, Roma Tre-press, 2022, 375 ss.;

Gallo, V., *Il trattamento dei dati personali nei sistemi di intelligenza artificiale*, in Riccio, Gio.M., Ziccardi, G., e Scorza, G. (a cura di), *Intelligenza artificiale. Profili giuridici*, Padova, Cleup, 2022, 117 ss.;

Gallone, G., *Il Consiglio di Stato marca la distinzione tra algoritmo, automazione ed intelligenza artificiale*, in *Diritto di Internet*, 2022, 157 ss.;

Gamberale, R., *Il trattamento dei dati sensibili*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. I, Milano, Giuffrè, 2006, 1071 ss.;

Gamberale, R., *Il settore sanitario*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. II, Milano, Giuffrè, 2006, 1501 ss.;

Gambini, M., *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *Espaço jurídico*, vol. 14, fasc. 1, 2013, 149 ss.;

Gambini, M., *Responsabilità e risarcimento nel trattamento dei dati personali*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura
di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1017 ss.;

Gambino, A.M., e Petti, R., *Privacy e proprietà intellettuale*, in Tosi, E. (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019, 229 ss.;

Gambino, A.M., e Mula, D., *Diritti fondamentali, protezione dei dati e cybersecurity*, in Gambino, A.M., e Stazi, A. (a cura di), *La circolazione dei dati. Titolarità, strumenti negoziali, diritti e tutele*, Pisa, Pacini, 2020, 23 ss.;

Gambino, A.M., Maggio, E., e Occorsio, V., *La riforma del fascicolo sanitario elettronico*, in *Diritto mercato tecnologia*, *www.dimt.it*, 22 luglio 2020;

Gambino, A.M., e Tuzzolino, D., *Location Data and Privacy*, in Senigaglia, R., Irti, C., e Bernes, A. (a cura di), *Privacy and Data Protection in Software Services*, Berlino, Springer, 2022, 141 ss.;

Gambino, A.M., *IA e pratiche commerciali scorrette*, in Camardi, C. (a cura di), *La via europea per l'intelligenza artificiale. Atti del convegno del progetto dottorale di alta formazione in scienze giuridiche, Ca' Foscari Venezia, 25-26 novembre 2021*, Padova, CEDAM, 2022, 383 ss.;

Garaci, I., *Profili di tutela delle persone vulnerabili nell'ecosistema digitale. Il divieto di profilazione dei minori di età ai fini di* marketing, in Orlando, S., e Capaldo, G. (a cura di), *Annuario 2022 Osservatorio Giuridico sulla Innovazione Digitale*, Roma, sapienza Università Editrice, 2022, 89 ss.;

Garaci, I., *Minori e pubblicità mirata*, in *Diritto mercato tecnologia*, *www.dimt.it*, 24 gennaio 2022; Garaci, I., e

Montinaro, R. (a cura di), *La sostenibilità dell'innovazione digitale*, Napoli, Unior press, 2023;

García Mexía, P., *L'esperienza spagnola in materia di protezione dei dati personali*, in Ferrari, G.F. (a cura di), *La legge sulla privacy dieci anni dopo*, Milano, EGEA, 2008, 65 ss.;

Garofalo, A.M., *Cookies and the Passive Role of the Data Subject*, in Senigaglia, R., Irti, C., e Bernes, A. (a cura di), *Privacy and Data Protection in Software Services*, Berlino, Springer, 2022, 73 ss.;

Garofalo, G., *Trattamento e protezione dei dati personali: spunti rimediali in ambito sanitario*, in *Dir. fam. e pers*., 2021,

1392 ss.; Gaspari, F., *La circolazione dei dati genetici e delle biobanche: limiti e prospettive* de iure condendo, in

Federalismi, fasc. 5, 2021,
130 ss., consultabile all'indirizzo *www.federalismi.it*, 12 febbraio 2021;

Gatt, L., *et al*., *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività*
della tutela dei dati personali, in *Pol. dir*., 2017, 363 ss.;

Gatt, L., Caggiano, I.A., e Montanari, R. (a cura di), *Privacy and consent. A legal and UX&HMI approach for data protection*, Università degli Studi Suor Orsola Benincasa, 2021;

Gaudino, G., *Il sistema sanzionatorio*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. II, Milano, Giuffrè, 2006, 2211 ss.;

Giordano, R., *La tutela amministrativa e giurisdizionale dei dati personali*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1001 ss.;

Giorio, D., *Il GDPR negli enti pubblici fra opportunità e difficoltà operative*, in *Ciberspazio e diritto*, 2018, 141 ss.;

Giovanella, F., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 92, d.lgs. 30 giugno 2003, n. 196, 1284 ss.;

Giovannangeli, F.S., *L'informativa agli interessati e il consenso al trattamento*, in Panetta, R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, Milano, Giuffrè, 2019, 99 ss.;

Girotto, S., *Il trattamento dei dati biometrici*, in Canestrari, S., Ferrando, G., Mazzoni, C.M., Rodotà, S., e Zatti, P. (a cura di), *Il governo del corpo*, nel *Trattato di biodiritto* diretto da Rodotà e Zatti, t. I, Milano, Giuffrè, 2011, 1237 ss.;

Giuca, M., *Responsabilità penale e auto a guida autonoma: brevi riflessioni sulla recente riforma del Code de la route francese*, in Camardi, C. (a cura di), *La via europea per l'intelligenza artificiale. Atti del convegno del progetto dottorale di alta for- mazione in scienze giuridiche, Ca' Foscari Venezia, 25-26 novembre 2021*, Padova, CEDAM, 2022, 185 ss.;

Giuggioli, P.F., *Tutela della privacy e consumatore*, in Tosi, E. (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati per- sonali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019, 263 ss.;

Giusti, C., *Big data ed internet delle cose: quale destino per la tutela della privacy*, in *www.comparazionedirittocivile.it*, ottobre 2017; Glancy, D.J., *The Invention of the Right to Privacy*, in *Arizona Law Review*, 1979, vol. 21, n. 1, 1 ss.;

Glennie, H.R., *Electronic Health Records: Where They Are Now and Where They Need to Be*, in Ma, R. (a cura di), *Clinical Costing Techniques and Analysis in Modern Healthcare Systems*, Hershey, IGI Global, 2019, 87 ss.;

Gliatta, G., *Il diritto alla privacy in ambito medico: trattamento dei dati sensibili e fascicolo sanitario elettronico*, in *La resp. civ.*, 2010, 682 ss.;

Gobbato, S., *Big data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo*, in *MediaLaws*, 2019, fasc. 3, 148 ss.;

Gómez Álvarez, F.J., *La protección de los datos de carácter personal relativos a la salud en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, in *Derecho y Salud*, Vol. 27, Extraordinario XXVI Congreso, 2017, 238 ss.;

González Fuster, G., Van Brakel, R., e De Hert, P. (a cura di), *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics*, Cheltenham, Elgar, 2022;

Gorassini, A., *Il valore della cultura giuridica nell'era digitale*, in *Tecnologie e diritto*, 2021, fasc. 2, 38 ss.;

Gori, F., *et al*., *Telemedicina: da emergenza a nuova normalità. Riflessioni medico-legali*, in *Resp. civ. e prev*., 2021, 699 ss.; Gostin, L.O., e Lazzarini, Z., *Human Rights and Public Health in the AIDS Pandemic*, Oxford University Press, 1997;

Grady, C., *et al*., *Broad consent for research with biological samples: workshop conclusions*, in *American Journal of Bioethics*, 2015, vol. 15, n. 9, 34 ss.;

Gramunt Fombuena, D., *Dati personali e comunicazioni elettroniche. L'attuazione della direttiva CE n. 2002/58 nell'ordinamento spagnolo*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 945 ss.;

Grandi, C., *Prefazione*, in Thiene, A., e Corso, S. (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza*, Napoli, Jovene, 2023, XI ss.;

Granelli, C., *Autodeterminazione e scelte di fine vita*, in *Jus civile*, 2019, 548 ss.;

Granieri, M., *Una proposta di lettura sulla tutela risarcitoria nella vicenda del trattamento dei dati personali*, in *Danno e resp*., 1998, 221 ss.;

Granieri, M., *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civ. comm*., 2017, 165 ss.;

Graziadei, M., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 2, reg. Ue n. 679/2016, 130 ss.;

Gupta, N., e Dutta, A., *A Study on Data Protection and Privacy Issues in Healthcare Data*, in Mandal, J.K., *et al.* (a cura di), *Proceedings of International Conference on Advanced Computing Applications*, Berlino, Springer, 2022, 289 ss.;

Gutwirth, S., *et al.* (a cura di), *Reinventing Data Protection?*, Berlino, Springer, 2009;

Hallinan, D., *Protecting genetic privacy in biobanking through data protection law*, Oxford University Press, 2021;

Hansson, M.G., *Striking a Balance Between Personalised Genetics and Privacy Protection from the Perspective of GDPR*, in Sloken- berga, S., *et al.* (a cura di), *GDPR and Biobanking Individual Rights, Public Interest and Research Regulation across Europe*, Berlino, Springer, 2021, 31 ss.;

Harman, L.B., *et al*., *Electronic Health Records: Privacy, Confidentiality, and Security*, in *Virtual Mentor. American Medical Association Journal of Ethics*, 2012, vol. 14, n. 9, 712 ss.;

Herveg, J. (a cura di), *La protection des données médicales. Les défis du XXI^e siècle*, Limal, Anthemis, 2008; Herveg, J.,

Data Protection and Biobanks in 2018, in *European Journal of Health Law*, vol. 25, n. 5, 2018, 479 ss.;

Herveg, J., e Altavilla, A., *Introducing Key Elements Regarding Access to Personal Data for Scientific Research in the Perspective of Developing Innovative Medicines*, in *European Journal of Health Law*, vol. 27, n. 3, 2020, 195 ss.;

Hoffman, S., *Electronic Health Records and Medical Big Data. Law and policy*, Cambridge University Press, 2016;

Hoeren, T., *Datenschutz in Europa – Der zweite Entwurf einer EG-Datenschutzrichtlinie und dessen Auswirkungen auf die deutsche Privatwirtschaft (Data protection und European business)*, in *WM - Zeitschrift für Wirtschafts- und Bankrecht*, 1994, 1 ss.;

Hoeren, T., *Dateneigentum und Datenbesitz*, in Pertot, T. (a cura di), *Rechte an Daten*, Tubinga, Mohr Siebeck, 2020, 37 ss.; Holmes, J.H., *et al.*, *A 21st Century Embarrassment of Riches: The Balance Between Health Data Access, Usage, and Sharing*, in
Yearbook of Medical Informatics, 2018, 5 ss.;

Hoofnagle, C.J., *et al*., *The European Union general data protection regulation: what it is and what it means*, in *Information & Communications Technology Law*, vol. 28, n. 1, 2019, 65 ss.;

Hordern, V., *Data Protection Compliance in the Age of Digital Health*, in *European Journal of Health Law*, vol. 23, n. 3, 2016, 248 ss.;

Horgan, D., *et al*., *European Health Data Space—An Opportunity Now to Grasp the Future of Data-Driven Healthcare*, in *Healthcare*, 2022, 10, 1629;

Hors-Fraile, S., *et al*., *The Unintended Consequences of Social Media in Healthcare: New Problems and New Solutions*, in *Yearbook of Medical Informatics*, 2016, 47 ss.;

Hubmann, H., *Der zivilrechtliche Schutz der Persönlichkeit gegen Indiskretion*, in *JuristenZeitung*, 1957, 521 ss.;

Hubmann, H., *Das Persönlichkeitsrecht*, 2a ed., Münster-Köln, Böhlau, 1967;

Iacobucci, S., *Il trattamento dei dati personali del lavoratore tra informativa e consenso*, in Bianchini, M., Pasqualetto, E., e Zamuner,
E. (a cura di), *Percorsi di ricerca del dottorato in diritto internazionale, diritto privato e del lavoro dell'Università di Padova*, Padova University Press, 2021, 13 ss.;

Iamiceli, P., *Liceità, correttezza, finalità nel trattamento dei dati personali*, in Pardolesi, R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003, 395 ss.;

Iannini, A., *L'Autorità Garante per la protezione dei dati personali e le nuove sfide del Regolamento europeo*, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 47 ss.;

Iannuzzi, A., e Laviola, F., *I diritti fondamentali nella transizione digitale fra libertà e uguaglianza*, in *Dir. cost*., 2023, fasc. 1, 9 ss.;

Iaquinta, F., e Ingrao, A., *La privacy e i dati sensibili del lavoratore legati all'utilizzo di social networks. Quando prevenire è meglio che curare*, in *Dir. rel. ind*., 2014, 1027 ss.;

Iorio, C., *Intelligenza artificiale e responsabilità: spunti ricostruttivi*, in *Tecnologie e diritto*, 2021, fasc. 2, 51 ss.;

Ippoliti Martini, C., *Il meccanismo di coerenza. Comitato europeo per la protezione dei dati*. Sez. II: *Comitato europeo per la prote- zione dei dati*, in Finocchiaro, G. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 552 ss.;

Ippoliti Martini, C., *Comitato europeo per la protezione dei dati*, in Finocchiaro, G. (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 725 ss.;

Irti, C., *Dato personale, dato anonimo e crisi del modello normativo dell'identità*, in *Jus civile*, 2020, 379 ss.; Irti, C., *Consenso "negoziato" e circolazione dei dati personali*, Torino, Giappichelli, 2021;

Irti, C., *Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data*, in Senigaglia, R., Irti, C., e Bernes, A. (a cura di), *Privacy and Data Protection in Software Services*, Berlino, Springer, 2022, 49 ss.;

Irti, C., *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano*, in *Persona e mercato*, 2023, fasc. 1, 32 ss.;

Irti, N., *L'ordine giuridico del mercato*, Roma-Bari, Laterza, 1998;

Irti, N., *Il diritto nell'età della tecnica*, Napoli, Editoriale Scientifica, 2007;

Iuliani, A., *Note minime in tema di trattamento dei dati personali*, in *Eur. e dir. priv.*, 2018, 293 ss.;

Izzo, U., *Medicina e diritto nell'era digitale: i problemi giuridici della cybermedicina*, in *Danno e resp*., 2000, 807 ss.;

Jameson, F., *Postmodernism, or, The Cultural Logic of Late Capitalism*, Durham, NC, Duke University Press, 1991;

Kasperbauer, T.J., *Protecting health privacy even when privacy is lost*, in *Journal of medical ethics*, vol. 46, n. 11, 2020, 768 ss.; Kayaalp, M., *Patient Privacy in the Era of Big Data*, in *Balkan Medicine Journal*, 2018, vol. 35, n. 1, 8 ss.;

Kaye, J., *et al*., *Governing Biobanks: Understanding the Interplay between Law and Practice*, Oxford, Hart Publishing, 2012;

Kindt, E.J., *Biometric data processing: Is the legislator keeping up or just keeping up appearances?*, in González Fuster, G., Van Brakel, R., e De Hert, P. (a cura di), *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics*, Cheltenham, Elgar, 2022, 375 ss.;

Kirschen, S., *Il codice della privacy, fra tradizione e innovazione*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. I, Milano, Giuffrè, 2006, 5 ss.;

Klesta Dosi, L., *Assistenza sanitaria e tutela del cittadino. Modelli privatistici e orizzonte europeo*, Torino, Giappichelli, 2008;

Knoppers, B.M., *Of biobanks, medical data and population genetics: whither identifiability?*, in Herveg, J. (a cura di), *La protection des données médicales. Les défis du XXI^e siècle*, Limal, Anthemis, 2008, 79 ss.;

Knoppers, B.M., e Zawati, M.H., *Population biobanks and access*, in Canestrari, S., Ferrando, G., Mazzoni, C.M., Rodotà, S., e Zatti,
P. (a cura di), *Il governo del corpo*, nel *Trattato di biodiritto* diretto da Rodotà e Zatti, t. I, Milano, Giuffrè, 2011, 1181 ss.;

Ko, H., *et al*., *Structure and enforcement of data privacy law in South Korea*, in *International Data Privacy Law*, vol. 7, n. 2, 2017, 100 ss.;

Kosta, E., *Consent in European Data Protection Law*, Leiden-Boston, Brill-Martinus Nijhoff Publishers, 2013;

Kosta, E., in Kuner, C., Bygrave, L.A., e Docksey, C. (a cura di), *The EU General Data Protection Regulation (GDPR). A Commen- tary*, Oxford University Press, 2020, *sub* art. 7, 345 ss.;

Kosta, E., in Kuner, C., Bygrave, L.A., e Docksey, C. (a cura di), *The EU General Data Protection Regulation (GDPR). A Commen- tary*, Oxford University Press, 2020, *sub* art. 8, 355 ss.;

Kostkina, Y., *Verhältnis von datenschutzrechtlicher Einwilligung und Vertrag*, in Troiano, S., e Schmidt-Kessel, M. (a cura di),
Diritto, cambiamenti e tecnologie nel dialogo italo-tedesco, Napoli, Edizioni Scientifiche Italiane, 2022, 29 ss.;

Kotschy, W., in Kuner, C., Bygrave, L.A., e Docksey, C. (a cura di), *The EU General Data Protection Regulation (GDPR). A Com- mentary*, Oxford University Press, 2020, *sub* art. 6, 321 ss.;

Kulesza, J., e Delerue, F., *Cybersecurity in the Year of the Plague: Due Diligence as a Remedy to Malicious Activities*, in *Tecnologie e diritto*, 2020, 404 ss.;

Kuner, C., Bygrave, L.A., e Docksey, C. (a cura di), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020;

Kuner, C., Bygrave, L.A., e Docksey, C., *Background and Evolution of the EU General Data Protection Regulation (GDPR)*, in Kuner, C., Bygrave, L.A., e Docksey, C. (a cura di), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020, 1 ss.;

La Spina, A., *La trasmisión de los datos de carácter personal del consumidor para la adquisición de servicios y contenidos digitales*, in *Jus civile*, 2021, 1663 ss.;

La Spina, A., *Complessità e identità personale*, Edizioni Scientifiche Italiane, Napoli, 2022; Lagioia, F., *L'intelligenza artificiale in sanità: un'analisi giuridica*, Torino, Giappichelli, 2020;

Lagioia, F., Sartor, G., e Simoncini, A., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e data protection*, Milano, Giuffrè, 2021, *sub* art. 22, reg. Ue n. 679/2016, 378 ss.;

Lamarque, E., *Privacy e salute*, in Losano, M.G. (a cura di), *La legge italiana sulla* privacy. *Un bilancio dei primi cinque anni*, Roma- Bari, Laterza, 2001, 333 ss.;

Lamberti, A., *Emergenza sanitaria, Costituzione, soggetti deboli: vecchi e nuovi diritti alla prova della pandemia*, in *Federalismi*, fasc. 6, 2022, 159 ss., in *www.federalismi.it*, 23 febbraio 2022;

Lambertucci, P., *Trattamento dei dati personali e rapporto di lavoro*, in Cuffaro, V., e Ricciuto, V. (a cura di), *La disciplina del trattamento dei dati personali*, Torino, Giappichelli, 1997, 423 ss.;

Langhanke, C., e Schmidt-Kessel, M., *Consumer Data as Consideration*, in *Journal of European Consumer and Market Law*, 2015, 218 ss.;

Latorre Luna, L., *Salud pública y* big data*: COVID-19. Reflexión jurídica sobre la normativa de datos de salud y de aplicación de herramientas big data en el ámbito de la investigación biomédica y de la asistencia sanitaria*, in *Derecho y Salud*, vol. 31,
n. 1, 2021, 6 ss.;

Lattanzi, R., *Dati sensibili: una categoria problematica nell'orizzonte europeo*, in *Eur. e dir. priv.*, 1998, 713 ss.;

Lattanzi, R., *Protecting health care data: from medical secrecy to personal data protection. Solution found?*, in Herveg, J. (a cura di),
La protection des données médicales. Les défis du XXI^{e} *siècle*, Limal, Anthemis, 2008, 21 ss.;

Lattanzi, R., *Ricerca genetica e protezione dei dati personali*, in Canestrari, S., Ferrando, G., Mazzoni, C.M., Rodotà, S., e Zatti, P. (a cura di), *Il governo del corpo*, nel *Trattato di biodiritto* diretto da Rodotà e Zatti, t. I, Milano, Giuffrè, 2011, 319 ss.;

Latte, S., *Immuni: inquadramento e prime considerazioni ad un mese dal via*, in *European Journal of Privacy Law & Technologies*, 2020, 362 ss.;

Lattuneddu, F., *L'evoluzione della tutela del diritto alla privacy*, in *Quaderni di diritto e politica ecclesiastica*, 2014, 966 ss.; Lattuneddu, F., *L'ampliamento giurisprudenziale dei confini del diritto alla privacy*, in *Quaderni di diritto e politica ecclesiastica*,
2015, 943 ss.;

Laus, F., *L'intervento in materia sanitaria del Garante per la protezione dei dati personali*, in *Biodiritto*, 2012, fasc. 1, 129 ss.;

Lavacca, G., *et al*., *"Internet never forgets"(?). Diritto all'oblio e diritto alla cancellazione, quali gli usi e quali i limiti*, in *Ciberspazio e diritto*, 2019, 437 ss.;

Laviola, F., *Algoritmico, troppo algoritmico: decisioni amministrative automatizzate, protezione dei dati personali e tutela delle li- bertà dei cittadini alla luce della più recente giurisprudenza amministrativa*, in *BioLaw Journal - Rivista di BioDiritto*, 2020, fasc. 3, 389 ss.;

Lea, N.C., *et al*., *Between Scylla and Charybdis: Charting the Wicked Problem of Reusing Health Data for Clinical Research Informatics*, in *Yearbook of Medical Informatics*, 2018, 170 ss.;

Leanza, C., *La telemedicina: profili civilistici di responsabilità*, in *Rass. dir. farm.*, 2020, 531 ss.;

Macchia, M., *Applicazioni di tracciamento e Stato di diritto*, in *www.irpa.eu, Osservatorio sullo Stato digitale*, 9 luglio 2020;

Mačėnaitė, M., e Kosta, E., *Consent for processing children's personal data in the EU: following in US footsteps?*, in *Information & Communications Technology Law*, vol. 26, n. 2, 2017, 146 ss.;

Mačėnaitė, M., *Protecting Children Online: Combining the Rationale and Rules of Personal Data Protection Law and Consumer Protection Law*, in Bakhoum, M., Conde Gallego, B., Mackenrodt, M.-O., e Surblytė-Namavičienė, G. (a cura di), *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Towards a Holistic Approach?*, Berlino, Sprin- ger, 2018, 331 ss.;

Macilotti, M., *Le biobanche: disciplina e diritti della persona*, in Canestrari, S., Ferrando, G., Mazzoni, C.M., Rodotà, S., e Zatti, P. (a cura di), *Il governo del corpo*, nel *Trattato di biodiritto* diretto da Rodotà e Zatti, t. I, Milano, Giuffrè, 2011, 1195 ss.;

Macilotti, M., voce «Biobanche», in *Digesto IV ed*., *Disc. priv*., *sez. civ*., VII, Torino, Utet, 2012, 134 ss.;

Macrì, I., *Cloud della Pubblica Amministrazione: una casa moderna per i dati degli Italiani*, in *Azienditalia*, 2021, 1847 ss.; Macrì, I., *Il PNRR italiano per la digitalizzazione e l'innovazione della Pubblica Amministrazione*, in *Azienditalia*, 2022, 38 ss.;

Macrì, I., *Dalle infrastrutture digitali delle Amministrazioni al cloud, il nuovo regolamento per la sicurezza dei dati e dei servizi pubblici*, in *Azienditalia*, 2022, 488 ss.;

Macrì, I., *Le strategie europee per la digitalizzazione e gli obiettivi italiani*, in *Azienditalia*, 2022, 713 ss.;

Maestri, E., *Giudizi di esistenza. Deliberare sulla vita umana nella riflessione bioetica contemporanea*, Napoli, Edizioni Scientifiche Italiane, 2010;

Maestri, E., *La dispensa umana. Aspetti scientifici, giuridici ed etici delle biobanche*, in Poggi, F. (a cura di), *Diritto e bioetica. Le questioni fondamentali*, Roma, Carocci, 2013, 71 ss.;

Maestri, E., *Lex informatica. Diritto, persona e potere nell'età del cyberspazio*, Napoli, Edizioni Scientifiche Italiane, 2015; Maestri, E., *Il minore come persona digitale. Regole, tutele e* privacy *dei minori sul* Web, in Thiene, A., e Marescotti, E. (a cura di),
La scuola al tempo dei social network, numero monografico degli *Annali online della Didattica e della Formazione Docente*, 2017, 7 ss.;

Maestri, E., *La persona digitale tra* habeas corpus *e* habeas data, in Bilotta, F., e Raimondi, F. (a cura di), *Il soggetto di diritto storia ed evoluzione di un concetto nel diritto privato*, Napoli, Jovene, 2020, 277 ss.;

Maestri, E., *Il feticcio della privacy nella sanità. Cura del paziente e biobanking genetico prima e dopo l'entrata in vigore del GDPR*, in Thiene, A., e Corso, S. (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza*, Napoli, Jovene, 2023, 23 ss.;

Maggino, F., e Cicerchia, G., *Algoritmi, etica e diritto*, in *Dir. inf*., 2019, 1161 ss.; Maggiolino, M., *Big data e prezzi personalizzati*, in *Concorrenza e mercato*, 2016, 95 ss.;

Maglio, M., Polini, M., e Tilli, N. (a cura di), *Manuale di diritto alla protezione dei dati personali. La privacy dopo il Regolamento Ue 2016/679*, Santarcangelo di Romagna, Maggioli, 2017;

Maglio, M., *Il regolamento europeo 2016/679 in materia di dati personali. Inquadramento generale e prospettive di sviluppo*, in Maglio, M., Polini, M., e Tilli, N. (a cura di), *Manuale di diritto alla protezione dei dati personali. La privacy dopo il Regolamento Ue 2016/679*, Santarcangelo di Romagna, Maggioli, 2017, 55 ss.;

Maglio, M., *Il valore economico dei dati personali: spunti per un'analisi economica della* data protection, in Maglio, M., Polini, M., e Tilli, N. (a cura di), *Manuale di diritto alla protezione dei dati personali. La privacy dopo il Regolamento Ue 2016/679*, Santarcangelo di Romagna, Maggioli, 2017, 79 ss.;

Maglio, M., *Dati personali ed attività sanitaria*, in Maglio, M., Polini, M., e Tilli, N. (a cura di), *Manuale di diritto alla protezione dei dati personali. La privacy dopo il Regolamento Ue 2016/679*, Santarcangelo di Romagna, Maggioli, 2017, 527 ss.;

Malagnino, M.E., *Il ruolo del garante all'alba del GDPR: verso un'autorità*, in Panetta, R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018,* Milano, Giuffrè, 2019, 435 ss.;

Mantelero, A., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 35, reg. Ue n. 679/2016, 532 ss.;

Mantelero, A., *Big data and data protection*, in González Fuster, G., Van Brakel, R., e De Hert, P. (a cura di), *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics*, Cheltenham, Elgar, 2022, 335 ss.;

Mantovani, M., in Barba, A., e Pagliantini, S. (a cura di), *Delle persone. Leggi collegate*, II, nel *Commentario del Codice civile*, diretto da Enrico Gabrielli, Torino, Utet, 2019, *Introduzione* l. n. 219/2017, 1447 ss.;

Mantovani, M., *Relazione di cura e disposizioni anticipate di trattamento*, in *Nuove leggi civ. comm*., 2019, 188 ss.;

Mantovani, M., *GDPR, minori e marketing*, in E. de Belvis (a cura di), *Diritto di famiglia e nuove tecnologie*, Napoli, Edizioni Scientifiche Italiane, 2022, 239 ss.;

Manzo, V., e Marco, B., *From information privacy to emergency privacy*, in *European Journal of Privacy Law & Technologies*, 2020, fasc. 1, 83 ss.;

Maqueo Ramírez, M.S., Moreno González, J, e Recio Gayo, M., *Protección de datos personales, privacidad y vida privada: la in- quietante búsqueda de un equilibrio global necesario*, in *Revista de Derecho*, vol. 30, n. 1, 2017, 77 ss.;

Marano, V., *Protezione dei dati personali, libertà religiosa e autonomia delle Chiese*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a
cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 579 ss.;

Maras, M.-H., e O'Brien, W., *Discrimination, stigmatization, and surveillance: COVID-19 and social sorting*, in *Information & Com- munications Technology Law*, in *www.tandfonline.com*, 20 luglio 2022;

Marcello, D., *Responsabilità e corresponsabilità nel trattamento dei dati personali*, in *www.giustiziacivile.com*, 14 settembre 2018;

Marcenò, V., *L'inserimento della legge sulla privacy nel sistema giuridico italiano*, in Losano, M.G. (a cura di), *La legge italiana sulla* privacy. *Un bilancio dei primi cinque anni*, Roma-Bari, Laterza, 2001, 29 ss.;

Marchese, A., *Profili civilistici dell'*information technology *in àmbito sanitario*, Napoli, Edizioni Scientifiche Italiane, 2021; Marchetti, G., e Thobani, S., *La tutela contrattuale dei consumatori di contenuti e servizi digitali*, in Magri, G., Martinelli, S., e
Thobani, S. (a cura di), *Manuale di diritto privato delle nuove tecnologie*, Torino, Giappichelli, 2022, 35 ss.;

Marcoccia, E., *La tutela dei minori*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. I, Milano, Giuffrè, 2006, 333 ss.;

Marcoccia, E., *Trattamenti per finalità di ricerca*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. II, Milano, Giuffrè, 2006, 1815 ss.;

Marelli, L., e Testa, G., *Scrutinizing the EU General Data Protection Regulation. How will new decentralized governance impact research?*, in *Science*, vol. 320, n. 6388, 496 ss.;

Maresca, A., Ciucciovino, S., e Alvino, I., *Regolamento UE 2016/679 e rapporto di lavoro*, in Califano, L., e Colapietro, C. (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017, 311 ss.;

Marì, J., *El Delegado de Protección de Datos en el Reglamento General de Protección de Datos*, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 99 ss.;

Marino, G., *Internet e tutela dei dati personali: il consenso ai* cookie, in *Jus civile*, 2020, 398 ss.;

Marnau, N., e Sorge, C., *From law to engineering: A computer science perspective on privacy and data protection*, in González Fuster, G., Van Brakel, R., e De Hert, P. (a cura di), *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics*, Cheltenham, Elgar, 2022, 197 ss.;

Marotta, G., *Ordinamento sanitario e diritto di accesso: analisi della giurisprudenza amministrativa*, in *Corti supreme e salute*, 2021, fasc. 3, 587 ss.;

Martinelli, S., *Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in internet e le problematiche poste dalla deindicizzazione*, in *Dir. inf.*, 2017, 565 ss.;

Mendelson, Dan., e Mendelson, Dav., *Legal protections for personal health information in the age of Big Data – a proposal for regulatory framework*, in *Ethics, Medicine and Public Health*, 2017, vol. 3, n. 1, 37 ss.;

Meneghetti, M.C., *Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*, in Finocchiaro, G. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 423 ss.;

Meneghetti, M.C., *Consenso* bis*: la Corte di giustizia torna sui requisiti di un valido consenso privacy*, in *MediaLaws*, 2021, fasc. 1, 266 ss.;

Mercadante, G., *Le nuove sfide del diritto europeo nell'era dei big data*, in *Ciberspazio e diritto*, 2018, 21 ss.; Merla, L.,

Big Data e diritto: una sfida all'effettività, in *MediaLaws*, 2021, fasc. 1, 218 ss.;

Merloni, F. (a cura di), *La trasparenza amministrativa*, Milano, Giuffrè, 2008;

Messina, S., *L'adeguamento della normativa nazionale al Regolamento*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 119 ss.;

Messinetti, D., voce «Personalità (diritti della)», in *Enc. del dir*., XXXIII, Milano, Giuffrè, 1983, 355 ss.;

Messinetti, R., *Circolazione dei dati personali e autonomia privata*, in Zorzi Galgano, N. (a cura di), *Persona e mercato dei dati.*
Riflessioni sul GDPR, Padova, CEDAM, 2019, 137 ss.;

Messinetti, R., *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, in Zorzi Galgano, N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, CEDAM, 2019, 167 ss.;

Messinetti, R., *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. e impr*., 2019, 861 ss.;

Messinetti, R., *Comunicare nell'infosfera. La vulnerabilità della persona digitale*, in *Federalismi*, n. 18, 2021, IV ss., in *www.fede- ralismi.it*, 28 luglio 2021;

Messinetti, R., *La* Privacy *e il controllo dell'identità algoritmica*, in *Contr. e impr. Eur*., 2021, 121 ss.; Mete, E., *Uso dei*

dati, etica e diritti, in *www.giustiziacivile.com*, 22 settembre 2020;

Mezzanotte, F., *Rischio e responsabilità nei sistemi dell'*Internet of Things, in Garaci, I., e Montinaro, R. (a cura di), *La sostenibilità dell'innovazione digitale*, Napoli, Unior press, 2023, 137 ss.;

Michalowski, M., Raza Abidi, S.S., Abidi, S. (a cura di), *Artificial Intelligence in Medicine*, Berlino, Springer, 2022;

Micozzi, F.P., *Sanzioni e responsabilità amministrative e penali*, in Cassano, G., *et al.* (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018, n. 101*, Milano, Giuffrè, 2018, 383 ss.;

Micozzi, F.P., *Le tecnologie, la protezione dei dati e l'emergenza Coronavirus: rapporto tra il possibile e il legalmente consentito*, in
BioLaw Journal - Rivista di BioDiritto, 2020, fasc. 1, 623 ss.;

Miccú, R., *Questioni attuali intorno alla digitalizzazione dei servizi sanitari nella prospettiva multilivello*, in *Federalismi*, fasc. 5,
2021, 1 ss., consultabile all'indirizzo *www.federalismi.it*, 12 febbraio 2021;

Miccú, R., Ferrara, M., e Ingenito, C. (a cura di), *La digitalizzazione dei servizi sanitari, il diritto alla salute e la tutela dei dati personali*, numero monografico di *Federalismi*, fasc. 5, 2021, in *www.federalismi.it*, 12 febbraio 2021;

Miele, M. (a cura di), *La crisi del diritto*, Padova, CEDAM, 2022, rist. anast. dell'ed. del 1953;

Miele, P., voce «Cause di giustificazione», in *Enc. del dir*., VI, Milano, Giuffrè, 1960, 590 ss.;

Milapidou, M., *The impact of EU Regulation 2016/679 on the Greek health system*, in Fares, G. (a cura di), *The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis*, Torino, Giappichelli, 2021, 163 ss.;

Miniscalco, N., *La sorveglianza attiva per contrastare la diffusione dell'epidemia da Covid-19: strumento di controllo e di garanzia per i cittadini?*, in *Osservatorio costituzionale AIC*, fasc. 3, 2020, 95 ss.;

Miniscalco, N., *La personalità in rete: protezione dei dati personali, identità digitale e diritto all'oblio*, in Casadei, T., e Pietropaoli,
S. (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano, Wolters Kluwer, 2021, 31 ss.;

Morrone, A., e Minni, F., *La salute come valore costituzionale e fonte di diritti soggettivi alla luce della giurisprudenza costituzionale*, in Alpa, G. (a cura di), *La responsabilità sanitaria. Commento alla l. 8 marzo 2017, n. 24*, 2a ed., Pisa, Pacini, 2022, 120 ss.;

Moruzzi, M., *E-Health e fascicolo sanitario elettronico*, Milano, Il Sole 24 Ore, 2009;

Mostert, M., *et al*., *From Privacy to Data Protection in the eu: Implications for Big Data Health Research*, in *European Journal of Health Law*, vol. 25, n. 1, 2018, 43 ss.;

Mota Donate, G., *Salud digital: un nuevo paradigma también para el ámbito de la conciliación de derechos*, in *Derecho y Salud*, vol. 30, n. 2, 2020, 112 ss.;

Motroni, R., *Il Regolamento (UE) 2016/679 tra soggetti giuridici del mercato ed oggetto economico*, in *www.federalismi.it*, 28 giugno 2017;

Motroni, R., *Il «Coronavirus»: il miglior promoter dell'economia digitale?*, in *Nuova giur. civ. comm*., 2020, suppl., 99 ss.;

Muciaccia, N., *Osservazioni preliminari per uno studio sul riutilizzo dei* big healthcare data, in *Riv. dir. priv*., 2020, 345 ss.;

Mula, D., *Elaborazione e sfruttamento dei dati mediante algoritmi*, in Gambino, A.M., e Stazi, A. (a cura di), *La circolazione dei dati.*
Titolarità, strumenti negoziali, diritti e tutele, Pisa, Pacini, 2020, 127 ss.;

Mulà, P.P., *La tutela della privacy in ambito sanitario*, Santarcangelo di Romagna, Maggioli, 2018;

Mulazzani, G., *Il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in Finocchiaro, G. (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 194 ss.;

Mulazzani, G., *Il trattamento di categorie particolari di dati personali, necessario per motivi di pubblico interesse rilevante*, in Fi- nocchiaro, G. (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 229 ss.;

Mulazzani, G., *Le sanzioni amministrative in materia di protezione dei dati personali nell'ordinamento europeo ed in quello nazio- nale*, in Finocchiaro, G. (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 791 ss.;

Mulder, T., e Tudorica, M., *Privacy policies, cross-border health data and the GDPR*, in *Information & Communications Technology Law*, vol. 28, n. 3, 2019, 261 ss.;

Muraro, G., e Rebba, V., *La sanità del futuro: spesa, occupazione e rapporto pubblico-privato*, in Aa.Vv., *Tecnologia e Società. II. Sviluppo e trasformazione della società*, Atti dei Convegni Lincei Roma, 5-6 aprile 2001, Accademia dei Lincei, Roma, 2001, 171 ss.;

Naddeo, F., *Il consenso al trattamento dei dati personali del minore*, in *Dir. inf*., 2018, 27 ss.;

Nannini, U.G., *Il consenso al trattamento medico. Presupposti teorici e applicazioni giurisprudenziali in Francia, Germania e Italia*, Milano, Giuffrè, 1989;

Natoli, U., *La protezione dei diritti dell'uomo e la Carta Sociale Europea*, in *Dem. e dir*., 1967, 1, 56 ss., e in *Rev. dr. contemp*., 1968, 1 ss., ora in *Diritti fondamentali e categorie generali. Scritti di Ugo Natoli*, Milano, Giuffrè, 1993, 397 ss.;

Naty-Daufin, P., e Carmona, E., *Les nouvelles technologies au service de la santé*, in Raimondeau, J., *et al.* (a cura di), *Manuel de santé publique*, Rennes, Presses de l'EHESP, 2020, 479 ss.;

Navarretta, E., in Bianca, C.M., e Busnelli, F.D. (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003,*
n. 196, Codice della privacy, Padova, CEDAM, 2007, *sub* art. 11, 241 ss.;

Navone, G., *Ieri, oggi e domani della responsabilità civile da illecito trattamento dei dati personali*, in *Nuove leggi civ. comm*., 2022, 132 ss.;

Negri, S., *Consenso informato, diritti umani e biodiritto internazionale*, in *Biodiritto*, 2012, fasc. 2, 97 ss.;

Negro, A., *I danni da pericolo*, nel *Trattato dei nuovi danni*, diretto da Cendon, vol. II, Malpractice *medica. Prerogative della persona. Voci emergenti della responsabilità*, Padova, CEDAM, 2011, 919 ss.;

Netter, E., *Numérique et grandes notions du droit privé. La personne, la propriété, le contrat*, Amiens, Ceprisca, 2019;

Nelkin, D., *Informazione genetica: bioetica e legge*, in *Riv. crit. dir. priv*., 1994, 491 ss.;

Panetta, R., *Diritti, regole, libere professioni e mercato, tra circolazione e protezione dei dati*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. I, Milano, Giuffrè, 2006, 161 ss.;

Panetta, R., *Il trasferimento all'estero dei dati personali*, in Zorzi Galgano, N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, CEDAM, 2019, 357 ss.;

Panetta, R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, Milano, Giuffrè, 2019;

Panetta, R., Privacy is not dead: it's hiring!, in Panetta, R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, Milano, Giuffrè, 2019, 3 ss.;

Panetta, R., e Sartore, F., *L'equilibrio legislativo tra protezione e trasparenza dei dati*, in Alpa, G. (a cura di), *La responsabilità sanitaria. Commento alla l. 8 marzo 2017, n. 24*, 2a ed., Pisa, Pacini, 2022, 269 ss.;

Paradiso, M., *Dal matrimonio alla filiazione. Ritorno al futuro del diritto di famiglia*, in *Fam. e dir*., 2022, 1042 ss.;

Paravani, A., *L'adozione di misure di sicurezza*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. I, Milano, Giuffrè, 2006, 655 ss.;

Pardolesi, R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003;

Pardolesi, R., *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in Pardolesi, R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003, 1 ss.;

Parenzo, B., *Profilazione e discriminazione. Dal GDPR alla proposta di Regolamento sull'intelligenza artificiale*, in Camardi, C. (a cura di), *La via europea per l'intelligenza artificiale. Atti del convegno del progetto dottorale di alta formazione in scienze giuridiche, Ca' Foscari Venezia, 25-26 novembre 2021*, Padova, CEDAM, 2022, 335 ss.;

Parenzo, B., *Profilazione e discriminazione. Dal GDPR alla Proposta di Regolamento sull'IA*, in *Tecnologie e diritto*, 2023,

105 ss.; Paris, C., *Biobanche di ricerca e consenso informato "dinamico"*, in *Resp. med*., 2021, 249 ss.;

Paris, C., *Biobanche di ricerca e banca dati nazionale del DNA: un difficile bilanciamento tra interessi contrapposti*, in *BioLaw Journal - Rivista di BioDiritto*, *Special issue* 1, 2022, 83 ss.;

Parisi, A.G., *Illiceità del trattamento dei dati personali e rimedi (inibitori, risarcitori, satisfattivi e ablativi)*, in Stanzione, P. (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, Giappichelli, 2022, 209 ss.;

Pascuzzi, G., e Izzo, U., *Le problematiche giuridiche connesse all'utilizzo delle nuove tecnologie in sanità*, in *www.psychiatryonline.it*, 3 novembre 2012;

Pasquale, F., e Ragone, T.A., *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, in *Stanford Tech- nology Law Review*, 2014, vol. 17, 595 ss.;

Pasquale, F., *New Laws of Robotics. Defending Human Expertise in the Age of AI*, Cambridge-Londra, Belknap Press,

2020; Pasquariello, C., *I dati personali tra privacy e mercato: un difficile bilanciamento di interessi*, in Annoni, A., e

Thiene, A. (a cura di),
Minori e privacy. La tutela dei bambini e degli adolescenti alla luce del Regolamento (UE) 2016/679, Napoli, Jovene, 2019, 61 ss.;

Pasquino, T., *Tutela dei dati personali e regole di condotta nella prestazione di servizi della società dell'informazione*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 1073 ss.;

Pasquino, T., *Dignità della persona e diritti del malato*, in Lenti, L., Palermo Fabris, E., e Zatti, P. (a cura di), *I diritti in medicina*, nel *Trattato di biodiritto*, diretto da Rodotà e Zatti, Milano, Giuffrè, 2011, 543 ss.;

Pasquino, T., *Identità digitale della persona, diritto all'immagine e reputazione*, in Tosi, E. (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019, 93 ss.;

Passanante, L., *Prova e* privacy *nell'era di* internet *e dei* social network, in *Riv. trim. dir. e proc. civ*., 2018, 535 ss.;

Pastore, B., *Semantica della vulnerabilità, soggetto, cultura giuridica*, Torino, Giappichelli, 2021;

Pastore, B., *Le fonti del diritto al tempo dell'emergenza pandemica. Note su alcune tendenze in atto*, in *Società e diritti*, 2021, n. 11, 29 ss.;

Patti, S., *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ.*, 1999, II, 455 ss.;

Peigné, V., *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, in *Riv. it. med. leg.*, 2011, 1519 ss.;

Pellecchia, E., in Bianca, C.M., e Busnelli, F.D. (a cura di), *Tutela dei dati personali. Commentario alla l. 31 dicembre 1996, n. 675,* Padova, CEDAM, 1999, *sub* art. 22, 459 ss.;

Pellecchia, E., *Scelte contrattuali e informazioni personali*, Torino, Giappichelli, 2005;

Pellecchia, E., *La responsabilità civile per trattamento dei dati personali*, in *Resp. civ. e prev*., 2006, 223 ss.;

Pellecchia, E., voce «Dati personali (trattamento dei)», in *Il Diritto. Enc. giur. del Sole 24 Ore*, diretta da S. Patti, Milano, Il Sole 24 Ore, 2007, 4, 653 ss.;

Pellecchia, E., *Profilazione e decisioni automatizzate al tempo della* Black Box Society*: qualità dei dati e leggibilità dell'algoritmo nella cornice della* Responsible Research and Innovation, in *Nuove leggi civ. comm*., 2018, 1209 ss.;

Pellecchia, E., *Privacy, decisioni automatizzate e algoritmi*, in Tosi, E. (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019, 417 ss.;

Pellecchia, E., *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identifica- bilità nel GDPR*, in *Nuove leggi civ. comm*., 2020, 360 ss.;

Pellecchia, E., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 11, reg. Ue n. 679/2016, 270 ss.;

Peluso, M.G., Data Driven Innovation *in medicina, vantaggi e prospettive critiche*, in *Resp. med*., 2021, 225 ss.;

Penasa, S., e Tomasi, M., *The Italian Way for Research Biobanks After GDPR: Hybrid Normative Solutions to Balance the Protection of Individuals and Freedom of Research*, in Slokenberga, S., *et al*. (a cura di), *GDPR and Biobanking Individual Rights, Public Interest and Research Regulation across Europe*, Berlino, Springer, 2021, 309 ss.;

Perete Ramírez, C., e García Mexía, P., *La propiedad sobre el dato. ¿Cabe una vertiente patrimonial de la protección de datos?*, in *Revista de privacidad y derecho digital*, vol. 4, n. 15, 2019, 95 ss.;

Perlingieri, C., *L'incidenza dell'utilizzazione della tecnologia robotica nei rapporti civilistici*, in *Rass. dir. civ*., 2015, 1235

Perlingieri, C., *Responsabilità civile e robotica medica*, in *Tecnologie e diritto*, 2020, 161 ss.;

Perlingieri, C., *Diritto privato delle nuove tecnologie: contenuti e competenze*, in *Tecnologie e diritto*, 2021, fasc. 2, 70 ss.;

Perlingieri, G., *Pandemia da Coronavirus e rapporti contrattuali*, in Bocciolesi, E., e de Lucia, A. (a cura di), *Proposte interdisciplinari come contributi per ripartire nella società post-Covid-19*, Napoli, Edizioni Scientifiche Italiane, 2023, 345 ss.;

Perlingieri, P., *La personalità umana nell'ordinamento giuridico*, Napoli-Camerino, Edizioni Scientifiche Italiane, 1972;

Perlingieri, P., *Il diritto alla salute quale diritto della personalità*, in *Rass. dir. civ*., 1982, 1020 ss.;

Perlingieri, P., *Il diritto civile nella legalità costituzionale*, Napoli, Edizioni Scientifiche Italiane, 1984;

Perlingieri, P., *Diritto comunitario e legalità costituzionale. Per un sistema italo-comunitario delle fonti*, Napoli, Edizioni Scientifiche Italiane, 1992;

Perlingieri, P., *Il diritto alla salute quale diritto della personalità*, in Perlingieri, P., *La persona e i suoi diritti. Problemi del diritto civile*, Napoli, Edizioni Scientifiche Italiane, 2005, 101 ss.;

Perlingieri, P., *La pubblica amministrazione e la tutela della* privacy. *Gestione e riservatezza dell'informazione nell'attività ammini- strativa*, in Perlingieri, P., *La persona e i suoi diritti. Problemi del diritto civile*, Napoli, Edizioni Scientifiche Italiane, 2005, 255 ss.;

Perlingieri, P., *Il "diritto privato europeo" tra riduzionismo economico e dignità della persona*, in *Eur. e dir. priv*., 2010, 345 ss.; Perlingieri, P., Privacy *digitale e protezione dei dati personali tra persona e mercato*, in *Foro nap.*, 2018, 481 ss.;

Perlingieri, P., *Sul trattamento algoritmico dei dati*, in *Tecnologie e diritto*, 2020, 181 ss.; Perlingieri, P., *Note sul «potenziamento cognitivo»*, in *Tecnologie e diritto*, 2021, fasc. 1, 209 ss.;

Pertot, T., *Intelligenza artificiale e circolazione dei dati personali: basi giuridiche per il trattamento ed esigenze di tutela dell'utente interessato*, in Troiano, S. (a cura di), *Diritto privato e nuove tecnologie. Riflessioni incrociate tra esperienze giuridiche a confronto*, Napoli, Edizioni Scientifiche Italiane, 2022, 21 ss.;

Pioggia, A., *Consenso informato ai trattamenti sanitari e amministrazione della salute*, in *Riv. trim. dir. pubbl*., 2011, 127 ss.; Pioggia, A., *La sanità italiana di fronte alla pandemia. Un banco di prova che offre una lezione per il futuro*, in *Dir. pubbl*., 2020, 385 ss.;

Pioggia, A., *Diritto sanitario e dei servizi sociali*, 3a ed., Torino, Giappichelli, 2020;

Pioggia, A., *Il Fascicolo sanitario elettronico: opportunità e rischi dell'interoperabilità dei dati sanitari*, in Cavallo Perin, R. (a cura di), *L'amministrazione pubblica con i* big data*: da Torino un dibattito sull'intelligenza artificiale*, Torino, 2021, 215 ss.;

Pioggia, A., *La sanità nel Piano Nazionale di Ripresa e Resilienza*, in *Giornale di diritto amministrativo*, 2022, 165 ss.;

Piraino, A., *Privacy e comunicazioni elettroniche*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. II, Milano, Giuffrè, 2006, 1555 ss.;

Piraino, F., *Il codice della* privacy *e la tecnica del bilanciamento di interessi*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. I, Milano, Giuffrè, 2006, 695 ss.;

Piraino, F., *La liceità e la correttezza*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. I, Milano, Giuffrè, 2006, 745 ss.;

Piraino, F., *Per una teoria della ragionevolezza in diritto civile*, in *Eur. e dir. priv*., 2014, 1287 ss.;

Piraino, F., *Il contrasto sulla nozione di dato sensibile, sui presupposti e sulle modalità del trattamento*, in *Nuova giur. civ. comm.*, 2017, I, 1232 ss.;

Piraino, F., *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm*., 2017, 369 ss.;

Piraino, F., *I "diritti dell'interessato" nel Regolamento generale sulla protezione dei dati personali*, in Caterina, R. (a cura di), *GDPR tra novità e discontinuità*, in *Giur. it*., 2019, 2789 ss.;

Pirozzi, F., *Il diritto all'autodeterminazione nell'attività sanitaria*, in *Riv. it. med. leg*., 2020, 91 ss.;

Pisani, C., Proia, G., e Topo, A. (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Milano, Giuffrè, 2022;

Pitea, C., e Tomasi, L., nel *Commentario breve alla Convenzione europea dei diritti dell'uomo Bartole De Sena Zagrebelsky*, 2012, *sub* art. 8, 297 ss.;

Pitruzzella, G., *Big data, competition and privacy: a look from the antitrust perspective*, in *Concorrenza e mercato*, 2016, 15 ss.; Pitruzzella, G., *L'Unione europea come "comunità di valori" e la forza costituzionale del valore dello "stato di diritto"*, in *Federalismi*, fasc. 28, 2021, IV ss., in *www.federalismi.it*, 15 dicembre 2021;

Piva, P., *Principi e metodi di interpretazione della Corte di giustizia nel sistema giuridico dell'UE*, in *Ars interpretandi*, 2020, 117 ss.;

Pizzetti, F., *Postfazione*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. II, Milano, Giuffrè, 2006, 2275 ss.;

Pizzetti, F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016;

Pizzetti, F. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018;

Pizzetti, F., *GDPR e Intelligenza artificiale. Codici di condotta, certificazioni, sigilli, marchi e altri poteri di* soft law *previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA*, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 69 ss.;

Pizzetti, F. (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, Giappichelli, 2021;

Pizzetti, F., *Il sistema normativo di protezione dei trattamenti di dati personali nel quadro europeo e nazionale*, in Pizzetti, F. (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, Giappichelli, 2021, 3 ss.;

Pizzolato, F., *Autodeterminazione e relazionalità nella tutela della salute*, in *Corti supreme e salute*, 2018, fasc. 2, 429 ss.;

Plaia, A., *La responsabilità da illecito trattamento dei dati personali*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. II, Milano, Giuffrè, 2006, 2005 ss.;

Poggi, A., *Dati personali. Una soluzione «giurisdizionale» oppure «amministrativa» per effettiva tutela del cittadino?*, in Losano,
M.G. (a cura di), *La legge italiana sulla* privacy. *Un bilancio dei primi cinque anni*, Roma-Bari, Laterza, 2001, 115 ss.;

Poggi, A., *Green pass, obbligo vaccinale e le scelte del Governo*, in *Federalismi*, n. 21, 2021, IV ss., in *www.federalismi.it*, 8 settembre 2021;

Poletti, D., in Bianca, C.M., e Busnelli, F.D. (a cura di), *Tutela dei dati personali. Commentario alla l. 31 dicembre 1996, n. 675*, Padova, CEDAM, 1999, *sub* art. 23, 560 ss.;

Poletti, D., in Bianca, C.M., e Busnelli, F.D. (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n.*
196, Codice della privacy, Padova, CEDAM, 2007, *sub* art. 75, 1195 ss.;

Poletti, D., in Bianca, C.M., e Busnelli, F.D. (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n.*
196, Codice della privacy, Padova, CEDAM, 2007, *sub* art. 76, 1212 ss.;

Poletti, D., *Comprendere il Reg. UE 2016/679: un'introduzione*, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 9 ss.;

Poletti, D., e Causarano, M.C., *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in Tosi, E. (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019, 369 ss.;

Poletti, D., *Le condizioni di liceità del trattamento dei dati personali*, in Caterina, R. (a cura di), *GDPR tra novità e discontinuità*, in
Giur. it., 2019, 2783 ss.;

Poletti, D., *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza*, in *Persona e mercato*, 2020, fasc. 2, 65 ss.;

Poletti, D., in Pertot, T. (a cura di), *Rechte an Daten*, Tubinga, Mohr Siebeck, 2020, *Holding Data between possessio and detentio*, 127 ss.;

Poletti, D., Contact tracing *e app immuni: atto secondo*, in *Persona e mercato*, 2021, fasc. 1, 91 ss.;

Poletti, D., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 6, reg. Ue n. 679/2016, 192 ss.;

Poletti, D., *Gli intermediari dei dati*, in Morace Pinelli, A. (a cura di), *La circolazione dei dati personali. Persona, contratto e mercato*, Pisa, Pacini, 2023, 105 ss.;

Polini, M., *Privacy e protezione dei dati personali nell'ordinamento europeo e italiano*, in Maglio, M., Polini, M., e Tilli, N. (a cura di), *Manuale di diritto alla protezione dei dati personali. La privacy dopo il Regolamento Ue 2016/679*, Santarcangelo di Romagna, Maggioli, 2017, 25 ss.;

Polito, F., *et al.* (a cura di), *Sicurezza e privacy in ambito sanitario*, Roma, Edisef, 2012;

Politou, E., *et al*., *Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions*, in *Journal of Cybersecurity*, 2018, vol. 4, n. 1, 1 ss.;

Politou, E., *et al.*, *Privacy and Data Protection Challenges in the Distributed Era*, Berlino, Springer, 2021;

Pollicino, O., e Bassini, M., Social network *e tutela dei dati personali*, in Scaffardi, L. (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, Torino, Giappichelli, 2018, 65 ss.;

Pollicino, O., e Bassini, M., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 8, Carta dei diritti fondamentali dell'Unione europea, 36 ss.;

Polvani, T., *La responsabilità da illecito trattamento dei dati personali*, in Adinolfi, A., e Simoncini, A. (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuri- diche*, Napoli, Edizioni Scientifiche Italiane, 2022, 557 ss.;

Popoli, A.R., Social network *e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, in *Dir. inf.*, 2014, 981 ss.;

Popoli, A.R., *Codici di condotta e certificazioni*, in Finocchiaro, G. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 367 ss.;

Popoli, A.R., *Codici di condotta e certificazioni*, in Finocchiaro, G. (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 527 ss.;

Porcelli, M., *Tecnologie robotiche e responsabilità per danni tra prospettive reali e falsi miti*, in *Tecnologie e diritto*, 2020, 506 ss.; Pormeister, K., *Genetic data and the research exemption: is the GDPR going too far?*, in *International Data Privacy Law*, vol. 7, n. 2, 2017, 137 ss.;

Pormeister, K., *The logical fallacies of the legal bases for data processing in and beyond clinical trials*, in *International Data Privacy Law*, vol. 12, n. 2, 2022, 132 ss.;

Porrini, D., *Asimmetrie informative e concorrenzialità nel mercato assicurativo: che cosa cambia con i big data?*, in *Concorrenza e mercato*, 2016, 139 ss.;

Post, R., *Three Concepts of Privacy*, in *Georgetown Law Journal*, 2001, vol. 89, n. 6, 2087 ss.;

Posteraro, N., *Cure oltre lo Stato: l'effettività del diritto alla salute alla luce del d.lgs. n. 38 del 2014*, in *www.federalismi.it*, 23 novembre 2016;

Posteraro, N., *La responsabilità del medico nelle prime applicazioni della legge Gelli-Bianco*, Roma, Dike, 2019;

Posteraro, N., e Cavalcanti, G., *Sanità digitale in Italia: il Fascicolo Sanitario Elettronico (FSE) dopo le modifiche introdotte dal decreto Rilancio*, in *www.irpa.eu, Osservatorio sullo Stato digitale*, 25 marzo 2021;

Posteraro, N., *Active international healthcare mobility and urban accessibility: the essential role of Italian cities and urban planning in the development of foreign healthcare tourism*, in *www.federalismi.it*, 13 gennaio 2021;

Posteraro, N., *Lo Stato Digitale nel PNRR – La telemedicina*, in *www.irpa.eu, Osservatorio sullo Stato digitale*, 29 luglio 2021; Posteraro, N., *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *www.federalismi.it*, 17 novembre 2021;

Posteraro, N., *The digitalization of the healthcare sector in Italy: the Electronic Health Record*, in Sandulli, M.A., e Aperio Bella, F. (a cura di), *Shaping the Future of Health Law: Challenges for Public Law*, in *www.federalismi.it*, 17 novembre 2021, 10 ss.;

Posteraro, N., *Il fascicolo sanitario elettronico*, in Bontempi, V. (a cura di), *Lo Stato digitale nel Piano nazionale di ripresa e resi- lienza*, Università degli Studi Roma Tre, 2022, 187 ss.;

Posteraro, N., *La telemedicina*, in Bontempi, V. (a cura di), *Lo Stato digitale nel Piano nazionale di ripresa e resilienza*, Università degli Studi Roma Tre, 2022, 201 ss.;

Previti, L., *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *Federalismi*, fasc. 25, 2022, 65 ss., in *www.federalismi.it*, 5 ottobre 2022;

Price, W.N., e Cohen, I.G., *Privacy in the age of medical big data*, in *Nature Medicine*, 2019, vol. 25, 37 ss.;

Principato, A., *Verso nuovi approcci alla tutela della* privacy*:* privacy by design e privacy by default settings, in *Contr. e impr. Eur.*, 2015, 197 ss.;

Prins, C., *Property and Privacy: European Perspectives and the Commodification of our Identity*, in *Information Law Series*, 2006, vol. 16, 223 ss.;

Proia, G., *Trattamento dei dati personali, rapporto di lavoro e l'«impatto» della nuova disciplina dei controlli a distanza*, in *Riv. it. dir. lav.*, 2016, 547 ss.;

Proietti, G., *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati personali*, in *Contr. e impr.*, 2022, 880 ss.; Prosser, W.L., *Privacy*, in *California Law Review*, 1960, vol. 48, n. 3, 383 ss.;

Provolo, D., *L'identità genetica nella tutela penale della privacy e contro la discriminazione*, Padova University Press, 2018; Pucella, R., *Autodeterminazione e responsabilità nella relazione di cura*, Milano, Giuffrè, 2010;

Pucella, R., *L'illiceità dell'atto medico tra lesione della salute e violazione del consenso*, in Belvedere, A., e Riondato, S. (a cura di),
Le responsabilità in medicina, nel *Trattato di biodiritto* diretto da Rodotà e Zatti, Giuffrè, 2011, 185 ss.;

Pucella, R., *Onere della prova nella responsabilità medica: l'impatto della Legge Gelli-Bianco*, in *Resp. med*., 2022, 365 ss.; Pucella, R., *Scelte tragiche e dilemmi giuridici ai tempi della pandemia*, in *Nuova giur. civ. comm*., 2020, suppl., 24 ss.;

Pucella, R., e Bettoncelli, G., *Brevi riflessioni sulla tragica esperienza da Covid-19: la prospettiva del giurista e del medico di medi- cina generale*, in *Resp. med*., 2020, 197 ss.;

Punzi, A., *La persona nei dati. Ragioni e modelli di una regolamentazione*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 761 ss.;

Punzi, A., *Il dialogo delle intelligenze tra umanesimo e tecnoscienza*, in *Persona e mercato*, 2023, 161 ss.;

Pupolizio, I., *Materiali per uno studio sociologico della distinzione tra diritto pubblico e diritto privato*, in *Sociologia del diritto*, 2012, fasc. 2, 7 ss.;

Purpura, A., *Il consenso nel mercato dei dati personali. Considerazioni al tempo dei* big data, in *Jus civile*, 2022, 891 ss.;

Putignani, A., *Consenso e disposizione della privacy*, in Clemente, A. (a cura di), *Privacy*, Padova, CEDAM, 1999, 213 ss.;

Putignani, A., *Prospettive costituzionali del diritto di privacy*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. I, Milano, Giuffrè, 2006, 109 ss.;

Py, B., e Olech, V., *Impact of EU Regulation 2016/679 on the French health system*, in Fares, G. (a cura di), *The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis*, Torino, Giappichelli, 2021, 141 ss.;

Quinn, P., *The Anonymisation of Research Data — A Pyric Victory for Privacy that Should Not Be Pushed Too Hard by the eu Data Protection Framework?*, in *European Journal of Health Law*, vol. 24, n. 4, 2017, 347 ss.;

Quiroz Vitale, M.A., in Sciaudone, R., e Caravà, E. (a cura di), *Il codice della privacy. Commento al D.Lgs. 30 giugno 2003, n. 196 e al D.Lgs. 10 agosto 2018, n. 101 alla luce del Regolamento (UE) 2016/679 (GDPR)*, Pisa, Pacini, 2019, *sub* art. 2-*sexies*, 73 ss.;

Raimondeau, J., e Carmona, E., *Les données de santé*, in Raimondeau, J., *et al.* (a cura di), *Manuel de santé publique*, Rennes, Presses de l'EHESP, 2020, 101 ss.;

Ramaccioni, G., *La risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali*, in Ruscello, F. (a cura di), *Studi in onore di Davide Messinetti*, II, Napoli, Edizioni Scientifiche Italiane, 2008, 243 ss.;

Rapisarda, I., *Consenso informato e autodeterminazione terapeutica*, in *Nuove leggi. civ. comm*., 2019, 43 ss.;

Rapisarda, I., *La* privacy *sanitaria alla prova del* mobile ecosystem*. Il caso delle* app *mediche*, in *Nuove leggi civ. comm*., 2023, 184 ss.;

Ratti, M., *Il regime sanzionatorio previsto dal Regolamento per l'illecito trattamento dei dati personali*, in Finocchiaro, G. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 595 ss.;

Ratti, M., *La responsabilità da illecito trattamento dei dati personali nel nuovo Regolamento*, in Finocchiaro, G. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 615 ss.;

Riccio, Gio.M., Privacy *e dati sanitari*, in Cardarelli, F., Sica, S., e Zeno-Zencovich, V. (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, Giuffrè, 2004, 247 ss.;

Riccio, Giu.M., in Sica, S., e Stanzione, P. (a cura di), *La nuova disciplina della privacy. Commentario al d.lgs. 30 giugno 2003, n.*
196, Bologna, Zanichelli, 2004, *sub* artt. 23 ss., 89 ss.;

Riccio, Gio.M., Scorza, G., e Belisario, E. (a cura di), *GDPR e normativa privacy. Commentario*, Milano, Ipsoa, 2018;

Riccio, Gio.M., e Pezza, F., *Portabilità dei dati personali e interoperabilità*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 397 ss.;

Riccio, Gio.M., *La giurisprudenza su Facebook / Casa Pound e l'esigenza di eteroregolazione del contratto con il social network*, in Stanzione, P. (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, Giappichelli, 2022, 339 ss.;

Riccio, Gio.M., Ziccardi, G., e Scorza, G. (a cura di), *Intelligenza artificiale. Profili giuridici*, Padova, Cleup, 2022; Riccio,

Gio.M., *Il metaverso e la necessità di superare i dogmi proprietari*, in *Diritto di Internet*, 2023, 233 ss.;

Ricciuto, V., *Comunicazione e diffusione dei dati personali e trattamento di dati particolari*, in Cuffaro, V., e Ricciuto, V., (a cura di), *La disciplina del trattamento dei dati personali*, Torino, Giappichelli, 1997, 267 ss.;

Ricciuto, V., *Le finalità del Codice*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 13 ss.;

Ricciuto, V., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf.*, 2018, 689 ss.;

Ricciuto, V., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in Cuffaro, V., D'Ora-
zio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 23 ss.;

Ricciuto, V., *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, in Zorzi Galgano, N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, CEDAM, 2019, 95 ss.;

Ricciuto, V., *Circolazione e scambio di dati personali. Il problema della regolazione del nuovo fenomeno patrimoniale*, in Aa.Vv.,
Per i cento anni dalla nascita di Renato Scognamiglio, Napoli, Jovene, 2022, 905 ss.;

Ricciuto, V., *Il trattamento dei dati personali come nuovo fenomeno patrimoniale*, in D'Auria, M. (a cura di), *I problemi dell'infor-*
mazione nel diritto civile, oggi. Studi in onore di Vincenzo Cuffaro, Roma Tre-press, 2022, 323 ss.; Ricciuto, V.,

L'equivoco della privacy. Persona vs *dato personale*, Napoli, Edizioni Scientifiche Italiane, 2022;

Ricciuto, V., *Il consenso negoziale nella circolazione dei dati personali*, in Morace Pinelli, A. (a cura di), *La circolazione dei dati personali. Persona, contratto e mercato*, Pisa, Pacini, 2023, 65 ss.;

Riccobene, A., *Il danno cagionato per effetto del trattamento e i diversi modelli risarcitori*, in Panetta, R. (a cura di), *Libera circola- zione e protezione dei dati personali*, t. II, Milano, Giuffrè, 2006, 2019 ss.;

Richards, N., Serwin, A., e Blake, T., *Understanding American privacy*, in González Fuster, G., Van Brakel, R., e De Hert, P. (a cura di), *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics*, Cheltenham, Elgar, 2022, 60 ss.;

Richardson, M., *The Right to Privacy. Origins and Influence of a Nineteenth-Century Idea*, Cambridge University Press, 2017;

Rinoldi, D.G., *«In deroga… e in conformità»: prospettive dell'Unione europea della salute muovendo dall'art. 168 TFUE per andar ben oltre (verso un comparto sanitario federale continentale?)*, in *Corti supreme e salute*, 2022, fasc. 1, 273 ss.;

Rizzo, A., *La crisi pandemica e la nuova centralità delle politiche sanitarie europee alla luce della disciplina "EU4Health"*, in *Studi sull'integrazione europea*, 2021, 107 ss.;

Rodotà, S., *Elaboratori elettronici e controllo sociale*, Bologna, il Mulino, 1973;

Rodotà, S., *Protezione dei dati e circolazione delle informazioni*, in *Riv. crit. dir. priv*., 1984, 721 ss.; Rodotà, S., *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in *Pol. dir*., 1991, 521 ss.; Rodotà, S., *Tecnologie e diritti*, Bologna, il Mulino, 1995;

Rodotà, S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv*., 1997, 583 ss.;

Rodotà, S., *Relazione per l'anno 1997 del garante per la protezione dei dati personali*, in *Dir. inf*., 1998, 553 ss.;

Rodotà, S., *Prefazione*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. I, Milano, Giuffrè, 2006, VII ss.;

Rodotà, S., *La persona*, in Castronovo, C., e Mazzamuto, S. (a cura di), *Manuale di diritto privato europeo*, vol. I, *Fonti, persone e famiglia*, Milano, Giuffrè, 2007, 193 ss.;

Rodotà, S., *Editoriale*, in *Riv. crit. dir. priv*., 2009, 3 ss.;

Rodotà, S., *Data Protection as a Fundamental Right*, in Gutwirth, S., *et al.* (a cura di), *Reinventing Data Protection?*, Berlino, Sprin- ger, 2009, 77 ss.;

Rodotà, S., *Il nuovo* habeas corpus*: la persona costituzionalizzata e la sua autodeterminazione*, in Rodotà, S., e Tallacchini, M. (a cura di), *Ambito e fonti del biodiritto*, nel *Trattato di biodiritto* diretto da Rodotà e Zatti, Milano, Giuffrè, 2010, 169 ss.;

Rodotà, S., *Il corpo "giuridificato"*, in Canestrari, S., Ferrando, G., Mazzoni, C.M., Rodotà, S., e Zatti, P. (a cura di), *Il governo del corpo*, nel *Trattato di biodiritto* diretto da Rodotà e Zatti, t. I, Milano, Giuffrè, 2011, 51 ss.;

Rodotà, S., *Prefazione*, in Trojsi, A., *Il diritto del lavoratore alla protezione dei dati personali*, Torino, Giappichelli, 2013;

Rodotà, S., *Il diritto di avere diritti*, 3a ed., Bari-Roma, Laterza, 2017;

Rodotà, S., *Vivere la democrazia*, Bari-Roma, Laterza, 2018;

Rodotà, S., *Controllo e privacy della vita quotidiana. Dalla tutela della vita privata alla protezione dei dati personali*, in *Riv. crit. dir. priv*., 2019, 9 ss.;

Rodriguez, D., *Le figure professionali*, in Lenti, L., Palermo Fabris, E., e Zatti, P. (a cura di), *I diritti in medicina*, nel *Trattato di biodiritto*, diretto da Rodotà e Zatti, Milano, Giuffrè, 2011, 115 ss.;

Rodríguez Ayuso, J. F., *Protección de datos personales en el contexto de la Covid-19: legitimación en el tratamiento de datos de salud por las Administraciones Públicas*, in *Revista catalana de Dret públic*, 2020, fasc. 3, 137 ss.;

Rolando, F., *La tutela della salute nel diritto dell'Unione europea e la risposta dell'UE all'emergenza Covid-19*, in *L'emergenza sanitaria Covid-19 e il diritto dell'Unione europea. La crisi, la cura, le prospettive*, numero speciale di Eurojus, 2020;

Romagnoli, G., *La trasparenza dei dati ed il diritto di accesso alla «documentazione sanitaria disponibile»*, in *Resp. med*., 2020, 345 ss.;

Romano, F., *Intelligenza Artificiale e amministrazioni pubbliche: tra passato e presente*, in *Ciberspazio e diritto*, 2020, 69 ss.; Romeo, F., *Il governo giuridico delle tecniche dell'informazione e della comunicazione*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1243 ss.;

Rosenberg, N., *et al.*, *Scienza, tecnologia, società alle soglie del XXI secolo. Atti del congresso*, Stresa, 25-26 ottobre 1996, Milano, 1997;

Rossetti, A., *Agenti naturalmente automatici*, in *Notizie di Politeia*, 2021, n. 143, 144 ss.;

Rossi, L.S., *Brevi osservazioni sulle recenti tendenze evolutive della giurisprudenza della Corte di Giustizia dell'Unione europea sulla protezione dei dati personali*, in Rossi Dal Pozzo, F. (a cura di), *Mercato unico digitale, dati personali e diritti fondamentali*, numero speciale di *Eurojus*, 2020, 51 ss.;

Rossi Carleo, L., *Il mercato tra scelte volontarie e comportamenti obbligatori*, in Ruscello, F. (a cura di), *Studi in onore di Davide Messinetti*, I, Napoli, Edizioni Scientifiche Italiane, 2008, 843 ss.;

Rossi Dal Pozzo, F. (a cura di), *Mercato unico digitale, dati personali e diritti fondamentali*, numero speciale di *Eurojus*, 2020;

Rothstein, M.A., *Big Data, Surveillance Capitalism, and Precision Medicine: Challenges for Privacy*, in *The Journal of Law Medicine & Ethics*, 2021, vol. 49, n. 4, 666 ss.;

Rotondo, A., *Prevenzione e contrasto della minaccia informatica in Europa: note a margine del Regolamento (UE) 2019/881*, in *Tecnologie e diritto*, 2020, 195 ss.;

Rouvroy, A., e Poullet, Y., *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Im- portance of Privacy for Democracy*, in Gutwirth, S., *et al.* (a cura di), *Reinventing Data Protection?*, Berlino, Springer, 2009, 45 ss.;

Rubecchi, M., *I decreti del Presidente. Studio su d.P.C.m., atti normativi del governo e dinamiche decisionali*, Torino, Giappichelli, 2022;

Rubinstein, I.S., *Big Data: The End of Privacy or a New Beginning?*, in *International Data Privacy Law*, vol. 3, n. 2, 2013, 74 ss.;

Ruffolo, U., *Dati personali: trattamento e responsabilità*, in Cuffaro, V., Ricciuto, V., e Zeno-Zencovich, V. (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffrè, 1999, 281 ss.;

Ruffolo, U., *Intelligenza Artificiale,* machine learning *e responsabilità da algoritmo*, in Gabrielli, E., e Ruffolo, U. (a cura di), *Intel- ligenza Artificiale e diritto*, in *Giur. it*., 2019, 1689 ss.;

Ruffolo, U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, Giuffrè, 2020;

Ruffolo, U., *L'Intelligenza artificiale in sanità: dispositivi medici, responsabilità e "potenziamento"*, in Gabrielli, E., e Ruffolo, U. (a cura di), *La responsabilità medica*, in *Giur. it*., 2021, 502 ss.;

Rufo, L., *Social media e consulto medico: tra opportunità e rischi per i pazienti*, in *Inform. e dir*., 2017, fasc. 1-2, 383 ss.;

Rufo, L., *L'intelligenza artificiale in sanità: tra prospettive e nuovi diritti*, in D'Aloia, A. (a cura di), *Intelligenza artificiale e diritto.*
Come regolare un mondo nuovo, Milano, FrancoAngeli, 2021, 451 ss.;

Rugani, G., *Il diritto all'oblio dell'articolo 17 Regolamento (UE) 2016/679: una grande novità? Una denominazione opportuna?*, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 455 ss.;

Rugani, G., *Le condizioni ricavabili dal Regolamento generale sulla protezione dei dati per le applicazioni nazionali di tracciamento dei contatti: alcune considerazioni*, in *European Papers*, vol. 5, fasc. 1, 2020, 633 ss.;

Ruggeri, L., *La dicotomia dati personali e dati non personali: il problema della tutela della persona nei c.dd. dati misti*, in *Dir. fam. e pers*., 2023, 808 ss.;

Ruggieri, F., *Trattamento dei dati personali e tutela dei minori*, in Orlando, S., e Capaldo, G. (a cura di), *Annuario 2022 Osservatorio Giuridico sulla Innovazione Digitale*, Roma, sapienza Università Editrice, 2022, 325 ss.;

Ruotolo, G.M., *I dati non personali: l'emersione dei* big data *nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 2018, 97 ss.;

Ruotolo, G.M., *Scritti di diritto internazionale ed europeo dei dati*, Bari, Cacucci, 2021;

Ruscello, F., *Rilevanza dei diritti della persona e «ordinamento comunitario»*, Napoli, Edizioni Scientifiche Italiane, 1993;

Russo, E., *L'interpretazione dei testi normativi comunitari*, nel *Trattato di diritto privato* a cura di Iudica e Zatti, Milano, Giuffrè, 2008;

Senigaglia, R., *Social Media, Mobile Apps and Children Protection*, in Senigaglia, R., Irti, C., e Bernes, A. (a cura di), *Privacy and Data Protection in Software Services*, Berlino, Springer, 2022, 35 ss.;

Sergi, A., *Intelligenza artificiale e soggettività giuridica: profili storici e questioni ontologiche*, in Riccio, Gio.M., Ziccardi, G., e Scorza, G. (a cura di), *Intelligenza artificiale. Profili giuridici*, Padova, Cleup, 2022, 15 ss.;

Séroussi, B., *et al*., *Transforming Data into Knowledge: How to Improve the Efficiency of Clinical Care?*, in *Yearbook of Medical Informatics*, 2017, 4 ss.;

Séroussi, B., *et al*., *Transparency of Health Informatics Processes as the Condition of Healthcare Professionals' and Patients' Trust and Adoption: the Rise of Ethical Requirements*, in *Yearbook of Medical Informatics*, New York, Thieme, 2020, 7 ss.;

Serra, A., *Note in tema di trattamento dei dati personali e di disciplina dell'impresa*, in Cuffaro, V., Ricciuto, V., e Zeno-Zencovich,V. (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffrè, 1999, 103 ss.;

Simeone, G., *Machine Learning e tutela della Privacy alla luce del GDPR*, in Alpa, G. (a cura di), *Diritto e intelligenza artificiale*, Pisa, Pacini, 2020, 275 ss.;

Soffientini, M., *Impatto privacy dell'intelligenza artificiale in ambito sanitario*, in *Diritto e pratica del lavoro*, 2021, 291 ss.;

Solas-Martínez, J.L., *et al*., *Artificial Intelligence and Augmented Reality in Physical Activity: A Review of Systems and Devices*, in Geroimenko, V. (a cura di), *Augmented Reality and Artificial Intelligence. The Fusion of Advanced Technologies*, Berlino, Springer, 2023, 245 ss.;

Soulamia, L.F., *et al*., *Health Data, Information, and Knowledge Sharing for Addressing the COVID-19*, in *Yearbook of Medical Informatics*, 2021, 4 ss.;

Sganga, C., *A Decade of Fair Balance Doctrine, and How to Fix It: Copyright Versus Fundamental Rights Before the CJEU from Promusicae to Funke Medien, Pelham and Spiegel Online*, in *European Intellectual Property Review*, vol. 11, 2019, 683 ss.;

Shabani, M., e Borry, P., *Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation*, in *European Journal of Human Genetics*, vol. 26, 2018, 149 ss.;

Sica, S., in Giannantonio, E., Losano, M.G., e Zeno-Zencovich, V. (a cura di), *La tutela dei dati personali. Commentario alla l.675/1996*, Padova, CEDAM, 1997, *sub* art. 18, 174 ss.;

Sica, S., *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ*., 2001, II, 621 ss.; Sica, S., *La «riforma» della privacy ed il nuovo sistema di informativa e consenso: ben più di una modifica applicativa*, in *Corr. giur*.,2002, 537 ss.;

Sica, S., e Stanzione, P. (a cura di), *La nuova disciplina della privacy. Commentario al d.lgs. 30 giugno 2003, n. 196*, Bologna, Zanichelli, 2004;

Sica, S., in Sica, S., e Stanzione, P. (a cura di), *La nuova disciplina della privacy. Commentario al d.lgs. 30 giugno 2003, n. 196*, Bologna, Zanichelli, 2004, *sub* artt. 7 ss., 39 ss.;

Sica, S., *Le tutele civili*, in Cardarelli, F., Sica, S., e Zeno-Zencovich, V. (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, Giuffrè, 2004, 541 ss.;

Sica, S., *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in Sica, S., D'Antonio, V., e Riccio, Gio.M. (a cura di), *La nuova disciplina europea della privacy*, Padova, CEDAM, 2016, 1 ss.;

Sica, S., D'Antonio, V., e Riccio, Gio.M. (a cura di), *La nuova disciplina europea della privacy*, Padova, CEDAM, 2016;

Sica, S., *La responsabilità civile per il trattamento illecito dei dati personali*, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 161 ss.;

Sica, S., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 82, reg. Ue n. 679/2016, 887 ss.;

Sica, S., *Pubblico e privato al tempo della trasformazione digitale*, in *Tecnologie e diritto*, 2021, fasc. 2, 89 ss.;

Sica, S., e D'Antonio, V., *La* commodification *dei dati personali nella* data driven society, in Stanzione, P. (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, Giappichelli, 2022, 129 ss.;

Simitis, S., *«Sensitive Daten» – Zur Geschichte und Wirkung einer Fiktion*, in *Festschrift zum 65. Geburtstag von Mario M. Pedraz- zini*, Bern, Stämpfli, 1990, 469 ss.;

Simitis, S., *Il contesto giuridico e politico della tutela della privacy*, in *Riv. crit. dir. priv*., 1997;

Simitis, S., *Revising Sensitive Data. Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, in *www.coe.int*, 1999;

Simitis, S., Hornung, G., e Spiecker gen. Döhmann, I. (a cura di), *Kommentar Datenschutzrecht*, Baden-Baden. Nomos, 2019;

Simoncini, A., *L'algoritmo* incostituzionale*: intelligenza artificiale e il futuro delle libertà*, in D'Aloia, A. (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, FrancoAngeli, 2021, 167 ss.;

Simoncini, A., *La proposta di regolazione europea dell'intelligenza artificiale. Prime riflessioni*, in Adinolfi, A., e Simoncini, A. (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, Edizioni Scientifiche Italiane, 2022, 1 ss.;

Simoncini, A., *Quale modello per la regolazione dell'intelligenza artificiale? L'Europa al bivio*, in Camardi, C. (a cura di), *La via europea per l'intelligenza artificiale. Atti del convegno del progetto dottorale di alta formazione in scienze giuridiche, Ca' Foscari Venezia, 25-26 novembre 2021*, Padova, CEDAM, 2022, 239 ss.;

Sinisi, M., *Data governance and Clinical risk management*, in Sandulli, M.A., e Aperio Bella, F. (a cura di), *Shaping the Future of Health Law: Challenges for Public Law*, in *www.federalismi.it*, 17 novembre 2021, 14 ss.;

Sirgiovanni, B., *Dal consenso dell'interessato alla "responsabilizzazione" del titolare del trattamento dei dati genetici*, in *Nuove leggi civ. comm.*, 2020, 1010 ss.;

Slama, A.-G., *La regressione democratica*, trad. Brambilla, Milano, Spirali, 2006;

Slokenberga, S., *et al.* (a cura di), *GDPR and Biobanking Individual Rights, Public Interest and Research Regulation across Europe*, Berlino, Springer, 2021;

Slokenberga, S., *et al.*, *Governing, Protecting, and Regulating the Future of Genome Editing: The Significance of ELSPI Perspectives*, in *European Journal of Health Law*, vol. 29, n. 3-5, 2022, 327 ss.;

Smyth, S.M., *Biometrics, Surveillance and the Law. Societies of Restricted Access, Discipline and Control*, Londra, Routledge, 2019;

Snijders, T., e van Deursen, S., *The Road Not Taken – the CJEU Sheds Light on the Role of Fundamental Rights in the European Copyright Framework – a Case Note on the* Pelham, Spiegel Online *and* Funke Medien *Decisions*, in *International Review of Intellectual Property and Competition Law*, vol. 50, 2019, 1176 ss.;

Solinas, C., *La nuova figura del responsabile della protezione dei dati*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 879 ss.;

Solinas, C., *Il mercato dei dati personali: the Elephant in the room*, in Morace Pinelli, A. (a cura di), *La circolazione dei dati personali.Persona, contratto e mercato*, Pisa, Pacini, 2023, 189 ss.;

Solove, D.J., *The Myth of the Privacy Paradox*, in *GW Law Faculty Publications & Other Works*, in *www.scholarship.law.gwu.edu*, 1° febbraio 2020;

Solove, D.J., *Introduction: privacy self-management and the consent dilemma*, in *Harvard Law Review*, 2013, 1880 ss.;

Soro, A., *Autodeterminazione terapeutica ed autodeterminazione informativa: i nuovi aspetti della dignità*, intervento al Convegno "La smaterializzazione dei documenti e il suo impatto sul sistema salute", in *www.garanteprivacy.it*, 6 maggio 2016;

Soro, A., *Persone in rete. I dati tra poteri e diritti*, Roma, Fazi Editore, 2018;
Soro, A., *L'universo dei dati e la libertà della persona. Discorso del Presidente*, in *www.garanteprivacy.it*, 7 maggio 2019;

Soro, A., *Democrazia e potere dei dati. Libertà, algoritmi, umanesimo digitale*, Milano, Baldini+Castoldi, 2019;

Sorrentino, E., e Spagnuolo, A.F., *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico*, in *Federalismi*, fasc. 30, 2020, 251, consultabile all'indirizzo *www.federalismi.it*, 4 novembre 2020;

Spangaro, A., *L'ambito di riferimento materiale del nuovo Regolamento*, in Finocchiaro, G. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 23 ss.;

Spangaro, A., *L'ambito di applicazione materiale della disciplina del Regolamento europeo 679/2016*, in Finocchiaro, G. (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zani- chelli, 2019, 27 ss.;

Spiecker gen. Döhmann, I., *Information Management*, in Cane, P., *et al.* (a cura di), *The Oxford Handbook of Comparative Adminis- trative Law*, Oxford, 2020, 677 ss.;

Spiecker gen. Döhmann, I., *The impact of EU Regulation 2016/679 on the German health system*, in Fares, G. (a cura di), *The Pro- tection of Personal Data Concerning Health at the European Level. A Comparative Analysis*, Torino, Giappichelli, 2021, 83 ss.;

Spiecker gen. Döhmann, I., Papakonstantinou, V., Hornung, G., e de Hert, P. (a cura di), *General Data Protection Regulation. Article- by-Article Commentary*, Baden-Baden, Nomos, 2023;

Spina, A., *Alla ricerca di un modello di regolazione per l'economia dei dati. Commento al Regolamento (UE) 2016/679*, in *Rivista della Regolazione dei mercati*, 2016, 143 ss.;

Spina, A., *La medicina degli algoritmi: Intelligenza Artificiale, medicina digitale e regolazione dei dati personali*, in Pizzetti, F. (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018, 319 ss.;

Spoto, G., *I diritti dei consumatori*, in Panetta, R. (a cura di), *Libera circolazione e protezione dei dati personali*, t. I, Milano, Giuffrè, 2006, 387 ss.;

Stanzione, M.G., *Identità del figlio e diritto di conoscere le proprie origini*, Torino, Giappichelli, 2015;

Stanzione, M.G., *Il nuovo regolamento europeo sulla protezione dei dati personali: genesi e ambito di applicazione*, in *www.compa- razionedirittocivile.it*, giugno 2016;

Stanzione, M.G., *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. e dir. priv.*, 2016, 1249 ss.;

Stanzione, M.G., *Genesi a ambito di applicazione*, in Sica, S., D'Antonio, V., e Riccio, Gio.M. (a cura di), *La nuova disciplina europea della privacy*, Padova, CEDAM, 2016, 13 ss.;

Stanzione, M.G., *Libertà di espressione e diritto alla privacy nel dialogo delle corti. Il caso del diritto all'oblio*, in *Eur. e dir. priv.*, 2020, 991 ss.;

Stanzione, M.G., *La protezione dei dati personali tra «consumerizzazione» della* privacy *e principio di* accountability, in *Compara- zione e diritto civile*, 2022, 1 ss.;

Stanzione, M.G., *Consenso e trattamento di dati personali nella dimensione europea*, in Stanzione, P. (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, Giappichelli, 2022, 77 ss.;

Stanzione, P., *Data Protection and vulnerability*, in *European Journal of Privacy Law & Technologies*, 2020, fasc. 2, 9 ss.;

Stanzione, P., *Introduzione*, in Stanzione, P. (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, Giappichelli, 2022, 1 ss.;

Stanzione, P., *La via europea all'intelligenza artificiale*, in Camardi, C. (a cura di), *La via europea per l'intelligenza artificiale. Atti del convegno del progetto dottorale di alta formazione in scienze giuridiche, Ca' Foscari Venezia, 25-26 novembre 2021*, Padova, CEDAM, 2022, 513 ss.;

Stanzione, P., *Decisioni automatizzate e ruolo della privacy*, in Salanitro, U. (a cura di), *SMART la persona e l'infosfera*, Pisa, Pacini, 2022, 99 ss.;

Stazi, A., *Data Circulation and Legal Safeguards: a European Perspective*, in *Comparative Law Review*, 2019, 89 ss.;

Steeves, V., e Mačėnaitė, M., *Data protection and children's online privacy*, in González Fuster, G., Van Brakel, R., e De Hert, P. (a cura di), *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics*, Cheltenham, Elgar, 2022, 358 ss.;

Stefanelli, S., *Trattamento di dati personali per scopi di ricerca scientifica*, in Cassano, G., *et al.* (a cura di), *Il processo di adegua- mento al GDPR. Aggiornato al D.lgs. 10 agosto 2018, n. 101*, Milano, Giuffrè, 2018, 319 ss.;

Stefanelli, S., in Sciaudone, R., e Caravà, E. (a cura di), *Il codice della privacy. Commento al D.Lgs. 30 giugno 2003, n. 196 e al D.Lgs. 10 agosto 2018, n. 101 alla luce del Regolamento (UE) 2016/679 (GDPR)*, Pisa, Pacini, 2019, *sub* art. 92, 328 ss.;

Stefanini, E., *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Padova, CEDAM, 2008;

Tacconi, C., *La disciplina della* privacy *e la tutela del lavoratore*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 479 ss.;

Taddei Elmi, G., e Contaldo, A. (a cura di), *Intelligenza artificiale. Algoritmi giuridici. Ius condendum o "fantadiritto"?*, Pisa, Pacini, 2020;

Tampieri, M., *Il diritto all'oblio e la tutela dei dati personali*, in *Resp. civ. e prev.*, 2017, 1010 ss.;

Tampieri, M., *L'intelligenza artificiale: una nuova sfida anche per le automobili*, in *Contr. e impr*., 2020, 732 ss.;

Tassone, B. (a cura di), *L'impatto del DSA sull'ordinamento italiano (Speciale ragionato)*, in *Diritto di Internet*, 2023, 3 ss.;

Tavella, G., *Dal diritto come testo al diritto come* code*: considerazioni e prospettive di indagine*, in Camardi, C. (a cura di), *La via europea per l'intelligenza artificiale. Atti del convegno del progetto dottorale di alta formazione in scienze giuridiche, Ca' Foscari Venezia, 25-26 novembre 2021*, Padova, CEDAM, 2022, 497 ss.;

Terrasi, A., *Il rapporto tra diritto alla* privacy *e protezione dei dati personali tra Corte di Giustizia dell'Unione europea e Corte europea dei diritti dell'uomo*, in Distefano, M. (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Napoli, Editoriale Scientifica, 2017, 127 ss.;

Terzis, P., *Compromises and Asymmetries in the European Health Data Space*, in *European Journal of Health Law*, in *brill.com*, 27 ottobre 2022;

Terzis, P., e Santamaria Echeverria, (E.) OE., *Interoperability and governance in the European Health Data Space regulation*, in*Medical Law International*, in *journals.sagepub*.com, 24 aprile 2023; Tesauro, G., *Diritto dell'Unione europea*, 7a ed., Padova, CEDAM, 2012;
Tescaro, M., *La prevenzione del contagio come esimente dalla responsabilità per violazione della privacy del malato di HIV*, in *La resp. civ*., 2005, 1015 ss.;

Tessaro, T., *Rapporto tra accesso e* privacy *nella Pubblica Amministrazione: problemi giuridici e applicativi*, in Ferrari, G.F. (a cura di), *La legge sulla privacy dieci anni dopo*, Milano, EGEA, 2008, 147 ss.;

Thakkar, V., e Gordon, K., *Privacy and Policy Implications for Big Data and Health Information Technology for Patients: A Histor- ical and Legal Analysis*, in Lau, F., *et al*. (a cura di), *Improving Usability, Safety and Patient Outcomes with Health Infor- mation Technology*, 2019, 413 ss.;

Thiene, A., in De Cristofaro, G., e Zaccaria, A. (a cura di), *Commentario breve al diritto dei consumatori. (Codice del consumo e legislazione complementare)*, 2a ed., Padova, CEDAM, 2013, *sub* artt. 114 ss., d.lgs. n. 206 del 2005, 735 ss.;

Thiene, A., *La tutela della personalità dal* neminem laedere *al* suum cuique tribuere, in *Riv. dir. civ*., 2014, 351 ss.; Thiene,

A., *Salute, riserbo e rimedio risarcitorio*, in *Riv. it. med. leg.*, 2015, 1407 ss.;

Thiene, A., *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo*, in *Nuove leggi civ. comm.*, 2017, 410 ss.;

Thiene, A., *I diritti della personalità dei minori nello spazio virtuale*, in Thiene, A., e Marescotti, E. (a cura di), *La scuola al tempo dei social network*, numero monografico degli *Annali online della Didattica e della Formazione Docente*, 2017, 26.;

Thiene, A., *I diritti morali d'autore*, in *Riv. dir. civ*., 2018, 1522 ss.;
Thiene, A., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 9, reg. Ue n. 679/2016, *I. Profili generali*, 240 ss.;

Thiene, A., e Corso, S. (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza*, Napoli, Jovene, 2023;

Thiene, A., e Corso, S., *Premessa*, in Thiene, A., e Corso, S. (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza*, Napoli, Jovene, 2023, IX s.;

Trapani, M., *GDPR e Intelligenza Artificiale: i primi passi tra* governance, *privacy, trasparenza e* accountability, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 319 ss.;

Tresca, M., *Lo «Stato digitale»*. Big data, open data *e algoritmi: i dati al servizio della pubblica amministrazione*, in *Riv. trim. dir. pubbl*., 2021, 545 ss.;

Trezza, R., *Diritto e intelligenza artificiale. Etica* - Privacy - *Responsabilità* - *Decisione*, Pacini, Pisa, 2020; Trezza, R.,

Preliminary profiles on the civil liability of health robots, in *Iura and legal systems*, VIII.2021/3;

Trezza, R., *La tutela della persona umana nell'era dell'intelligenza artificiale: rilievi critici*, in *Federalismi*, n. 16, 2022, 277 ss., in
www.federalismi.it, 15 giugno 2022;

Trimarchi, P., *Rischio e responsabilità oggettiva*, Milano, Giuffrè, 1961;

Trimarchi, P., voce «Illecito (diritto privato)», in *Enc. del dir*., XX, Milano, Giuffrè, 1970, 90 ss.;

Troiano, S., *Il diritto alla portabilità dei dati personali*, in Zorzi Galgano, N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, CEDAM, 2019, 195 ss.;

Trolli, F., *La successione* mortis causa *nei dati personali del defunto e i limiti al loro trattamento*, in *Jus civile*, 2019, 313

ss.; Trolli, F., *La destinazione* post *mortale dei dati raccolti dal titolare del trattamento*, in *Ricerche giuridiche*, 2019, 95

ss.; Trolli, F., *Note sulla efficacia retroattiva della L. n. 219/2017*, in *Fam. e dir*., 2021, 435 ss.;

Tuccari, E., *I diritti dell'interessato*, in Magri, G., Martinelli, S., e Thobani, S. (a cura di), *Manuale di diritto privato delle nuove tecnologie*, Torino, Giappichelli, 2022, 151 ss.;

Tuccillo, R., in Barba, A., e Pagliantini, S. (a cura di), *Delle persone. Leggi collegate*, II, nel *Commentario del Codice civile*, diretto da Enrico Gabrielli, Torino, Utet, 2019, *sub* art. 9, reg. Ue n. 679/2016, 152 ss.;

Turco, V., *Il trattamento dei dati personali nell'ambito del rapporto di lavoro*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di),
I dati personali nel diritto europeo, Torino, Giappichelli, 2019, 517 ss.;

Turk, M., *Electronic Health Records: How to Suture the Gap Between Privacy and Efficient Delivery of Healthcare*, in *Brooklyn Law review*, vol. 80, n. 3, 2015, 565 ss.;

Turri, G., *Fragilità delle persone e incapacità genitoriale*, in *Minorigiustizia*, 2007, fasc. 3, 7 ss.;

Tuzzolino, D., *La portabilità dei dati sanitari*, in Thiene, A., e Corso, S. (a cura di), *La protezione dei dati sanitari. Privacy e inno- vazione tecnologica tra salute pubblica e riservatezza*, Napoli, Jovene, 2023, 59 ss.;

Twigg-Flesner, C., *Disruptive Technology – Disrupted Law? How the Digital Revolution Affects (Contract) Law*, in De Franceschi,
A. (a cura di), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*, Cambridge, Intersentia, 2016, 21 ss.;

Tzanou, M. (a cura di), *Health Data Privacy under the GDPR. Big Data Challenges and Regulatory Responses*, Londra, Routledge, 2021;

Ubertazzi, T.M., *Il diritto alla* privacy. *Natura e funzioni giuridiche*, Padova, CEDAM, 2004;

Ubertazzi, T.M., *Functional evolution of the right to privacy*, in *Comparazione e diritto civile*, 2021, 857 ss.;

Ubertazzi, T.M., *Ripensando alla revoca del consenso nella prospettiva funzionale della* privacy, in *Contr. e impr*., 2022, 27 ss.;

Uda, G.M., *Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*, in Cuffaro, V., D'Orazio, R., e Ricciuto, V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 557 ss.;

Ulissi, L., *I profili di responsabilità della macchina dell'apprendimento nell'interazione con l'utente*, in Alpa, G. (a cura di), *Diritto e intelligenza artificiale*, Pisa, Pacini, 2020, 435 ss.;

Vantin, S., *Alcune osservazioni su normatività e concetto di diritto tra intelligenza artificiale e algoritmizzazione del mondo*, in Giolo,O. (a cura di), *L'algoritmo alla prova del caso concreto: stereotipi, serializzazione, discriminazione*, in *GenIUS*, 2022, fasc. 1, 45 ss.;

Varani, E., *Il diritto di accesso ai documenti amministrativi contenenti dati sanitari*, in *Foro amm. - TAR*, 2005, 929 ss.;

Venchiarutti, A., *CoViD-19 e diritto alla riservatezza del paziente*, in *Nuova giur. civ. comm*., 2020, suppl., 40 ss.;

Venditti, C., *Questioni di biodiritto connesse al superamento dei naturali limiti umani*, in Catalano, R., e Venditti, C., *Questioni di biodiritto nella filmografia cyberpunk*, Napoli, Editoriale scientifica, 2017, 29 ss.;

Venuti, M.C., *Gli atti di disposizione del corpo*, Milano, Giuffrè, 2002;

Vercellone, P., voce «Personalità (diritti della)», in *Noviss. Digesto it*., XII, Torino, Utet, 1965, 1083 ss.;

Verdolini, E., *Regolare l'economia digitale. Intervista a Giusella Finocchiaro*, in *Pandora Rivista*, 2021, fasc. 3 *Tempi della tecnica*, 46 ss.;

Verhenneman, G., *et al*., *How GDPR Enhances Transparency and Fosters Pseudonymisation in Academic Medical Research*, in
European Journal of Health Law, vol. 27, n. 1, 2020, 35 ss.;

Vernaglione, P., *Il libertarismo: la teoria, gli autori, le politiche*, Soveria Mannelli, Rubbettino, 2003;

Veronesi, P., *Il corpo e la Costituzione. Concretezza dei "casi" e astrattezza della norma*, Milano, Giuffrè, 2007;

Veronesi, P., *Il "caso Dobbs": originalismo "estremo" e crisi del costituzionalismo negli States*, in *BioLaw Journal - Rivista di BioDiritto, Special issue* 1, 2023, 105 ss.;

Versaci, G., *Personal data and Contract law: challenges and concerns about the economic exploitation of the right to data protection*, in *European Review of contract law*, vol. 14, n. 4, 2018, 374 ss.;

Versaci, G., *La contrattualizzazione dei dati personali dei consumatori*, Napoli, Edizioni Scientifiche Italiane, 2020;

Versaci, G., *Consenso al trattamento dei dati personali e* dark patterns *tra opzionalità e condizionalità*, in *Nuove leggi civ. comm.*, 2022, 1130 ss.;

Versaci, G., *Consenso al trattamento dei dati personali e* dark patterns *tra opzionalità e condizionalità*, in D'Auria, M. (a cura di), *I*
problemi dell'informazione nel diritto civile, oggi. Studi in onore di Vincenzo Cuffaro, Roma Tre-press, 2022, 455 ss.;

Vessia, F., *Big data: dai vantaggi competitivi alle pratiche abusive*, in *Giur. comm.*, 2018, 1064 ss.;

Vettori, G., *Privacy: un primo bilancio*, in *Riv. dir. priv*., 1998, 673 ss.;

Vicarelli, G., e Bronzini, M., *La sanità digitale: dimensioni di analisi e prospettive di ricerca*, in *Politiche sociali*, 2018;

Viciani, S., *Strategie contrattuali del consenso al trattamento dei dati personali*, in *Riv. crit. dir. priv*., 1999, 159 ss.;

Viciani, S., *Sicurezza e privacy nella "prescrizione elettronica"*, in *www.giustiziacivile.com*, 28 giugno 2016; Vigevani,

G.E., *Piattaforme digitali private, potere pubblico e libertà di espressione*, in *Dir. cost*., 2023, fasc. 1, 41 ss.;

Viglianisi Ferraro, A., *Danno da illegittimo trattamento dei dati personali, tra "inasprimento sanzionatorio" europeo ed "interpre- tazioni restrittive" della giurisprudenza italiana*, in *Riv. dir. priv*., 2020, 85 ss.;

Vigorito, A., *La "patrimonializzazione" dei dati personali a partire della recente controversia AGCM-Facebook*, in *www.giustizia-civile.com*, 20 aprile 2020;

Vilasau Solana, M., *El RGPD: entre la tutela del interesado y la saturación informativa*, in Mantelero, A., e Poletti, D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, 2018, 115 ss.;

Villani, L., *Biobanche e test rivelatori di informazioni genetiche: spunti di riflessione per un nuovo consenso informato*, in *La resp. civ*., 2010, 140 ss

Zanichelli, M., *La persona nell'orizzonte giuridico contemporaneo*, in Zanichelli, M. (a cura di), *La persona come categoria bioetica. Prospettive umanistiche*, Milano, FrancoAngeli, 2019, 181 ss.;

Zanichelli, M., *L'intelligenza artificiale e la persona: tra dilemmi etici e necessità di regolazione giuridica*, in *Teoria e critica della regolazione sociale*, 2021, fasc. 2, 141 ss.;

Zanovello, F., *Anonimato materno e diritto dell'adottato a conoscere le proprie origini: la parola al legislatore*, in *Studium iuris*, 2019, 1183 ss.;

Zanovello, F., *Emergenza epidemiologica da COVID-19 e modalità di consegna della ricetta medica: il parere del Garante Privacy*, in *www.rivistaresponsabilitamedica.it*, 6 aprile 2020;

Zanovello, F., Contact *tracing ed emergenza sanitaria: una sfida difficile*, in *Resp. med*., 2020, 291 ss.;

Zanovello, F., in D'Orazio, R., Finocchiaro, G., Pollicino, O., e Resta, G. (a cura di), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, *sub* art. 2 *septies*, d.lgs. n. 196 del 2003, 1051 ss.;

Zanovello, F., *Misure di garanzia e rischio di* data breach *in ambito sanitario*, in Thiene, A., e Corso, S. (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza*, Napoli, Jovene, 2023, 129

Zatti, P., *Dal consenso alla regola: il giurista in bioetica*, in *Riv. crit. dir priv*., 1994, 523 ss.;

Zatti, P., *Lo specchio giuridico*, in Pierri, M. (a cura di), *Genitori e Figli nel Tempo. Per un disegno guida nella psicoterapia della psicosi*, Bologna, Patron, 1999, 22 ss.;

Zatti, P., *Il diritto a scegliere la propria salute (in margine al caso S. Raffaele)*, in *Nuova giur. civ. comm*., 2000, II, 1 ss.;

Zatti, P., *Note sulla semantica della dignità*, in Zatti, P. (a cura di), *Maschere del diritto volti della vita*, Milano, Giuffrè, 2009;

Zatti, P.., *Principi e forme del "governo del corpo"*, in Canestrari, S., Ferrando, G., Mazzoni, C.M., Rodotà, S., e Zatti, P. (a cura di), *Il governo del corpo*, nel *Trattato di biodiritto* diretto da Rodotà e Zatti, t. I, Milano, Giuffrè, 2011, 99 ss.;

Zatti, P., *Il corpo e la nebulosa dell'appartenenza: dalla sovranità alla proprietà*, in C.M. Mazzoni (a cura di), *Per uno statuto del corpo*, Milano, Giuffrè, 2008, 69 ss.;

Zatti, P., *La via (crucis) verso un diritto della relazione di cura*, in *Riv. crit. dir. priv*., 2018, 3 ss.;

Zatti, P., *Spunti per una lettura della legge sul consenso informato e DAT*, in *Nuova giur. civ. comm.*, 2018, I, 247 ss.;

Zatti, P., *Spunti per una lettura della legge sul consenso informato e DAT*, in *www.rivistaresponsabilitamedica.it*, 31 gennaio 2018;

Zatti, P., *Brevi note sull'interpretazione della legge n. 219 del 2017*, in *Nuove leggi civ. comm*., 2019;

Zatti, P., *L'*intendance suivra*...?*, in *Nuova giur. civ. comm*., 2021, II, 182 ss.;

Zatti, P., *La questione dell'aiuto medico a morire nella sentenza della Corte costituzionale: il "ritorno al futuro" della l. 219/2017*, in *Resp. med*., 2022, 155 ss.;

Zeno-Zencovich, V., *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium iuris*, 1997, 467 ss.;

Zeno-Zencovich, V., voce «Cosa», nel *Digesto IV ed*., *Disc. priv*., *sez. civ*., III, Torino, Utet, 1998, 438 ss.;

Zeno-Zencovich, V., *Sull'informazione come "bene" (e sul metodo del dibattito giuridico)*, in *Riv. crit. dir. priv*., 1999, 485.;

Zeno-Zencovich, V., *Ragioni ed obiettivi del codice*, in Cardarelli, F., Sica, S., e Zeno-Zencovich, V. (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, Giuffrè, 2004, 1 ss.;

Zeno-Zencovich, V., *Dieci anni di legislazione sui dati personali: tentativo di un bilancio*, in Ferrari,G.F. (a cura di), *La legge sulla privacy dieci anni dopo*, Milano, EGEA, 2008, 35 ss.;

Zeno-Zencovich, V., *La "comunione" dei dati personali. Un contributo al sistema dei diritti della personalità*, in *Dir. inf*., 2009, 5 ss.;

Zeno-Zencovich, V., *I diritti della personalità*, in *Diritto civile*, diretto da Lipari, N., e Rescigno, P., Milano, Giuffrè, 2009, I, 495 ss.;