



MARIA SAMANTHA ESPOSITO

Assegnista di ricerca in Diritto privato – Politecnico di Torino

TUTELA DEI DATI PERSONALI E RICERCA SCIENTIFICA IN AMBITO SANITARIO: IL GDPR E IL REGOLAMENTO SULLO SPAZIO EUROPEO DEI DATI SANITARI (EHDS)

SOMMARIO: 1. L'oggetto di indagine. – 2. L'impatto delle innovazioni tecnologico-informatiche sulla ricerca scientifica e sulla protezione dei dati personali. – 3. Il GDPR e il trattamento dei dati nella ricerca scientifica in ambito sanitario: le basi giuridiche. – 3.1. Il trattamento ulteriore per scopi di ricerca scientifica: opportunità e limiti. – 3.2. Le deroghe ai diritti degli interessati e le garanzie adeguate per il trattamento dei dati a fini di ricerca scientifica. – 3.3. L'uniformazione parziale e le sue implicazioni per la ricerca scientifica. – 4. Il Regolamento sullo Spazio Europeo dei Dati Sanitari e l'uso secondario dei dati sanitari elettronici. – 4.1. Il ruolo degli interessati nell'uso secondario dei dati sanitari. – 5. Brevi osservazioni conclusive.

1. – Negli ultimi anni, l'impatto delle nuove tecnologie informatiche sulla tutela del diritto alla salute è divenuto sempre più evidente¹, offrendo strumenti preziosi per lo sviluppo di terapie, farmaci e dispositivi medici, nonché soluzioni per migliorare l'erogazione delle prestazioni sanitarie e la gestione delle informazioni². Anche la ricerca scientifica³ in campo medico, fondamentale per il progresso della scienza⁴, è stata, e continua a essere, profondamente influenzata dalla rapida evoluzione tecnologica. L'uso di strumenti avanzati per la raccolta, l'analisi e la condivisione dei dati ha, infatti, notevolmente potenziato le tecniche diagnostiche e

¹ La diffusione di questi strumenti e tecniche può essere riassunta nel fenomeno dell'e-Health. L'espressione "sanità digitale", nella sua accezione più ampia, si riferisce all'utilizzo delle tecnologie dell'informazione e della comunicazione (ICT) a supporto della salute e dei settori correlati, come i servizi di assistenza sanitaria e la ricerca. Inoltre, emergono nuove aree, come l'uso di strumenti informatici avanzati nella genomica e l'intelligenza artificiale applicata alle pratiche mediche e sanitarie (cfr. ORGANIZZAZIONE MONDIALE DELLA SANITÀ (OMS), *Risoluzione WHA58.28*, in *Fifty-Eighth World Health Assembly Geneva*, 16-25 maggio 2005, disponibile all'indirizzo <https://apps.who.int>).

² Ciò consente, dunque, di attuare il diritto alla salute nella sua più ampia accezione da ultimo accolta, che supera il tradizionale focus sul solo aspetto fisico-funzionale per includere la piena realizzazione della persona e dei suoi bisogni psico-fisici (v. anche il Preambolo della Costituzione dell'Organizzazione Mondiale della Sanità (OMS) del 1948). Il diritto alla salute, inteso come fattispecie «complessa», è infatti un concetto relativamente recente, arricchitosi nel corso del tempo grazie all'influenza di diversi fattori storici, politici e sociali. Si rinvia per un approfondimento, tra gli altri, a D. MORANA, *La salute come diritto costituzionale. Lezioni*, 4^o ed., Giappichelli, Torino, 2021, 1; ID., *La salute nella costituzione italiana. Profili sistemati*, Giuffrè, Milano, 2002, 1; M. LUCIANI, voce *Salute, 1) Diritto alla salute – dir. cost.*, in *Enc. giur.*, XXVII, Treccani, Roma, 1991, 5.

³ Il diritto alla scienza e al progresso scientifico, in quanto diritto umano, è stato espressamente riconosciuto dall'ONU, con conseguente dovere degli Stati di implementare adeguati strumenti di attuazione e tutela: cfr. UNITED NATIONS-COMMITTEE ON ECONOMIC, SOCIAL AND CULTURAL RIGHTS, *General comment No. 25 (2020) on science and economic, social and cultural rights (article 15 (1) (b), (2), (3) and (4) of the International Covenant on Economic, Social and Cultural Rights*, in UN Doc. E/C.12/GC/25, del 30 aprile 2020. In argomento, v., tra gli altri, G. PERRONE, *Scienza e diritti economici, sociali e culturali: Il Commento generale n. 25 del Comitato dei diritti economici, sociali e culturali*, in *Dir. um. dir. int.*, 2020, 3, 786 ss. V. anche l'art. 27 della Dichiarazione universale dei diritti umani (UDHR).

⁴ Cfr. P. GUARDA, *Il regime giuridico dei dati della ricerca scientifica*, ES, Napoli, 2021, 39.



sperimentali⁵, assumendo un ruolo centrale nella tutela della salute⁶ e contribuendo all'innalzamento della qualità e dell'efficacia delle prestazioni offerte⁷.

Questi aspetti richiedono un'attenta considerazione nella valutazione della legittimità delle innovazioni tecniche e tecnologiche in campo medico, soprattutto in relazione ad altri diritti meritevoli di pari tutela, che potrebbero subire un pregiudizio. Sebbene i benefici apportati da questi sviluppi alla salute individuale e collettiva siano innegabili, non si possono infatti trascurare i numerosi rischi che tale progresso comporta. Tra questi, l'attività di ricerca basata su un uso intensivo di dati può compromettere il diritto alla riservatezza e alla protezione dei dati personali, specialmente a causa della particolare sensibilità delle informazioni sanitarie⁸, mettendo in discussione l'efficacia dei tradizionali strumenti di tutela, rappresentati, in primo luogo, dal binomio "consenso e anonimizzazione".

L'impiego di tali tecnologie richiede, dunque, una rinnovata riflessione⁹ sulle soluzioni normative necessarie per garantire un adeguato bilanciamento tra l'esigenza di promuovere la ricerca medica, orientata al miglioramento della salute, anche collettiva, e la tutela degli interessi dei partecipanti agli studi.

In questa prospettiva, il presente contributo si propone di indagare, in primo luogo, l'impatto dei progressi tecnologici e informatici sulla tutela della riservatezza e dei dati personali nel contesto della ricerca scientifica in campo medico, con particolare riferimento alle criticità emerse dallo sviluppo della ricerca genomica e dall'uso dei Big Data. Successivamente, verranno approfonditi gli strumenti introdotti dal Regolamento Generale sulla Protezione dei Dati (GDPR) e dal Regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS) per rispondere alle sfide emergenti e garantire un corretto bilanciamento tra l'interesse al progresso scientifico in ambito sanitario e la tutela della riservatezza e dell'autodeterminazione informativa dei partecipanti.

Infine, saranno formulate alcune riflessioni conclusive sull'efficacia e sull'adeguatezza degli strumenti normativi proposti, valutandone la capacità di rispondere alle esigenze poste dalla ricerca scientifica contemporanea, mantenendo al contempo un equilibrio tra innovazione e salvaguardia degli interessi individuali.

2. – La ricerca scientifica, in particolare in ambito medico, rappresenta da sempre un settore in cui interessi individuali e collettivi si intrecciano e, talvolta, si contrappongono, rendendo necessario un costante bilanciamento. Questo equilibrio, inoltre, non è statico, ma richiede continui adattamenti in risposta ai cam-

⁵ In questa prospettiva, la libertà di ricerca scientifica non rappresenta, dunque, solo un interesse autonomo da tutelare, ma assume un ruolo determinante in quanto strumentale al raggiungimento di un elevato livello di salute, sia individuale che collettiva.

⁶ V. anche COMMISSIONE EUROPEA, *Piano d'azione "Sanità elettronica" 2012-2020 – Una sanità innovativa per il 21esimo secolo*, COM(2012) 736 final, 6 dicembre 2012, 4.

⁷ Il progresso tecnico e tecnologico rientra, dunque, tra le finalità proprie delle istituzioni, non solo in virtù del dovere di promuovere il diritto alla scienza e al progresso scientifico. Se, infatti, la salute non si riduce più alla semplice assenza di malattia, la sua tutela non può limitarsi all'erogazione di trattamenti finalizzati al superamento dello stato patologico o al mantenimento di un buono stato di salute fisica, ma deve necessariamente ampliarsi, includendo, ad esempio, interventi sanitari di carattere preventivo, nonché cure palliative e terapie del dolore. Con riferimento all'ordinamento italiano, cfr. artt. 9, comma 1, 32 e 33 Cost. In argomento, v., tra gli altri, D. MORANA, *Diritto alla salute, ricerca tecnico-scientifica e innovazioni tecnologiche*, in G. FERRI (a cura di), *Diritto costituzionale e nuove tecnologie*, Esi, Napoli, 2022, 324; L. MARILOTTI, *I dati genetici tra dimensione individuale e collettiva*, in *BioLaw Journal*, 2021, 1, 167; M.C. SPENA, *La salute tra nuove sfide della contemporaneità. Digitalizzazione, privacy e modelli di governance*, ES, Napoli, 2023, 24.

⁸ I dati sanitari sono stati infatti definiti come il "nocciolo (o nucleo) duro" della *privacy*, in quanto riguardano la sfera più intima della persona (cfr., tra gli altri, D. POLETTI, sub *Art. 23 (dati inerenti alla salute)*, in C.M. BIANCA-F.D. BUSNELLI, et al. (a cura di), *Tutela della privacy. Commentario alla legge 675/96*, in *Nuove leggi civ. comm.*, 1999, 2-3, 561, nt. 4.

⁹ V. anche M.C. SPENA, *La salute*, cit., 95, la quale evidenzia l'esigenza di una nuova «contestualizzazione» dei diritti fondamentali derivante dalla rivoluzione digitale. In generale, sulla necessità di ridefinire il bilanciamento tra diritti fondamentali alla luce dei mutamenti socio-economici e delle contingenze attuali, v. Corte Cost. 9 maggio 2013, n. 85, in *One Legale*.



biamenti sociali, tecnologici e scientifici. Anche la disciplina della tutela della riservatezza e dei dati personali dei partecipanti agli studi è interessata da questo dinamismo¹⁰, la quale è divenuta sempre più rilevante a fronte della centralità assunta dalle informazioni nella ricerca medica, sostituendo i “corpi materiali” come principale strumento di indagine¹¹.

In questo contesto, la tradizionale efficacia del consenso informato, quale strumento di garanzia per l’autodeterminazione informativa¹² dei partecipanti alla ricerca¹³, unitamente all’adeguatezza delle consoli-

¹⁰ La stessa nozione di “privacy” ha subito un profondo mutamento nel tempo, a causa dell’avanzare delle tecnologie informatiche, testimoniando così il “dinamismo” dei diritti fondamentali, capaci di rinnovarsi ed espandersi insieme a una realtà in continuo cambiamento (v. anche quanto osservato da S. RODOTÀ, *I nuovi diritti che hanno cambiato il mondo*. Stralcio dell’intervento alle “Lezioni Norberto Bobbio” – Torino 25/10/2004, disponibile sul sito *Privacy.it*; E. BRUGIOTTI, *La privacy attraverso le “generazioni dei diritti”*. *Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico*, in *www.dirittifondamentali.it*, 2013, 2, 1). In ritardo rispetto alle diverse esperienze straniere, nel nostro ordinamento la *privacy* è stata inizialmente riconosciuta come diritto alla riservatezza, ossia come divieto di ingerenza esterna nella sfera privata, in risposta alla crescente diffusione della stampa periodica e dei nuovi *media*. Con lo sviluppo delle tecnologie informatiche e dei metodi di rilevamento e trasferimento dei dati, è emersa una nuova dimensione della *privacy*, incentrata più sul controllo delle informazioni personali per prevenire abusi che sulla loro mera segretezza (v. anche S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Il Mulino, 1973, 130). Il progresso tecnologico ha quindi ridefinito il diritto alla *privacy*: accanto alla concezione negativa, volta a impedire che le informazioni private diventino di dominio pubblico, si è affermata una dimensione positiva, che include il diritto di conoscere e controllare le informazioni relative alla propria persona (cfr. A. MANTELE-RO, *Privacy*, in *Contr. impr.*, 2008, 3, 757 ss. In argomento, v. anche, tra gli altri, S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006).

¹¹ La regolamentazione della ricerca scientifica in ambito medico è stata inizialmente pensata per contrastare pratiche sperimentali gravemente lesive dei diritti fondamentali dell’essere umano. Le atrocità perpetrate durante la Seconda Guerra Mondiale portarono all’elaborazione del Codice di Norimberga nel 1947 (cfr. Nuremberg Code, 1947), un insieme di principi etici che ha posto le basi per la sperimentazione umana, sottolineando l’importanza del consenso volontario e informato e la necessità di rigorosi controlli per salvaguardare l’integrità e la dignità dei partecipanti. Il Codice di Norimberga, riconosciuto come documento fondamentale dell’etica medica, ha influenzato l’elaborazione di strumenti normativi successivi, che hanno esteso la loro portata dalla sperimentazione alla ricerca medica in generale. Tra questi, la Dichiarazione di Helsinki, adottata per la prima volta nel 1964 (WORLD MEDICAL ASSOCIATION, *Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects*, Adopted by the 18th WMA General Assembly, Helsinki, Finland, June 1964), ha rafforzato il concetto di consenso informato per la partecipazione alla ricerca e la protezione della dignità umana, includendo la salvaguardia della riservatezza dei dati personali dei soggetti coinvolti. Un altro esempio significativo è la Convenzione di Oviedo (COUNCIL OF EUROPE, *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, 1997), un trattato internazionale del Consiglio d’Europa che ha ampliato la protezione dei diritti umani nelle applicazioni biomediche, inserendola in un quadro giuridico internazionale. Il documento, oltre a ribadire l’essenzialità del consenso per gli interventi e la partecipazione alla ricerca scientifica nel campo della salute, sottolinea l’importanza di garantire il rispetto della vita privata nel trattamento delle informazioni relative ai pazienti e ai partecipanti agli studi. Con il progredire della scienza e della tecnologia, l’attenzione etica e normativa in ambito medico si è, dunque, progressivamente ampliata per affrontare le nuove sfide poste dalla ricerca scientifica. A partire dagli anni ’70, l’accelerazione nello sviluppo delle tecnologie informatiche ha, infatti, profondamente trasformato i processi di raccolta, archiviazione e analisi dei dati personali, con un impatto significativo anche nel campo della ricerca. In questo contesto, le normative introdotte per garantire il controllo e la riservatezza delle informazioni personali hanno inciso anche sulla regolamentazione etica della ricerca, estendendo la tutela dalla sola sfera fisica dei partecipanti a quella delle loro informazioni. Il rapporto tra ricercatori e partecipanti, inizialmente incentrato sulla protezione fisica, ha pertanto gradualmente incluso il dovere di salvaguardare la riservatezza e l’integrità dei dati raccolti. Successivamente, anche strumenti quali il consenso informato al trattamento dei dati personali e l’anonimizzazione sono divenuti fondamentali per assicurare ai partecipanti il controllo sulle proprie informazioni. In tale quadro, il consenso informato, originariamente concepito per tutelare l’autodeterminazione fisica dei partecipanti, si è evoluto fino a diventare uno strumento volto a garantire anche la loro autodeterminazione nella gestione dei dati, riflettendo così la crescente rilevanza della componente informativa.

¹² Sul diritto all’autodeterminazione informativa merita di essere ricordata l’importante decisione della Corte costituzionale tedesca: Bundesverfassungsgericht, 15 dicembre 1983, in *Entscheidungen des Bundesverfassungsgerichts*, 1984, 65, 1 ss. In dottrina v., tra gli altri, G. SARTOR, *Tutela della personalità e normativa per la «protezione dei dati»*. *La sentenza della Corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del «Datenschutz»*, in *Inf. dir.*, 1986, 3, 95 ss.; E. FIALOVA, *Data Portability and Informational Self-Determination*, in *Masaryk University Journal of Law and Technology*, 8, 2014, 47 ss. V. anche F. BIGNAMI-G. RESTA, *Transatlantic Privacy Regulation: Conflict and Cooperation*, in *Law and Contemporary Problems*, 2015, 78, 232.

¹³ Sulla distinzione tra autodeterminazione “informativa” e autodeterminazione “corporea”, si v. sopra nt. 11.



date misure di tutela della riservatezza¹⁴ hanno progressivamente rivelato i propri limiti con lo sviluppo della ricerca genomica, risultando sempre meno adeguate con l'avvento dei Big Data e delle tecnologie avanzate per la loro analisi¹⁵.

Il Progetto Genoma Umano¹⁶, finalizzato a mappare e sequenziare l'intero genoma, ha aperto nuove prospettive nel campo medico e biotecnologico, sollevando al contempo complesse questioni etiche e giuridiche. In particolare, la gestione dei dati genetici presenta notevoli criticità a causa del carattere mutevole della ricerca in questo settore, rendendo difficile ottenere un consenso effettivamente informato e specifico dai partecipanti. A ciò si aggiungono i progressi tecnologici, che oggi consentono la raccolta, l'analisi e la conservazione di grandi quantità di dati genetici, richiedendo nuove riflessioni in merito alla protezione dei dati personali e alla riservatezza degli interessati¹⁷. Questi dati, infatti, per loro natura, non possono essere completamente anonimizzati, rivelando informazioni particolarmente sensibili, come la predisposizione a determinate patologie, che riguardano non solo i soggetti direttamente coinvolti, ma anche i loro familiari¹⁸. Un altro aspetto rilevante riguarda la stabilità della sequenza del DNA¹⁹, che ne rende difficile la modifica al fine di mitigare eventuali rischi futuri, come quelli legati alla discriminazione in ambito lavorativo, assicurativo e sociale, sottolineando la necessità di garantire una protezione rigorosa di queste informazioni²⁰.

Le biobanche di popolazione accentuano queste problematiche. Raccogliendo su vasta scala campioni biologici e informazioni dettagliate sulla storia medica e genealogica dei partecipanti, queste strutture costituiscono risorse preziose per la ricerca, ma anche sistemi altamente sensibili sotto il profilo della protezione dei dati personali, soprattutto per quanto riguarda la sicurezza e l'incertezza legata agli utilizzi futuri²¹.

L'introduzione dei Big Data nella ricerca scientifica ha ulteriormente complicato le sfide legate al modello tradizionale di tutela dei dati personali. La possibilità di raccogliere e analizzare grandi quantità di dati provenienti da fonti eterogenee, quali cartelle cliniche elettroniche, applicazioni per il benessere e dispositivi indossabili, ha trasformato i metodi di ricerca, superando o integrando l'approccio statistico tradizionale basato su campioni limitati. L'impiego di algoritmi avanzati consente, infatti, di identificare schemi e correla-

¹⁴ Tra le quali l'anonimizzazione dei dati.

¹⁵ Sui limiti dei tradizionali strumenti di tutela derivanti dall'avvento dei Big Data e delle tecnologie di analisi avanzata, v., tra gli altri, M. MOSTERT-A.L. BREDENOORD-M.C. BIESAART, et al., *Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach*, in *European Journal of Human Genetics*, 2016, 7, 957 ss.

¹⁶ Sul Progetto Genoma Umano, avviato nel 1990 e completato nel 2003, v. NATIONAL HUMAN GENOME RESEARCH INSTITUTE (NHGRI), *The Human Genome Project*, disponibile all'indirizzo <https://www.genome.gov>.

¹⁷ In particolare, si è iniziato a parlare di "privacy genetica" per indicare lo specifico interesse che individui, famiglie e comunità hanno nei confronti delle informazioni genetiche. V., tra gli altri, B.M. KNOPPERS-M.J.S BEAUVAIS, *Three decades of genetic privacy: a metaphoric journey*, in *Human Molecular Genetics*, 2021, 20, 157. Le preoccupazioni relative alla riservatezza dei dati e ai limiti del consenso informato sono inoltre connesse al valore commerciale che ricerche e banche dati rappresentano per le aziende private, in particolare quelle farmaceutiche. In argomento v., tra gli altri, M. EVERETT, *The social life of genes: privacy, property and the new genetics*, in *Social Science & Medicine*, 2003, 56.

¹⁸ In argomento, v., tra gli altri, C. DONISI, *Gli enigmi della medicina predittiva*, in L. CHIEFFI (a cura di), *Il diritto alla salute alle soglie del terzo millennio. Profili di ordine etico, giuridico ed economico*, Giappichelli, Torino, 2003, 192.

¹⁹ La sequenza di DNA è considerata, in particolare, uno dei più importanti identificatori personali. Cfr., tra gli altri, AMERICAN SOCIETY OF HUMAN GENETICS, *ASHG Response to NIH on Genome-Wide Association Studies*, 2006, consultabile all'indirizzo <https://www.ashg.org>. In argomento v. anche, C. CASONATO-M. TOMASI, *Diritti e ricerca biomedica: una proposta verso nuove consuetudini*, in *BioLaw Journal*, 2019, 1, 348.

²⁰ V. anche ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document on Genetic Data (WP91)*, 17 marzo 2004 (tutti i documenti del Gruppo di lavoro art. 29 per la protezione dei dati citati nel presente contributo possono essere consultati all'indirizzo <https://ec.europa.eu>). In dottrina v., tra gli altri, M. EVERETT, *The social life*, cit., 55 ss.; J. MONDUCCI, *Il dato genetico tra autodefinizione informativa e discriminazione genotipica*, Bononia University Press, Bologna, 2013, 93 ss.

²¹ In argomento, tra gli altri, B.M. KNOPPERS e M. J. S. BEAUVAIS, *Three decades*, cit., 157 ss.



zioni prima sconosciuti, aprendo la strada a nuovi studi e ipotesi di ricerca²², ma riducendo al contempo la comprensione, da parte dei partecipanti, delle modalità e delle finalità del trattamento dei dati raccolti. Questi aspetti hanno sollevato interrogativi anche sul rispetto del principio di minimizzazione, che impone che i dati raccolti siano pertinenti e non eccedenti rispetto agli scopi prefissati. L'enorme volume di dati trattati accresce, inoltre, il rischio di re-identificazione, rendendo più complesso garantire un'effettiva anonimizzazione²³⁻²⁴.

In risposta a queste criticità, nel tempo sono emerse soluzioni mirate a bilanciare le esigenze della ricerca scientifica con la protezione dei diritti dei partecipanti. Una tendenza rilevante è stata il progressivo allontanamento dal tradizionale modello di consenso informato, basato su specificità e attualità per ogni singolo studio, verso approcci più flessibili. Un esempio significativo è il c.d. consenso ampio (*broad consent*), che consente l'impiego dei dati raccolti per una vasta gamma di ricerche future senza dover specificare ogni singolo utilizzo²⁵. Altri approcci rilevanti includono il c.d. consenso dinamico (*dynamic consent*), che permette ai partecipanti di aggiornare e gestire in modo continuo il proprio consenso adattandolo ai nuovi sviluppi della ricerca²⁶⁻²⁷, e il c.d. consenso presunto (*presumed consent*), che prevede l'inclusione automatica dei partecipanti nella ricerca o nella banca dati²⁸, con la possibilità di esprimere successivamente il proprio dissenso.

²² Si tratta, dunque, di un'inversione metodologica, in cui non si parte più da ipotesi predefinite, ma queste vengono generate direttamente dai dati, i quali possono anche non essere immediatamente correlati alla salute. Cfr. A. MANTELERO, *La privacy all'epoca dei Big Data*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019, 1187 e 1191; G. COMANDÉ, *Ricerca in sanità e data protection un puzzle...risolvibile*, in *Riv. it. med. leg.*, 2019, 1, 189.

²³ In argomento, tra gli altri, P. QUINN, *Research under the GDPR – a level playing field for public and private sector research?*, in *Life Sciences, Society and Policy*, 2021, 4, 3 s. e 17; N. PURTOVA, *The law of everything. Broad concept of personal data and future of EU data protection law*, in *Law, Innovation and Technology*, 2018, 10, 1, 40; S.R. PEPPET, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, in *Texas Law Review*, 2014, 85, 128 ss. In generale, si evidenzia la difficoltà di tracciare una netta linea di demarcazione tra dati personali e non personali, in particolare per i dati semplicemente anonimizzati, a causa della crescente quantità di dati a disposizione e del continuo sviluppo delle tecnologie di analisi. In questo senso, cfr. B. VAN DER SLOOT, *Regulating non-personal data in the age of Big Data*, in M. TZANOU (a cura di), *Health Data Privacy under the GDPR. Big Data Challenges and Regulatory Responses*, Routledge, 2021, 85 ss.

²⁴ Ulteriori criticità legate ai Big Data includono il rischio di perpetuare disuguaglianze sociali e discriminazioni. Questo rischio è particolarmente rilevante in ambito sanitario, dove le decisioni basate sui modelli predittivi dei Big Data possono replicare o addirittura aggravare le disuguaglianze nell'accesso alle cure e nel trattamento dei pazienti. In proposito, v. B.D. MITTELSTADT-L. FLORIDI, *The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts*, in *Science and Engineering Ethics*, 2016, 2, 322 s.

²⁵ Per questa soluzione v., tra gli altri, C. GRADY-L. ECKSTEIN-B. BERKMAN, et al., *Broad Consent for Research with Biological Samples: workshop conclusions*, in *The American Journal of Bioethics*, 2015, 9, 34 ss.; J.R. GULCHER-K. STEFANSSON, *The Icelandic Healthcare Database and Informed Consent*, in *New England Journal of Medicine*, 2000, 24, 1828; G. J. ANNAS, *Rules for Research on Human Genetic Variation: Lessons from Iceland*, ivi, 1832; K. STEINBEKK-B. KÅRE MYSKJA-B. SOLBERG, *Broad consent versus dynamic consent in biobank research: Is passive participation an ethical problem?*, in *European Journal of Human Genetics*, 2013, 897 ss. Tuttavia, non sono mancate critiche nei confronti di tale modello di consenso, soprattutto per quanto riguarda la trasparenza e la comprensione da parte dei partecipanti delle future applicazioni dei loro dati. In senso critico v., tra gli altri, T. PLOUG-S. HOLM, *Going beyond the false dichotomy of broad or specific consent: meta-perspective on participant choice in research using human tissue*, in *American Journal of Bioethics*, 2015, 9, 44 ss.; T. CAULFIELD-J. KAYE, *Broad consent in biobanking: Reflections on seemingly insurmountable dilemmas*, in *Medical Law International*, 2009, 2, 85 ss.

²⁶ V., tra gli altri, J. KAYE-E. WHITLEY-D. LUND, et al., *Dynamic consent: a patient interface for twenty-first century research networks*, in *European Journal of Human Genetics*, 2015, 141 ss.

²⁷ Un metodo alternativo elaborato è il c.d. meta-consent, che consente agli individui di definire in anticipo come gestire il proprio consenso per diversi tipi di ricerca o trattamenti dei dati. Al momento della raccolta, possono scegliere tra vari modelli di consenso (dinamico, ampio, generico o rifiuto) per diverse categorie di ricerca, individuate, tra l'altro, in base ai dati, agli strumenti utilizzati o al carattere generale o specifico della ricerca. Ad esempio, l'interessato può optare per un consenso ampio in un'area determinata e richiedere un consenso specifico per altre aree di studio più sensibili. Per tale soluzione v., tra gli altri, T. PLOUG-S. HOLM, *Going beyond*, cit., 46.

²⁸ In argomento, v., tra gli altri, S.Y.H. KIM, *Clinical Trials Without Consent?*, in *Perspectives in Biology and Medicine*, 2016, 1, 132 ss., il quale esclude l'ammissibilità del consenso presunto in modo generalizzato, ammettendo però che, in alcuni casi particolari e con rigorose limitazioni, esso potrebbe risultare eticamente accettabile.



Tuttavia, un eccessivo “allentamento” del requisito di specificità del consenso, associato alla crescente complessità della ricerca “post-genomica” e alla possibile asimmetria informativa tra i partecipanti e i ricercatori, rischia di trasformare il consenso in un mero atto formale, riducendo l’effettiva autodeterminazione degli interessati²⁹. Da ciò emerge l’esigenza di strumenti alternativi o complementari che possano offrire una tutela adeguata senza ostacolare il progresso scientifico³⁰.

Infine, sebbene l’anonimizzazione rappresenti una soluzione potenzialmente efficace nei confronti di molte di queste criticità, la sua applicazione deve confrontarsi non solo con le difficoltà legate alla natura dei dati trattati e all’uso dei Big Data, ma anche con le esigenze della ricerca, che spesso richiedono la capacità di monitorare i dati nel tempo, ad esempio, per valutare l’efficacia delle terapie o il decorso di una malattia³¹.

Alla luce di queste sfide derivanti dall’evoluzione tecnologica nella ricerca scientifica, in particolare in ambito sanitario, e dai limiti degli strumenti di tutela tradizionali, appare pertanto essenziale esaminare e valutare le soluzioni normative adottate dal legislatore europeo, principalmente attraverso il Regolamento generale sulla protezione dei dati personali (GDPR) e, più recentemente, tramite il Regolamento per l’istituzione dello Spazio Europeo dei Dati Sanitari (EHDS), al fine di garantire un adeguato equilibrio tra le esigenze della ricerca e la protezione dei soggetti coinvolti.

3. – Nel contesto delle sfide poste dall’evoluzione tecnologica e dalla globalizzazione, il Regolamento Generale sulla Protezione dei Dati (GDPR) si configura come una risposta uniforme e coerente del legislatore europeo, volta a garantire, da un lato, un adeguato livello di tutela delle persone fisiche e, dall’altro, a promuovere la libera circolazione dei dati personali³².

Questi obiettivi trovano espressione anche nelle disposizioni sul trattamento dei dati sanitari per finalità di ricerca scientifica, dove, attraverso un articolato sistema di divieti, eccezioni e prescrizioni di misure di garanzia adeguate, l’importanza attribuita al progresso scientifico per il miglioramento della qualità della vita della collettività³³ è attentamente bilanciata con la necessità di salvaguardare i diritti dei soggetti coinvolti³⁴.

²⁹ A. MANTELERO, *La privacy*, cit., 1190; ID., *Responsabilità e rischio nel Reg. Ue 2016/679*, in *Nuove leggi civ. comm.*, 2017, 1, 155.

³⁰ Tali osservazioni riguardano, dunque, il consenso come base giuridica per il trattamento dei dati personali e non quello richiesto per la partecipazione alla ricerca medica. Sotto il profilo etico, il consenso informato rimane necessario per il coinvolgimento di persone in progetti di ricerca che coinvolgono “corpi materiali”, salvo eccezioni in cui il soggetto non possa esprimerlo e la partecipazione sia ritenuta vantaggiosa per lo stesso, previa adozione di adeguate misure di salvaguardia (in merito alla necessità di distinguere tra consenso per il trattamento dei dati personali e consenso per la partecipazione alla ricerca, v. anche E.S. DOVE, *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*, in *The Journal of Law, Medicine & Ethics*, 2018, 4, 1022; EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 maggio 2020, 30 (i documenti dell’EDPB citati nel presente lavoro possono essere consultati sul sito ufficiale: www.edpb.europa.eu/); ID., *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, 2 febbraio 2021, 4; EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), *A Preliminary Opinion on data protection and scientific research*, 6 gennaio 2020, 18 (i documenti dell’EDPS citati nel presente lavoro possono essere consultati sul sito ufficiale: <https://www.edps.europa.eu/>).

³¹ In argomento v. anche, tra gli altri, M. MOSTERT-A.L. BREDENOORD, M.C. BIESAART, et al., *Big Data*, cit., 958.

³² V., in particolare, i considerando nn. 6 e 9 del GDPR. Il duplice obiettivo perseguito dal legislatore europeo emerge del resto chiaramente già dal titolo del Regolamento, oltre ad essere ulteriormente ribadito nel considerando n. 10 e nell’art. 1. In argomento, tra i molti, G. FINOCCHIARO, *Il quadro d’insieme sul regolamento europeo*, in ID. (opera diretta da), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018*, n. 101, Zanichelli, Bologna, 2019, 1 ss.; C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 2018, 22, 1 ss.

³³ Cfr. il considerando n. 157 del GDPR.

³⁴ V. anche EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 03/2020 on the processing of data concerning health for*



Nonostante l'ampio dibattito sull'impatto della nuova normativa sulla ricerca scientifica³⁵, il Regolamento non ha "stravolto"³⁶ l'impianto delineato dalla precedente Direttiva 95/46/CE. Pur mantenendo una certa continuità normativa, il GDPR ha tuttavia introdotto nuove previsioni che, insieme alle interpretazioni fornite dalle autorità europee, evidenziano l'intento di affrontare le sfide emergenti in tema di protezione dei dati personali in questo contesto.

Da questo angolo di osservazione, appaiono innanzitutto significative le ampie nozioni di «dati inerenti alla salute» e di «ricerca scientifica» adottate dal legislatore europeo, al fine di adeguarle alle potenzialità offerte dalle tecnologie *data-intensive*³⁷. In particolare, i «dati relativi alla salute» vengono definiti come i dati personali relativi alla salute fisica o mentale di una persona³⁸, inclusi i servizi di assistenza sanitaria, che rivelano «informazioni» sul suo stato di salute³⁹. Questa definizione, dunque, è significativamente più ampia rispetto al passato⁴⁰, avuto riguardo alla capacità delle moderne tecnologie di ottenere informazioni rilevanti anche da dati non strettamente sanitari. Come chiarito dal considerando n. 35 e ulteriormente approfondito dal Comitato europeo per la protezione dei dati⁴¹, tale nozione si estende, infatti, anche a informazioni derivate dall'analisi di dati biometrici⁴² o genetici e dai campioni biologici, nonché a quelle dedotte da riferimenti incrociati ad altri dati (che potrebbero rivelare, ad esempio, una predisposizione a malattie cardiovascolari attraverso misurazioni della pressione arteriosa)⁴³.

the purpose of scientific research in the context of the COVID-19 outbreak, 21 aprile 2020, 4 s., ove si evidenzia che le norme sulla protezione dei dati personali non prevalgono sulla libertà di scienza di cui all'art. 13 della Carta dei diritti fondamentali dell'UE, né viceversa. Di conseguenza, per rispettare «l'essenza» di questi diritti e libertà, è necessario un loro attento bilanciamento. Questo conferma quanto affermato in merito al diritto alla protezione dei dati, definito come un «diritto della persona tra le persone», richiamando così la relatività insita nei diritti della persona, il cui contenuto può essere soggetto a restrizioni giustificate dalla necessità di perseguire obiettivi di interesse generale. In questo senso, cfr. A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (opera diretta da) *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018*, n. 101, cit., 464 s.

³⁵ Secondo alcuni, le regole introdotte dal Regolamento ostacolerebbero eccessivamente l'attività dei ricercatori (v., tra gli altri, D. PELOQUIN-M. DI MAIO-B. BIERER, et al., *Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data*, in *European Journal of Human Genetics*, 2020, 697 ss.; M.C. PLOEM-M.L. ESSINK-BOT-K. STRONKS, *Proposed EU data protection regulation is a threat to medical research*, in *British Medical Journal*, 2013, 346, f3534, 1 s.), mentre, per altri, la disciplina introdotta favorirebbe eccessivamente la ricerca (in questo senso, tra gli altri, v. K. PORMEISTER, *Genetic data and the research exemption: is the GDPR going too far?*, in *International Data Privacy Law*, 2017, 7, 137 ss.).

³⁶ V. anche C. CASONATO-M. TOMASI, *Diritti*, cit., 348.

³⁷ Tali nozioni riflettono, dunque, il riconoscimento da parte del legislatore dell'ampia capacità informativa che caratterizza la ricerca scientifica *data-intensive*. Al riguardo, v. anche M. MOSTERT-A.L. BREDENOORD-M.C. BIESAART, et al., *Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach*, cit., 957.

³⁸ A ben vedere, l'ampio concetto di diritto alla salute da ultimo accolto (v. sopra par. 1, *sub* nt. 2), non più limitato al solo aspetto fisico-funzionale ma esteso alla piena realizzazione della persona e ai suoi bisogni psico-fisici, influisce anche su ciò che, dal punto di vista della *privacy* e della protezione dei dati, deve essere considerato «dato relativo alla salute» e, di conseguenza, sottoposto a una disciplina specifica rispetto ai dati «comuni».

³⁹ Cfr. art. 4, par. 1, n. 15, GDPR. La Direttiva 95/46/CE, invece, non forniva alcuna definizione specifica in merito, limitandosi a menzionare tra le categorie particolari di dati quelli «relativi alla salute e alla vita sessuale» (art. 8).

⁴⁰ Analogamente alla nozione di dato personale, anche quella di dato relativo alla salute è, pertanto, concepita in senso ampio.

⁴¹ Cfr., in particolare, EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 03/2020*, cit., 4.

⁴² Il considerando n. 35 include, infatti, anche «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». Ad esempio, i dati biometrici raccolti tramite strumenti di riconoscimento facciale possono essere analizzati per rilevare caratteristiche quali la simmetria del volto o la salute della pelle, che potrebbero indicare condizioni mediche come un episodio di ictus o patologie cutanee. V. anche A. DE FRANCESCHI, *Sub art. 4 (Definizioni)*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della privacy e data protection*, Giuffrè, Milano, 2021, 171.

⁴³ Il considerando n. 35 considera anche i dati contrassegnati da numeri, simboli o segni identificativi come può accadere nei registri ospedalieri e in quelli relativi a progetti di ricerca. In questo senso, cfr. A. DE FRANCESCHI, *Sub art. 4 (Definizioni)*, cit., 171. In



Allo stesso modo, la nozione di «ricerca scientifica», pur non definita espressamente dal Regolamento, trova importanti indicazioni nel considerando n. 159, che suggerisce un'interpretazione ampia, includendo attività di sviluppo tecnologico e dimostrazione, ricerca fondamentale e ricerca applicata. Questo approccio sottolinea, dunque, l'importanza di considerare come ricerca scientifica qualsiasi attività finalizzata a generare nuova conoscenza e a far progredire lo stato dell'arte in un settore scientifico specifico. La nozione include, inoltre, sia la ricerca pubblica che quella privata, anche a scopo di lucro⁴⁴, confermando l'importanza del settore privato, come nel caso delle case farmaceutiche, nel progresso scientifico e tecnologico⁴⁵.

Delineato l'ambito di applicazione del regolamento in relazione alla finalità di ricerca scientifica, è ora possibile soffermarsi sulle principali disposizioni ad essa dedicate, con particolare riferimento al trattamento dei dati relativi alla salute, le quali riflettono l'attenzione del legislatore verso le esigenze della ricerca contemporanea. Se da un lato il trattamento dei dati personali per finalità di ricerca scientifica è soggetto alle disposizioni generali previste dal Regolamento, compresi i principi fondamentali, i meccanismi di gestione del rischio e le tutele a favore degli interessati⁴⁶, dall'altro lato, infatti, il legislatore ha introdotto alcune deroghe e limitazioni che consentono di bilanciare le esigenze della ricerca che coinvolge dati relativi alla salute con il diritto alla protezione dei dati personali dei partecipanti.

Un primo aspetto da considerare, per verificare l'equilibrio delineato dal GDPR, riguarda le basi giuridiche che possono legittimare il trattamento dei dati personali in questo contesto.

Tra queste, vi è innanzitutto il consenso. Tradizionalmente considerato uno strumento di controllo significativo nella ricerca scientifica per prevenire abusi e garantire una scelta consapevole nella partecipazione a studi e sperimentazioni che possono influire sulla salute e l'integrità fisica, il consenso ha, invero, da sempre rappresentato anche la base giuridica principale per legittimare la ricerca che coinvolge dati personali⁴⁷.

Occorre tuttavia considerare distintamente il consenso richiesto per la partecipazione alla ricerca dal consenso inteso come fondamento legittimo per il trattamento dei dati personali⁴⁸. Il consenso al trattamento

argomento, v. anche G. CHASSANG, *The impact of the EU general data protection regulation on scientific research*, in *Ecancermedicalscience*, 2017, 11, 709.

⁴⁴ Un chiaro limite alla possibilità dei soggetti privati di beneficiare del regime di favore previsto per la ricerca scientifica dal GDPR emerge, tuttavia, dall'interpretazione offerta dal Gruppo di lavoro art. 29 per la protezione dei dati, il quale ha chiarito che il concetto di ricerca deve rimanere ancorato a rigorosi standard metodologici ed etici, conformi alle buone prassi (cfr. ID., *Guidelines on consent under Regulation 2016/679* (WP259), adottate il 28 novembre 2017 e da ultimo modificate il 10 aprile 2018, 28; EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), *A Preliminary Opinion*, cit., 11 s., il quale ha ulteriormente chiarito che la ricerca deve essere condotta con l'obiettivo di accrescere la conoscenza e il benessere collettivo della società, anziché servire prevalentemente uno o più interessi privati. V. anche EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 03/2020*, cit., 5 s.). Ad ogni modo, come giustamente osservato, sebbene la nozione di ricerca scientifica includa anche soggetti privati, le particolari condizioni previste per il trattamento di specifiche categorie di dati personali limitano di fatto le basi giuridiche a disposizione di coloro che operano per finalità commerciali, tra cui il consenso dell'interessato (in questo senso, cfr. P. QUINN, *Research*, cit., 24 ss.).

⁴⁵ L'importanza della componente privata e industriale nel progresso scientifico e tecnologico è, del resto, già sottolineata dall'art. 179, par. 1, TFUE, espressamente richiamato dal considerando in esame, che al contempo evidenzia l'esigenza di una libera circolazione delle conoscenze scientifiche e delle tecnologie a beneficio della società (in argomento, v. anche, tra gli altri, C. CASONATO-M. TOMASI, *Diritti*, cit., 351; P. GUARDA, *Il regime giuridico*, cit., 139).

⁴⁶ Cfr. il considerando n. 159.

⁴⁷ P. QUINN-L. QUINN, *Big genetic data and its big data protection challenges*, in *Computer Law & Security Review*, 2018, 1011, i quali evidenziano che il consenso al trattamento dei dati personali per finalità di ricerca è spesso considerato l'opzione di riferimento per i ricercatori, poiché risulta preferibile sotto il profilo etico ed è privilegiato nel GDPR, che ammette eccezioni per scopi di ricerca solo quando il consenso non è ritenuto strettamente necessario; R. DUCATO, *sub art. 89*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della privacy e data protection*, cit., 964.

⁴⁸ Riguardo alle vicende e agli sviluppi che hanno portato al riconoscimento del diritto all'autodeterminazione corporea da un lato e del diritto all'autodeterminazione informativa dall'altro, v. sopra *sub* nt. 11.



presenta, infatti, come già menzionato, profili di criticità nel contesto della ricerca scientifica contemporanea, segnata da avanzamenti tecnologici e informatici significativi, soprattutto in relazione alla predeterminazione delle finalità e al rispetto del principio di minimizzazione.

In questa prospettiva, pur mantenendo l'impostazione tradizionale e richiedendo requisiti rigorosi per il consenso al trattamento dei dati per scopi di ricerca scientifica⁴⁹, il legislatore europeo ha "consentito" un'attenuazione della rigidità nella specificazione delle finalità⁵⁰. Il Regolamento, infatti, riconosce il consenso come strumento essenziale di autodeterminazione, ma concede una maggiore flessibilità, ammettendo che le finalità della ricerca possano essere descritte in modo più generico, purché riguardino specifici settori e siano rispettate le norme deontologiche pertinenti⁵¹.

Per «compensare» questa maggiore flessibilità, il Comitato europeo per la protezione dei dati ha suggerito misure integrative idonee a garantire l'efficacia del consenso, come la delimitazione delle finalità della ricerca a un ambito scientifico specifico e la necessità di assicurare che gli interessati siano costantemente informati sullo sviluppo del progetto, consentendo loro di decidere se continuare a partecipare o revocare il consenso⁵²⁻⁵³.

L'obiettivo del legislatore non è, dunque, ove possibile⁵⁴, quello di abbandonare il paradigma consensualistico né di avallare un consenso "in bianco"⁵⁵, ma piuttosto di "ridimensionarlo" nei casi in cui le finalità del trattamento non possano essere definite con precisione fin dall'inizio, garantendo comunque adeguate misure di tutela.

Tuttavia, come discusso in precedenza⁵⁶, sebbene il consenso rappresenti uno strumento centrale per garantire all'interessato un certo controllo sull'uso delle proprie informazioni, presenta diversi limiti che emergono in modo evidente nel contesto della ricerca scientifica avanzata, i quali rimangono in gran parte irrisolti

⁴⁹ Cfr. art. 4, par. 1, n. 11, nonché l'art. 6, par. 1, lett. a. Al riguardo, v. anche EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 05/2020*, cit., 7 ss.; ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on consent*, cit., 4 ss. È pertanto necessario che il consenso sia realmente informato e consapevole, riflettendo una piena comprensione, da parte dell'interessato, delle modalità con cui i propri dati saranno utilizzati. In questo senso, v., tra gli altri, S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, Giuffrè, Milano, 2006, 1016. In generale, sui requisiti del consenso v., tra gli altri, F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (opera diretta da) *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018*, n. 101, cit., 151 ss.

⁵⁰ Cfr. considerando n. 33 del GDPR, la cui operatività, pur non avendo carattere vincolante, è stata più volte confermata anche dalle autorità europee e nazionali: v., tra gli altri, i documenti del Comitato europeo per la protezione dei dati richiamati alla nota successiva e GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 27 aprile 2023*, 27 aprile 2023, doc. web. n. 9898815 (tutti i documenti del Garante per la protezione dei dati personali citati nel presente contributo possono essere consultati all'indirizzo www.garanteprivacy.it).

⁵¹ V. EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 05/2020*, cit., 31 ss., dove si evidenzia inoltre che, nel caso del trattamento di particolari categorie di dati, l'applicazione di questo approccio "flessibile" in relazione al consenso richiede un'interpretazione più rigorosa e un livello di controllo più elevato. Sull'esatta portata del considerando n. 33 è atteso, tuttavia, un ulteriore chiarimento da parte dell'EDPB, nelle future linee guida sul trattamento dei dati personali per finalità di ricerca scientifica, più volte annunciate ma non ancora adottate (v. EUROPEAN DATA PROTECTION BOARD (EDPB), *Document on response*, cit., 7).

⁵² V. EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 05/2020*, cit., 30; ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on consent*, cit., 27 ss.

⁵³ L'equilibrio tra le esigenze della ricerca e i diritti degli interessati è ulteriormente rafforzato dalle garanzie previste dall'art. 89, par. 1, del GDPR, che richiede l'adozione di misure adeguate per proteggere i diritti e le libertà dei partecipanti alla ricerca, come la minimizzazione dei dati e la loro sicurezza. Sull'art. 89, par. 1, del GDPR, v. oltre par. 3.2.

⁵⁴ Al riguardo, v. quanto evidenziato oltre.

⁵⁵ Il Comitato ha in particolare chiarito che non si tratta dell'ammissibilità di un "ampio consenso" (*broad consent*): cfr. EUROPEAN DATA PROTECTION BOARD (EDPB), *Document on response*, cit., 7; ID., *Guidelines 05/2020*, cit., 7.

⁵⁶ V. sopra par. 2.



nonostante le possibilità di modulare il consenso per specifici ambiti⁵⁷. Inoltre, il consenso non esclude l'insorgere di difficoltà per lo svolgimento della ricerca, specialmente negli studi longitudinali, in quanto può essere revocato in qualsiasi momento dall'interessato⁵⁸, senza eccezioni per la ricerca scientifica⁵⁹.

Alla luce di tali difficoltà, emerge l'importanza di poter ricorrere ad altre basi giuridiche per l'uso dei dati, che offrono maggiore flessibilità per la ricerca pur garantendo i diritti degli interessati. Gli artt. 6 e 9 del Regolamento prevedono, infatti, ulteriori basi giuridiche e deroghe⁶⁰ che legittimano il trattamento dei dati sanitari per scopi di ricerca scientifica, offrendo così una maggiore flessibilità, pur nel rispetto di limiti e garanzie adeguate⁶¹.

Oltre al consenso, tra le basi giuridiche più rilevanti per la ricerca⁶² vi sono l'interesse pubblico e il legittimo interesse del titolare⁶³, da considerarsi, nel caso di dati sensibili, in relazione alle deroghe al divieto di trattamento previste dall'art. 9, par. 2⁶⁴, in particolare alle lett. *i* e *j*, che permettono il trattamento per motivi di interesse pubblico nel settore della sanità pubblica o per scopi di ricerca scientifica, sulla base del diritto dell'Unione o nazionale⁶⁵.

⁵⁷ Sui limiti dell'“apertura” offerta dal considerando n. 33 del GDPR, si è espresso, tra gli altri, R. MARTÍNEZ MARTÍNEZ, *Towards Regulation for the European Health Data Research: A Comparative Analysis*, in V. COLCELLI-R. CIPPITANI-C. BROCHHAUSEN-DELIUS, et al. (a cura di), *GDPR Requirements for Biobanking Activities Across Europe*, Springer International Publishing, Berlino, 2023, 414 s., il quale ha evidenziato come la necessità, sottolineata dall'EDPB, di prevedere un consenso per “fasi successive”, costringerebbe i ricercatori a richiedere ripetutamente il consenso. Questo meccanismo potrebbe portare a esiti simili a quelli osservati con le politiche sui *cookies*, ma con effetti opposti: mentre le continue richieste di autorizzazione per i *cookies* hanno portato gli utenti ad accettare senza riflettere, nel contesto dei dati sanitari, data la loro sensibilità, le ripetute richieste di consenso potrebbero indurre gli interessati a rifiutare automaticamente. Avanzano dubbi in merito alla soluzione offerta dal considerando n. 33 anche M. SHABANI e S. YILMAZ, *Lawfulness in secondary use of health data. Interplay between three regulatory frameworks of GDPR, DGA & EHDS*, in *Technology and Regulation*, 2022, 130.

⁵⁸ Cfr. art. 7, par. 3, GDPR. Questo diritto può, dunque, essere esercitato in qualsiasi momento, senza obbligo di giustificazione. La revoca, tuttavia, non pregiudica la liceità del trattamento effettuato in precedenza; il titolare è però tenuto a cessare le attività di trattamento in questione e, in assenza di un'altra base giuridica o di un motivo che giustifichi la conservazione dei dati per ulteriori trattamenti, deve procedere alla loro cancellazione (art. 17, par. 1, lett. *b*, e par. 3, GDPR).

⁵⁹ In proposito, è rilevante che il Regolamento riconosca espressamente il diritto di revoca in favore dell'interessato, a differenza del passato (in merito ai dibattiti sorti durante la vigenza della disciplina precedente, v., tra gli altri, F. CAGGIA, *sub art. 7*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della privacy e data protection*, cit., 223 ss.).

⁶⁰ L'art. 9 del GDPR, dedicato al trattamento di particolari categorie di dati, prevede, come già la precedente Direttiva, un divieto generale di trattare i dati che rientrano nell'ambito di tale disposizione. La portata di tale divieto è, tuttavia, “attenuata” attraverso un lungo e dettagliato elenco di deroghe, confermando che il diritto alla protezione dei dati personali non costituisce una prerogativa assoluta, ma deve essere bilanciato con altri diritti fondamentali parimenti meritevoli di tutela, in conformità al principio di proporzionalità (considerando n. 4). Cfr., inoltre, il considerando n. 51 GDPR, il quale conferma la necessità di applicare cumulativamente le eccezioni previste dall'art. 9, par. 2 GDPR con le «condizioni di liceità» previste dall'art. 6 GDPR.

⁶¹ In questi casi, il consenso prestato per la partecipazione ad attività di ricerca scientifica può essere considerato una garanzia aggiuntiva per il trattamento dei dati personali, oltre a quanto richiesto dall'art. 89 GDPR. In questo senso, cfr. EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 05/2020*, cit., 30; EUROPEAN DATA PROTECTION BOARD (EDPB), *Document on response*, cit., 4.

⁶² La ricerca scientifica, di per sé, non costituisce una base giuridica ai sensi dell'art. 6 del GDPR. È stato osservato che la scelta del legislatore mira a evitare il rischio di far prevalere indiscriminatamente le finalità della ricerca, sfruttando il pretesto di una presunta superiore utilità collettiva. Di conseguenza, la soluzione adottata richiede che, indipendentemente dalla base giuridica prescelta per il trattamento, si effettui un giudizio comparativo tra il tipo di ricerca, le informazioni da raccogliere e i diversi interessi dei partecipanti coinvolti. Al riguardo, v. A. BERNES, *La protezione dei dati personali nell'attività di ricerca scientifica*, in *Nuove leggi civ. comm.*, 2020, 1, 185 s.; S. SLOKENBERGA, *Scientific Research Regime 2.0? How the proposed EHDS Regulation may change the GDPR Research Regime*, in *Technology and Regulation*, 2022, 139. V. anche ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 03/2013 on purpose limitation* (WP203), adottate il 2 aprile 2013, 42. Ciò nonostante, la previsione di una specifica deroga al divieto di trattamento di particolari categorie di dati quando effettuato per scopi di ricerca scientifica (art. 9, par. 2, lett. *j*, GDPR), assente nella Direttiva, evidenzia l'importanza attribuita a tale attività, ampliando gli spazi di operatività della ricerca stessa.

⁶³ Previsti, rispettivamente, dall'art. 6, par. 1, lett. *e* e *f*, GDPR.

⁶⁴ V. sopra *sub* nt. 60.

⁶⁵ Cfr. EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 05/2020*, cit., 30 e *sub* nt. 72. In questo senso, v. anche P. QUINN, *Research*, cit., 9 ss.; G. COMANDÉ, *Ricerca*, cit., 197.



Quando il trattamento dei dati è giustificato dall'esecuzione di un compito di interesse pubblico, la legge interviene per bilanciare preventivamente i diritti individuali con le esigenze collettive legate alla ricerca. In questo contesto, è dunque la normativa nazionale o dell'Unione a stabilire la prevalenza dell'interesse pubblico⁶⁶, definendo le finalità e le condizioni del trattamento, il tipo di dati trattati, i soggetti coinvolti e il periodo di conservazione⁶⁷.

Ad ogni modo, non tutti gli studi rientrano nel concetto di "interesse pubblico" definito dal legislatore; pertanto, in alcuni casi, il legittimo interesse del titolare del trattamento⁶⁸ può costituire una valida alternativa al consenso, specialmente in relazione a progetti di ricerca che presentano significative implicazioni commerciali⁶⁹, come nel caso di sviluppo di prodotti farmaceutici⁷⁰. Anche in tali circostanze, il bilanciamento tra l'interesse del titolare del trattamento e i diritti degli interessati è determinato a priori dal legislatore, che riconosce il legittimo interesse del titolare come base giuridica. Questa scelta impone, tuttavia, al titolare di valutare attentamente le circostanze del caso concreto e di assumersi la responsabilità di proteggere i diritti degli interessati, in conformità al principio di *accountability*⁷¹.

Infine, anche quando il trattamento dei dati avviene senza il consenso dell'interessato, per motivi di interesse pubblico o di legittimo interesse del titolare, quest'ultimo conserva comunque il diritto di esercitare un controllo sui propri dati⁷² attraverso il diritto di opposizione (art. 21 GDPR), qualora sussistano motivi legati alla sua situazione particolare, sebbene questo diritto possa essere limitato in presenza di interessi superiori legati alla ricerca scientifica che giustificano la prosecuzione del trattamento⁷³.

⁶⁶ Questa base giuridica può applicarsi anche alle organizzazioni private che svolgono attività di ricerca nell'interesse pubblico, nonché a quelle ricerche che coinvolgono la collaborazione tra il settore pubblico e quello privato. In proposito, cfr. G. COMANDÉ, *Ricerca*, cit., 197.

⁶⁷ Cfr. il considerando n. 45 del GDPR.

⁶⁸ Tale base giuridica è stata tuttavia ritenuta la più «problematica» (cfr. D. POLETTI, *sub Art. 6*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della privacy e data protection*, cit., 200), a causa dell'indeterminatezza del concetto di «legittimo interesse» e della necessità per il titolare di operare un delicato e complesso bilanciamento d'interessi.

⁶⁹ V. EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*, 8 ottobre 2024, 11; ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP 217), 9 aprile 2014, 25. Al riguardo, è importante evidenziare che il considerando n. 47 esclude l'utilizzo della base giuridica in esame da parte di soggetti pubblici per i trattamenti effettuati nell'esecuzione dei loro compiti, stabilendo che spetta al legislatore prevedere per legge la base giuridica che autorizzi questi soggetti a trattare i dati personali. È stato tuttavia osservato che questa esclusione può risultare problematica, poiché la ricerca scientifica si caratterizza sempre più per la collaborazione tra il settore pubblico e quello privato: cfr. G. COMANDÉ, *Ricerca*, cit., 197.

⁷⁰ Questo conferma, dunque, che la ricerca scientifica, anche se orientata da obiettivi economici, può comunque contribuire al progresso della conoscenza e alla tutela della salute pubblica. In proposito, v. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 06/2014 on the notion of legitimate interests*, cit., 35. In argomento, v. anche, tra gli altri, I. RAPISARDA, *Ricerca scientifica e circolazione dei dati personali. Verso il definitivo superamento del paradigma privatistico?*, in *Eur. e Dir. Priv.*, 2021, 2, 309; A. BERNES, *La protezione*, cit., 189.

⁷¹ Ad ogni modo, il Regolamento fornisce parametri interpretativi importanti per evitare che questa base giuridica diventi un espediente per eludere la normativa sulla protezione dei dati personali: cfr. i considerando nn. 47-50 GDPR. Ulteriori indicazioni si rinviengono nelle linee guida e nelle decisioni adottate a livello europeo e nazionale (v., in particolare, EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 1/2024*, cit., 9 ss.; ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 06/2014 on the notion of legitimate interests*, cit., 30 ss.; GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento (UE) 2016/679*, 22 febbraio 2018, doc. web n. 8080493.

⁷² V. anche ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 15/2011 on the definition of consent* (WP187), 13 luglio 2011, 8, dove si evidenzia che l'opposizione rappresenta uno degli strumenti che consentono all'interessato di mantenere il controllo sulle informazioni che lo riguardano. In dottrina, tra gli altri, A. RICCI, *I diritti dell'interessato*, cit., 448.

⁷³ V. oltre.



3.1. – Nel quadro dell’attenzione che il GDPR dedica alle esigenze concrete della ricerca scientifica, occupa un ruolo di rilievo la disciplina dell’“ulteriore trattamento” (talvolta indicato come “uso secondario” o “riutilizzo”), definito come il trattamento dei dati personali per “finalità diverse” rispetto a quelle per cui sono stati originariamente raccolti (o generati)⁷⁴.

In generale, il principio della limitazione delle finalità consente ai titolari di trattare i dati personali raccolti per scopi determinati, espliciti e legittimi, anche per finalità ulteriori, purché «compatibili» con quelle iniziali⁷⁵. La valutazione di tale compatibilità si basa su diversi fattori, tra cui il rapporto tra le finalità originarie e quelle successive, il contesto della raccolta e la natura dei dati⁷⁶.

Una particolare considerazione è riservata⁷⁷ all’ulteriore trattamento per scopi di ricerca scientifica⁷⁸, che può essere ritenuto compatibile con le finalità iniziali, qualora conforme ai criteri sanciti dall’art. 89, par. 1, GDPR. Questa disposizione riveste un’importanza significativa, poiché i dati sanitari generati in contesti eterogenei possiedono un’utilità che trascende lo specifico uso clinico, diagnostico o anche di ricerca per cui sono stati eventualmente raccolti⁷⁹. Inoltre, come già evidenziato, la necessità di specifiche analisi sui dati emerge spesso solo dopo la loro raccolta, un aspetto accentuato nell’attuale contesto della ricerca *data intensive*. Il legislatore europeo ha, pertanto, chiarito, rispetto alla normativa precedente⁸⁰, la «presunzione di compatibilità» tra la finalità iniziale e quella successiva per la ricerca scientifica, escludendo, in linea di principio⁸¹, la necessità per il titolare del trattamento iniziale⁸² di ricercare una base giuridica distinta per l’ulteriore trattamento.

⁷⁴ Cfr. considerando n. 50 e art. 5, par. 1, lett. *b*, GDPR. Nel contesto in esame, tale concetto si riferisce al riutilizzo di dati personali, inclusi quelli sanitari derivati da campioni biologici, raccolti originariamente per scopi diversi, come ricerche con obiettivi differenti o attività di assistenza sanitaria. Tuttavia, in ambito sanitario viene impiegato il termine “uso secondario di dati” con un significato diverso, che può generare incertezza. L’uso secondario nel settore medico, infatti, si riferisce principalmente al riutilizzo di dati sanitari originariamente raccolti per finalità cliniche (ad esempio, diagnosi e trattamento) in nuovi contesti, come la ricerca scientifica, la medicina di precisione o la gestione delle politiche sanitarie.

⁷⁵ Cfr. art. 5, par. 1, lett. *b*, GDPR.

⁷⁶ Cfr. art. 6, par. 4 e considerando n. 50 del GDPR. V., inoltre, ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 03/2013 on purpose limitation*, cit., 23 ss.

⁷⁷ Una diversa precisazione è prevista dall’art. 6, par. 4 del GDPR, che esclude la necessità del test di compatibilità quando l’ulteriore trattamento si basa sul consenso dell’interessato o su una normativa dell’Unione o di uno Stato membro adottata ai sensi dell’art. 23 del GDPR. L’esclusione è tuttavia giustificata dal fatto che, nel primo caso, è l’interessato stesso a legittimare l’ulteriore trattamento, mentre, nel secondo caso, il bilanciamento degli interessi e le garanzie necessarie sono già stati valutati e incorporati nella relativa legislazione.

⁷⁸ Più precisamente, la disposizione in commento si riferisce agli ulteriori trattamenti effettuati a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

⁷⁹ V. anche R. BECKER-D. CHOKOSHVILI-G. COMANDÉ, 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*, 2023, 30, 131; M.L. MANIS, *The processing of personal data in the context of scientific research. The new regime under the EU-GDPR*, in *BioLaw Journal*, 2017, 3, 331.

⁸⁰ La presunzione di compatibilità era, infatti, già contemplata nella Direttiva n. 95/46/CE (art. 6, par. 1, lett. *b*) e, tuttavia, in mancanza di precise indicazioni, la sua applicazione aveva dato luogo a interpretazioni contrastanti.

⁸¹ V. quanto evidenziato oltre.

⁸² L’“ulteriore trattamento” di cui si discute viene sempre effettuato dal titolare del trattamento che ha inizialmente raccolto i dati per una finalità diversa, sia quando il successivo trattamento viene eseguito dal titolare stesso per scopi propri diversi da quelli originari, sia nel caso in cui i dati vengano comunicati a un terzo affinché quest’ultimo li tratti per finalità di ricerca proprie. In quest’ultimo scenario, l’“ulteriore trattamento” da parte del titolare originario consiste nella condivisione dei dati con il terzo; di conseguenza, spetta al primo verificare la compatibilità e la liceità dell’ulteriore trattamento, nonché informare l’interessato dell’intenzione di effettuare tale trattamento, come richiesto dagli articoli 13, par. 3, e 14, par. 4 del GDPR. Al contrario, per il terzo che richiede l’accesso ai dati per trattarli per scopi di ricerca scientifica propri, tale trattamento costituirà una finalità primaria, richiedendo quindi l’individuazione e l’applicazione di una propria base giuridica, distinta da quella utilizzata dal titolare originario, e il rispetto di tutti i requisiti previsti dal GDPR. Al riguardo, cfr. anche Cass. 7 ottobre 2021, n. 27325, in *DeJure*, la quale, chiamata a pronunciarsi sulla cessione di una bio-



Questa formulazione ha tuttavia contribuito all'emergere dell'idea che la ricerca scientifica goda di uno *status* privilegiato nel Regolamento, esonerando automaticamente i titolari dall'individuazione di una specifica base giuridica per l'ulteriore trattamento dei dati per finalità diverse rispetto a quelle originarie. Di conseguenza, sono emerse preoccupazioni riguardo all'adeguatezza della tutela dei dati personali, in particolare dei dati sanitari. Sebbene la norma faciliti la ricerca e renda più agevole lo svolgimento delle attività, è necessario riconsiderarne la portata: per beneficiare della presunzione di compatibilità prevista per la ricerca scientifica, è infatti necessario rispettare condizioni rigorose e tenere conto di determinati fattori⁸³. A tal proposito, anche le autorità europee hanno chiarito che la deroga non deve essere intesa come "un'autorizzazione generale" al trattamento ulteriore dei dati ogniqualvolta vi sia una finalità di ricerca⁸⁴.

Una delle questioni principali concerne il requisito della base giuridica. Ai sensi del considerando n. 50, quando l'"ulteriore trattamento" è compatibile con le finalità iniziali, «non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali». Questo potrebbe indurre a ritenere che la base giuridica originaria si "estenda" automaticamente al trattamento successivo⁸⁵. Una lettura approfondita del considerando e delle disposizioni del GDPR rivela, tuttavia, che ciò è valido solo qualora l'ulteriore trattamento soddisfi i requisiti della base giuridica originaria. In particolare, il considerando n. 50 richiede che il titolare effettui comunque un formale test di compatibilità – non necessario per la ricerca scientifica, in quanto la compatibilità si presume – solo «dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario». Tra questi requisiti fondamentali vi è l'obbligo di garantire che il successivo trattamento continui a rispettare le condizioni della base giuridica prescelta, ai sensi dell'art. 6, par. 1, GDPR, con la conseguenza che la sola "compatibilità" delle finalità non assicura la liceità del trattamento⁸⁶, essendo necessario accertare se la base giuridica originaria possa effettivamente "estendersi" all'ulteriore trattamento⁸⁷⁻⁸⁸. Inoltre, qualora l'ulteriore trattamento riguardi categorie particolari di dati, come quelli sanitari, il

banca contenente dati genetici (c.d. caso SharDna), ha evidenziato che «il trasferimento dei dati dal titolare originario ad un altro soggetto (...) dà luogo alla cessazione del trattamento originario – e non alla successione nello stesso –, comportando, quindi, l'inizio di un distinto trattamento ad opera del nuovo titolare, tenuto al rispetto della complessiva disciplina in tema di informativa e consenso»; GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 27 aprile 2023*, cit. In dottrina, v. R. BECKER-D. CHOKOSHVILI-G. COMANDÉ, et al., *Secondary use*, cit., 149, i quali evidenziano che «*the collection by a downstream controller effectively marks a "reset" in the chain to the extent that it takes place for a primary purpose, which needs a legal basis on its own*».

⁸³ Al riguardo, v. anche R. BECKER-D. CHOKOSHVILI-G. COMANDÉ, et al., *Secondary use*, cit., 147 s.

⁸⁴ Cfr. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 03/2013 on purpose limitation*, cit., 28.

⁸⁵ Tale interpretazione potrebbe sembrare ulteriormente supportata dal riferimento alla "liceità" contenuto nel considerando n. 50, il quale afferma che: «L'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile». Tuttavia, la nozione di liceità nel GDPR ha un ambito più ampio, non limitato alla semplice esistenza di una base giuridica adeguata. Questo concetto include, ad esempio, il rispetto delle norme relative al trattamento di categorie particolari di dati o al trasferimento di dati verso Paesi terzi e può essere influenzato anche dal rispetto delle normative nazionali. V. anche R. BECKER-D. CHOKOSHVILI-G. COMANDÉ, et al., *Secondary use*, cit., 154.

⁸⁶ Contrariamente a quanto affermato da alcuni autori, non si può pertanto ritenere che la disciplina della presunzione di compatibilità abbia introdotto un ulteriore fondamento per il riutilizzo dei dati nell'ambito della ricerca. La mancanza di volontà di individuare una specifica base giuridica per la ricerca scientifica emerge del resto chiaramente dall'art. 6 del GDPR, che non include un riferimento specifico a questo scopo (v. anche sopra, *sub* nt. 62).

⁸⁷ Ad esempio, se il trattamento originario si basava sul legittimo interesse, il titolare deve verificare che questa base giuridica giustifichi anche l'ulteriore trattamento. Alla luce di ciò, soprattutto nel caso della ricerca scientifica, le limitate basi giuridiche disponibili evidenziano la possibilità che la base giuridica originaria non sia sufficiente a giustificare l'ulteriore trattamento, richiedendo quindi al titolare di individuare una nuova base giuridica (v. sopra, *sub* par. 3).

⁸⁸ La ricostruzione delineata trova conferma nelle osservazioni espresse dal Gruppo di lavoro art. 29 in relazione alla Proposta di Regolamento sulla protezione dei dati personali. Anche con riferimento alla disciplina proposta nel Regolamento, come già per la Direttiva, l'Autorità europea ha, infatti, evidenziato che: «*these provisions (...) confuse two different concepts: the notion of 'compatibility' under Article 5(b) of the proposed Data Protection Regulation and the notion of 'lawful ground' under Article 6. As explained*



titolare dovrà anche verificare la conformità alle condizioni previste dall'art. 9, par. 2, GDPR.

A ciò si aggiunga che, oltre a garantire che l'ulteriore trattamento per finalità di ricerca scientifica sia supportato da una base giuridica adeguata, il titolare deve dimostrare il rispetto degli ulteriori requisiti di liceità previsti dal GDPR, tra cui i principi delineati dall'art. 5.

Come già menzionato, l'applicazione della "presunzione di compatibilità" è altresì subordinata all'adozione delle misure di salvaguardia stabilite dall'art. 89, par. 1, GDPR⁸⁹. Il titolare del trattamento è pertanto tenuto a implementare misure tecniche e organizzative appropriate, in particolare per garantire il rispetto del principio di minimizzazione, nonché dei principi di integrità e riservatezza dei dati⁹⁰, utilizzando, ove possibile, dati anonimi o anonimizzati. Qualora i dati siano comunicati a un terzo per scopi di ricerca, quest'ultimo è tenuto a garantire analoghe misure di protezione, oltre ad essere conforme agli altri requisiti sopra discussi⁹¹.

Occorre infine considerare la possibilità offerta agli Stati membri di introdurre ulteriori restrizioni⁹², che potrebbero, ad esempio, imporre al titolare del trattamento l'obbligo di ottenere un'autorizzazione preventiva dall'Autorità garante⁹³. L'ulteriore trattamento di dati sanitari per scopi di ricerca potrebbe anche essere soggetto a normative settoriali specifiche a livello nazionale, come le disposizioni sul segreto medico, le quali potrebbero limitare il riutilizzo dei dati raccolti in un contesto clinico⁹⁴.

Nel complesso, queste considerazioni evidenziano che il requisito della "compatibilità", la cui sussistenza è "presunta" per le finalità di ricerca scientifica, rappresenta una condizione necessaria ma non sufficiente

earlier, these two requirements are cumulative. Processing of personal data for the purposes of historical, statistical or scientific research must be based on one of the legal grounds (points a to f), in any event. Article 83 may help assess under what conditions further use may be compatible (and more generally, what safeguards must be applied in case of any processing for historical, statistical or scientific purposes) but cannot provide a substitute for an appropriate lawful ground for the processing» (cfr. ID., *Opinion 03/2013 on purpose limitation*, cit., 33; nello stesso senso, v. anche EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), *Preliminary Opinion*, cit., 22 s.) In dottrina, accolgono tale soluzione, tra gli altri, R. BECKER-D. CHOKOSHVILI-G. COMANDÉ, et al., *Secondary use*, cit., 149; M. SHABANI-S. YILMAZ, *Lawfulness*, cit., 130. V., inoltre, S. SLOKENBERGA, *Scientific Research*, cit., 139, la quale evidenzia la presenza, in dottrina, di due diverse interpretazioni della questione in esame.

⁸⁹ Al riguardo, v. più ampiamente oltre, *sub par. 3.2*.

⁹⁰ Cfr. EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 03/2020*, cit., 9.

⁹¹ V. sopra, *sub nt. 82*. V. anche i dubbi sollevati in proposito da R. BECKER-D. CHOKOSHVILI-G. COMANDÉ, et al., *Secondary use*, cit., 148, riguardo alla questione se, nei casi in cui i dati personali siano comunicati a terzi affinché questi ultimi li utilizzino per finalità di ricerca proprie, l'accertamento dell'effettiva esistenza e operatività delle garanzie previste dall'art. 89 del GDPR debba rientrare nel test di compatibilità che il titolare originario dei dati è tenuto a svolgere per valutare la legittimità dell'ulteriore trattamento, oppure se siano sufficienti le mere rassicurazioni fornite dal terzo in merito alla loro presenza.

⁹² V. oltre, *sub par. 3.3*.

⁹³ In proposito, per quanto riguarda la disciplina italiana, l'art. 110-*bis* del d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, contiene una disposizione specifica per il "trattamento ulteriore" dei dati personali a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi (ossia, soggetti diversi dal titolare che ha originariamente raccolto i dati). In particolare, si prevede che il Garante possa autorizzare, anche mediante provvedimenti generali, il trattamento ulteriore di dati personali da parte di tali soggetti terzi quando, per ragioni particolari, informare gli interessati risulti impossibile, comporti uno sforzo sproporzionato, o rischi di compromettere gravemente il raggiungimento delle finalità della ricerca. Tale autorizzazione è concessa a condizione che siano adottate misure adeguate di tutela, in conformità all'art. 89 del GDPR, comprese forme preventive di minimizzazione e di anonimizzazione dei dati. Il trattamento da parte del soggetto terzo sarà pertanto possibile solo in presenza di tale autorizzazione da parte dell'Autorità garante (la disposizione rappresenta, dunque, una specificazione a livello nazionale dell'art. 15, par. 5, lett. *b*, del GDPR). In argomento v., tra gli altri, L. BOLOGNINI-S. ZIPPONI, *Tutela dei dati personali nel settore della ricerca scientifica e delle sperimentazioni cliniche: la normativa italiana*, in ID.-ID. (a cura di), *Privacy e diritto dei dati sanitari*, Giuffrè, 2024, 221 ss.; S. MELCHIONNA, *sub art. 110-bis. Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici*, in R. 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)*, Pacini, 2019, 461 ss.

⁹⁴ V. R. BECKER-D. CHOKOSHVILI-G. COMANDÉ, et al., *Secondary use*, cit., 151.



per legittimare l'ulteriore trattamento, dovendo essere soddisfatte altre condizioni affinché esso sia effettivamente lecito⁹⁵. Questo mette in luce, pertanto, l'esigenza di riconsiderare l'interpretazione di un regime di eccessivo favore per la ricerca scientifica, rafforzando l'importanza di un'applicazione rigorosa delle tutele previste dal GDPR.

3.2. – Le regole finora esaminate evidenziano come, nell'ambito del Regolamento, il bilanciamento tra la tutela degli interessi individuali e le esigenze della ricerca scientifica assuma connotati specifici, articolandosi attraverso un complesso processo di contemperamento. Questo approccio emerge chiaramente anche nella disciplina relativa all'esercizio dei diritti dell'interessato⁹⁶, nel caso in cui i suoi dati personali siano trattati per finalità di ricerca scientifica. Il Regolamento riconosce infatti che, in alcuni contesti, l'esercizio di tali diritti potrebbe rendere impossibile o compromettere gravemente il conseguimento degli obiettivi della ricerca. Di conseguenza, sono previste specifiche limitazioni, alcune già contemplate e applicabili direttamente dal titolare del trattamento, mentre altre possono essere introdotte mediante il diritto dell'Unione o degli Stati membri⁹⁷. In ogni caso, l'adozione di adeguate misure di salvaguardia, in conformità all'art. 89 del GDPR, è necessaria per evitare, per quanto possibile, un pregiudizio ai diritti e alle libertà dell'interessato.

Le limitazioni espressamente previste riguardano il diritto alla cancellazione, il diritto di opposizione e il diritto di essere informato. Il diritto alla cancellazione⁹⁸, che consente all'interessato di ottenere la rimozione dei propri dati – tra l'altro, nel caso di revoca del consenso o opposizione al trattamento –, può essere infatti limitato nel contesto della ricerca scientifica, qualora tale cancellazione comprometta i risultati dello studio⁹⁹. In tal modo, il Regolamento offre al titolare del trattamento un importante strumento per bilanciare gli effetti negativi derivanti dall'esercizio dei diritti da parte degli interessati, sebbene l'onere della prova a carico del titolare debba essere interpretato in modo rigoroso¹⁰⁰.

Questa disposizione si collega a un'altra norma favorevole alla ricerca, riguardante la conservazione dei dati personali nel tempo. In particolare, in base al principio di limitazione della conservazione, i dati dovrebbero essere mantenuti in forma identificabile solo per il periodo necessario al raggiungimento degli scopi del trattamento; tuttavia, in presenza di adeguate garanzie, questo periodo può essere esteso per finalità di ricerca scientifica¹⁰¹.

Analoghi limiti a favore della ricerca si applicano all'esercizio del diritto di opposizione di cui all'art. 21 GDPR. Come anticipato, questo diritto consente all'interessato di opporsi (dunque, *ex post*) al trattamento

⁹⁵ In ogni caso, sulla questione si attende la pubblicazione delle linee guida sul trattamento dei dati personali per scopi di ricerca scientifica, la cui adozione è stata annunciata da tempo dall'EDPB (v. EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 03/2020*, cit., 9).

⁹⁶ In generale, sui diritti riconosciuti all'interessato v., tra gli altri, A. RICCI, *I diritti dell'interessato*, cit., 392 ss.

⁹⁷ Al riguardo, v. oltre, *sub* par. 3.3.

⁹⁸ Il Regolamento ha ampliato l'ambito di applicazione del diritto alla cancellazione rispetto a quanto previsto dalla precedente Direttiva, introducendo una disciplina specifica (v. art. 17 GDPR).

⁹⁹ Cfr. art. 17, par. 3, lett. *d*, GDPR.

¹⁰⁰ Questo limite deve tuttavia ritenersi applicabile agli studi già avviati o conclusi, mentre i dati conservati per un eventuale riutilizzo dovrebbero rimanere soggetti al diritto di cancellazione. Può infatti presupporre che, non essendo la ricerca ancora iniziata, in questi casi l'esercizio del diritto alla cancellazione non comprometta il raggiungimento degli obiettivi della ricerca. In questo senso, cfr. K. PORMEISTER, *Genetic data*, cit., 140; R. DUCATO, *sub art. 89*, cit., 973.

¹⁰¹ Cfr. art. 5, par. 1, lett. *e*, GDPR. In tal senso, v. anche l'art. 99, d.lgs. n. 196/2003, modificato dal d.lgs. n. 101/2018 in adeguamento della disciplina europea.



dei propri dati personali per motivi legati alla sua situazione particolare¹⁰², qualora il trattamento non si basi sul consenso¹⁰³. L'esercizio di tale diritto è tuttavia soggetto a limitazioni che, ancora una volta, mettono in evidenza la complessità del bilanciamento tra interessi individuali e interessi al progresso scientifico. In particolare, i motivi dell'interessato possono essere superati da interessi prevalenti, come quelli legati a scopi di ricerca (par. 1). Il par. 6 della stessa disposizione introduce inoltre una previsione esplicita, assente nella Direttiva precedente, che stabilisce la prevalenza delle finalità di ricerca sulle ragioni dell'interessato quando il trattamento è necessario per «l'esecuzione di un compito di interesse pubblico»¹⁰⁴.

Infine, un'ulteriore deroga riguarda gli obblighi informativi a carico del titolare del trattamento. In generale, nel rispetto del principio di trasparenza, gli interessati devono essere informati del trattamento dei propri dati e delle sue caratteristiche, anche nel caso di un ulteriore trattamento. Tale obbligo, che ricade sui titolari del trattamento, è fondamentale perché consente agli interessati di esercitare un controllo consapevole sui propri dati e, se necessario, di far valere i propri diritti in merito al trattamento¹⁰⁵. Tuttavia, il legislatore prevede eccezioni a questo obbligo quando i dati non siano raccolti direttamente dall'interessato¹⁰⁶ e la comunicazione di tali informazioni risulti impossibile o richieda sforzi sproporzionati¹⁰⁷, in particolare per i trattamenti a fini di archiviazione nel pubblico interesse, ricerca scientifica o storica, o finalità statistiche, oppure quando tale obbligo rischi di rendere impossibile o di compromettere gravemente il conseguimento delle finalità del trattamento (l'art. 14, par. 5, lett. b). In queste ipotesi, dunque, il titolare può essere esonerato dall'obbligo di informare l'interessato, previa adozione di adeguate misure di salvaguardia, come la pubblicazione delle informazioni sul proprio sito web e l'adozione di adeguate (ulteriori) misure tecniche e organizzative per tutelare i diritti degli interessati¹⁰⁸.

Come emerso dall'analisi precedente, il quadro normativo delineato dal Regolamento consente deroghe significative al regime generale di tutela dei dati personali per finalità di ricerca scientifica, purché il titolare adotti misure tecniche e organizzative idonee a proteggere i diritti e le libertà degli interessati. Le disposizioni a favore della ricerca scientifica, infatti, rimandano costantemente all'art. 89, par. 1, GDPR, che impone l'adozione di garanzie adeguate.

¹⁰² A differenza, dunque, del diritto di revoca, che può essere esercitato senza la necessità di fornire una motivazione (in proposito, v. anche quanto osservato da F. BRAVO, *Le condizioni*, cit., 159 s.).

¹⁰³ In particolare, questo diritto può essere esercitato nei casi in cui il trattamento si basi su un interesse legittimo del titolare o su ragioni di interesse pubblico.

¹⁰⁴ Come osservato, l'ambito di applicazione di questa previsione risulta piuttosto limitato, poiché non tutti i progetti di ricerca possono essere considerati necessari per l'esecuzione di un compito di interesse pubblico: cfr. M.L. MANIS, *The processing*, cit., 340.

¹⁰⁵ Cfr. ARTICLE 29 WORKING PARTY, *Guidelines on transparency under Regulation 2016/679* (WP260), adottate il 29 novembre 2017 e da ultimo modificate l'11 aprile 2018, 5; CGUE, conclusioni dell'Avvocato Generale Cruz Villalón, causa C-201/14, *Bara*, 9 luglio 2015, par. 74.

¹⁰⁶ A ben vedere, si tratta dell'ipotesi più frequente con riferimento ai trattamenti effettuati per finalità di ricerca scientifica, poiché i ricercatori spesso utilizzano dati raccolti durante i trattamenti sanitari dei pazienti, come quelli contenuti nelle cartelle cliniche. Non sono invece previste eccezioni per gli obblighi informativi nel caso in cui i dati siano ottenuti direttamente dall'interessato. Tuttavia, potrebbero esistere situazioni, come in alcuni esperimenti di psicologia, in cui informare l'interessato sugli scopi e le modalità della ricerca potrebbe comprometterne i risultati. La questione è stata sollevata dall'EDPB, che ha evidenziato la necessità di avviare un dibattito più ampio su questo aspetto (cfr. EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), *A Preliminary Opinion*, cit., 20 s.).

¹⁰⁷ Qualora il titolare intenda avvalersi di tale eccezione per ragioni di "sforzo sproporzionato", è tenuto a compiere un giudizio di bilanciamento, valutando lo sforzo necessario per fornire le informazioni rispetto all'impatto e agli effetti che la loro assenza potrebbe avere sull'interessato (il considerando n. 62 prevede che lo "sforzo sproporzionato" debba essere valutato tenendo conto del numero di soggetti interessati, della data di raccolta dei dati e delle eventuali garanzie adottate). Inoltre, qualora venga meno l'"impossibilità" di fornire le informazioni, il titolare del trattamento è tenuto a comunicarle immediatamente agli interessati.

¹⁰⁸ Le ulteriori garanzie potrebbero comprendere, ad esempio, una valutazione d'impatto, la pseudonimizzazione dei dati, la minimizzazione e l'adozione di misure tecniche e organizzative che assicurino un elevato livello di sicurezza (cfr. ARTICLE 29 WORKING PARTY, *Guidelines on transparency*, cit., 28 ss.).



In particolare, l'art. 89, par. 1, stabilisce che il trattamento dei dati personali per scopi di ricerca scientifica¹⁰⁹ deve essere accompagnato da misure appropriate, conformi ai principi del Regolamento e orientate verso lo scopo della ricerca. Queste misure devono pertanto tenere conto dei rischi specifici, come la probabilità e la gravità del rischio per i diritti e le libertà degli interessati, il tipo di dati trattati e le circostanze del caso concreto.

La presenza di una norma che prescrive l'adozione di garanzie specifiche dimostra, dunque, l'attenzione del legislatore alla complessità dei rischi legati alla ricerca e alla necessità di bilanciare l'interesse per il progresso scientifico con la tutela dei diritti fondamentali degli interessati. Sebbene l'art. 89, par. 1, GDPR non definisca la natura delle garanzie¹¹⁰, ne chiarisce gli scopi: l'adozione di misure tecniche e organizzative in grado di garantire, in primo luogo, il rispetto del principio di minimizzazione, in conformità ai principi di proporzionalità e necessità¹¹¹. Il trattamento deve quindi essere progettato per utilizzare solo i dati strettamente necessari e, ove possibile, per ricorrere a quelli anonimi; laddove l'anonimizzazione non sia possibile¹¹², le garanzie possono¹¹³ includere la pseudonimizzazione, purché quest'ultima consenta di raggiungere le finalità della ricerca.

Il richiamo alle misure tecniche e organizzative contenuto nell'art. 89, par. 1, GDPR, si collega inoltre chiaramente all'art. 32 del GDPR, che regola la sicurezza dei dati. Le garanzie adeguate devono includere, altresì, ulteriori meccanismi di gestione del rischio, come la protezione dei dati fin dalla progettazione e per impostazione predefinita (*data protection by design e by default*) e l'esecuzione di una valutazione d'impatto¹¹⁴. Infine, specifiche garanzie aggiuntive possono essere previste dagli Stati membri¹¹⁵.

Questa disposizione riflette pertanto l'approccio "aperto" del GDPR, in linea con il principio di *accountability*, che impone ai titolari del trattamento un ruolo "proattivo" nella gestione dei dati personali, con

¹⁰⁹ La disposizione si applica anche al trattamento dei dati per scopi di archiviazione nel pubblico interesse, ricerca storica e fini statistici.

¹¹⁰ Al riguardo, l'EDPB ha confermato che l'attuale mancanza di indicazioni su cosa possa o debba essere considerato una garanzia adeguata ai sensi dell'art. 89, par. 1, GDPR rappresenta un ostacolo per un corretto utilizzo delle eccezioni previste per il trattamento dei dati personali a fini di ricerca scientifica. Per questo motivo, lo stesso organismo ha annunciato (ormai da tempo) l'elaborazione di precisi chiarimenti volti a individuare le misure e le procedure che possano ritenersi adeguate a tale scopo. Cfr. EUROPEAN DATA PROTECTION BOARD (EDPB), *Document on response*, cit., par. 52-56. V. anche S. ZIPPONI-G. MARMORATO, *Tutela dei dati personali nel settore della ricerca scientifica e delle sperimentazioni cliniche: la normativa comunitaria*, in L. BOLOGNINI-S. ZIPPONI (a cura di), *Privacy e diritto dei dati sanitari*, cit., 193 s., i quali evidenziano come l'incertezza in merito alle condizioni di garanzia da adottare crei una situazione di confusione nello svolgimento delle attività di ricerca scientifica.

¹¹¹ Cfr. il considerando n. 156 del GDPR.

¹¹² In merito alle difficoltà pratiche di assicurare l'effettiva anonimizzazione dei dati nell'attuale contesto tecnologico e informatico, si veda quanto evidenziato sopra, par. 2.

¹¹³ Al riguardo v., tra gli altri, A. MACINATI, sub art. 89, in L. BOLOGNINI-E. PELINO (diretto da), *Codice della disciplina privacy*, Giuffrè, Milano, 2024, 431, dove si osserva come l'adozione dei dati "in chiaro" possa essere un'opzione praticabile, non subordinata alla pseudonimizzazione, nei casi in cui l'anonimizzazione impedisca il raggiungimento delle finalità. In ogni caso, in tali circostanze, il trattamento dei dati sarà consentito previa adozione di misure adeguate, diverse dalla pseudonimizzazione, che garantiscano, tra l'altro, il rispetto del principio di minimizzazione. V. anche A. BERNES, *La protezione*, cit., 200, il quale evidenzia come la disposizione in esame richieda di procedere attraverso dei «cerchi concentrici».

¹¹⁴ Sia l'art. 89, par. 1, sia i considerando nn. 156 e 159 del Regolamento, nel menzionare la necessità di garanzie adeguate al trattamento dei dati nel campo della ricerca, precisano che tali garanzie devono essere attuate in conformità al Regolamento. Questo suggerisce, dunque, l'esigenza di applicare tutti i meccanismi di tutela previsti dalla normativa, tenendo conto delle ulteriori cautele richieste dai particolari tipi di dati trattati.

¹¹⁵ Cfr. il considerando n. 156. In questo senso, tra gli altri, R. DUCATO, sub art. 89, cit., 968. In proposito, v. anche E. KINDT-C.A. FONTANILLO LÓPEZ-J. CZARNOCKI, et al., *Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research. Final Report (EDPS/2019/02-08)* (su commissione dell'European data protection Board), 2021, 9 s., disponibile all'indirizzo: <https://www.edpb.europa.eu>.



l'adozione di tutte le misure necessarie per garantire una tutela preventiva e continua durante l'intero ciclo di vita del trattamento¹¹⁶.

La conclusione che si può trarre dall'analisi della disciplina prevista dal Regolamento per la ricerca scientifica è pertanto che, sebbene questa possa rappresentare un "alleggerimento" rispetto al rigido quadro normativo sul trattamento dei dati sanitari, le preoccupazioni su un presunto "privilegio eccessivo" non appaiono del tutto giustificate. Il Regolamento impone, infatti, limiti e condizioni, insieme all'adozione di misure adeguate per prevenire, per quanto possibile, pregiudizi ai diritti degli interessati¹¹⁷. Anche in questo contesto si conferma, dunque, l'approccio generale della normativa, basato sull'equilibrio tra interessi contrapposti¹¹⁸. In particolare, di fronte ai limiti e alle nuove esigenze derivanti dall'attuale scenario tecnologico-informatico, che interessano anche il settore della ricerca scientifica, il legislatore garantisce la tutela dell'individuo non più solo attraverso l'autodeterminazione, ma mediante un sistema di responsabilità e gestione del rischio imposto a chi tratta i dati¹¹⁹.

3.3. – Se quella delineata sopra rappresenta la principale composizione degli interessi delineata dal Regolamento, l'effettivo punto di equilibrio tra interessi individuali e interessi collettivi, sottesi alla ricerca scientifica in ambito sanitario, è inevitabilmente influenzato dall'attuazione pratica di tale quadro normativo da parte degli Stati membri. Anche¹²⁰ a causa della limitata competenza dell'Unione Europea in questo ambito¹²¹, il Regolamento riconosce, infatti, agli Stati membri una significativa autonomia regolatoria, permettendo loro di mantenere o introdurre ulteriori condizioni¹²².

La prima area di discrezionalità nazionale emerge dall'art. 9, par. 4, GDPR, che autorizza gli Stati membri a mantenere o stabilire ulteriori previsioni, incluse restrizioni, per quanto riguarda il trattamento dei dati genetici, biometrici e relativi alla salute¹²³. Questo margine di autonomia è ulteriormente delineato dall'art.

¹¹⁶ Il rischio legato all'uso delle informazioni personali e la sua gestione rappresentano un elemento centrale della disciplina sulla protezione dei dati fin dalle sue origini. Tuttavia, nel corso degli anni, le risposte del legislatore sono variate in funzione delle specifiche tipologie di rischi che si presentavano. Ciò che distingue il Regolamento dal quadro normativo precedente è un cambiamento di *focus*: non più prevalentemente incentrato sulla legittimità del trattamento e sull'autodeterminazione dell'interessato, ma piuttosto orientato verso i profili di *accountability* e di gestione del rischio. In proposito, v., A. MANTELETO, *La gestione del rischio*, in G. FINOCCHIARO (opera diretta da) *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018*, n. 101, cit., 473 ss.; G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 1, 10 ss.

¹¹⁷ Condividono tale soluzione, tra gli altri, R. BECKER-D. CHOKOSHVILI-G. COMANDÉ, et al., *Secondary use*, cit., 155; M. SHABANI-S. YILMAZ, *Lawfulness*, cit., 130. V., inoltre, EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), *A Preliminary Opinion*, cit., 11, ove si evidenzia come l'obiettivo sia quello di individuare un "fair balance" tra gli interessi individuali e quelli sottesi alla ricerca scientifica.

¹¹⁸ V. sopra, *sub par.* 3.

¹¹⁹ V. sopra, *sub nt.* 116.

¹²⁰ Gli spazi di manovra concessi agli Stati membri nel GDPR riflettono anche la natura compromissoria che caratterizza molte volte i regolamenti europei su materie di ampia portata, dove spesso emergono divergenze significative tra le posizioni dei singoli Stati membri.

¹²¹ Cfr., tra gli altri, art. 4, par. 2, lett. *k* e par. 3 e art. 168 TFUE. In dottrina, tra gli altri, F. SCIALOIA, *L'Unione Europea apre la strada alla creazione dello spazio europeo dei dati sanitari*, in V. SALVATORE (a cura di), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Giappichelli, Torino, 2023, 204 ss.

¹²² V. anche il considerando n. 10 del GDPR.

¹²³ Al riguardo, sulla base di questo spazio di manovra, il legislatore italiano, in sede di adeguamento alla disciplina europea, aveva modificato l'art. 110 del Codice della Privacy (d.lgs. n. 196/2003). La nuova formulazione escludeva la necessità del consenso per il trattamento dei dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, tra l'altro, quando, per particolari ragioni, informare gli interessati risultava impossibile, comportava uno sforzo sproporzionato, o rischiava di com-



89, par. 2, GDPR, che, con riferimento ai trattamenti a fini di ricerca scientifica¹²⁴, consente agli Stati membri¹²⁵ di prevedere limitazioni specifiche all'esercizio di alcuni diritti degli interessati, oltre a quelle già stabilite dal Regolamento¹²⁶, nella misura in cui l'esercizio di tali diritti possa compromettere gravemente o rendere impossibile il conseguimento delle finalità della ricerca e tali deroghe siano necessarie al raggiungimento di questi obiettivi. In particolare, possono essere introdotte deroghe ai diritti di accesso (art. 15), rettifica (art. 16), limitazione del trattamento (art. 18) e opposizione (art. 21), con l'obbligo di stabilire adeguate garanzie per assicurare la tutela dei diritti e delle libertà degli interessati¹²⁷, in conformità ai principi generali del GDPR.

Le disposizioni sopra citate rappresentano le principali possibilità di intervento riservate agli Stati membri in materia di ricerca scientifica, ma altre norme del Regolamento offrono ulteriori spazi di flessibilità, rilevanti anche per questo contesto. Tuttavia, l'ampio ricorso a margini di discrezionalità nazionale ha finito per vanificare l'intento di uniformazione¹²⁸ che il Regolamento si proponeva di raggiungere¹²⁹, creando una frammentazione normativa che ostacola la ricerca scientifica, soprattutto a livello transnazionale¹³⁰.

A distanza di oltre sei anni dall'entrata in vigore della normativa, molte delle preoccupazioni iniziali riguardanti il suo impatto sulla ricerca scientifica si sono, di fatto, concretizzate. L'applicazione della disciplina si è rivelata, infatti, un mosaico particolarmente complesso per i ricercatori¹³¹ e, in assenza di ampi database e di un ambiente normativo favorevole, essenziali anche per lo sviluppo di sistemi di intelligenza artificiale in medicina, molti studiosi si rivolgono a imprese che raccolgono dati in grandi quantità situate al di

promettere gravemente le finalità della ricerca. Tuttavia, in tali casi, la norma richiedeva, oltre all'adozione di misure appropriate per tutelare gli interessati e il parere favorevole del comitato etico, anche la consultazione preventiva dell'Autorità garante. Questo approccio è stato oggetto di critiche per l'eccessiva rigidità introdotta, poiché di fatto introduceva un'ulteriore base giuridica rispetto a quelle già previste dal GDPR, generando potenziali ostacoli alla ricerca, soprattutto in ambito transnazionale. Cfr., tra gli altri, L. Bolognini-S. Zippone, *Tutela dei dati personali*, cit., 208 ss.; G. Comandé, *Ricerca*, cit., 204 s. In risposta a tali criticità, la legge 29 aprile 2024, n. 56, di conversione del d.l. 2 marzo 2024, n. 19, ha modificato nuovamente l'art. 110, eliminando l'obbligo di consultazione preventiva del Garante. V., inoltre, l'art. 2-septies, inserito con il d.lgs. n. 101/2018.

¹²⁴ La disposizione riguarda anche la ricerca storica o a fini statistici.

¹²⁵ Più precisamente, ai sensi dell'art. 89, par. 2, GDPR, le deroghe all'esercizio di alcuni diritti degli interessati possono essere stabilite non solo dal diritto degli Stati membri, ma anche dal diritto dell'Unione Europea.

¹²⁶ Con riferimento ai limiti già previsti dal Regolamento, v. sopra par. 3.2.

¹²⁷ Le garanzie sono quelle richieste dall'art. 89, par. 1, GDPR, le quali rappresentano, dunque, una tutela fondamentale per garantire il corretto bilanciamento degli interessi coinvolti.

¹²⁸ V., inoltre, R. Ducato, sub art. 89, cit., 975 e M.C. Daga, *Le disposizioni relative a specifiche situazioni di trattamento: l'attività di archiviazione e ricerca, il segreto professionale e le associazioni religiose*, in G. Finocchiaro (opera diretta da) *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018*, n. 101, cit., 928, le quali osservano come il rischio di frammentazione sia ulteriormente acuito dal fatto che, diversamente da quanto previsto, ad esempio, per i trattamenti di cui agli artt. 85 e 88 del GDPR, gli Stati membri non sono tenuti a notificare alla Commissione le norme che stabiliscono le deroghe ai diritti degli interessati ai sensi dell'art. 89, par. 2, GDPR, impedendo così a quest'ultima di intervenire in caso di contrasto tra le previsioni nazionali in corso di emanazione e il GDPR.

¹²⁹ Tale intento emerge, del resto, dalla scelta dello strumento regolamentare. Cfr. anche i considerando nn. 9, 10 e 13, GDPR. In argomento v., per tutti, G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 1, 5 s.

¹³⁰ La frammentazione delle normative nazionali è stata evidenziata anche da alcuni studi commissionati dalle autorità europee per valutare le regole adottate in materia di dati sanitari alla luce del GDPR. Tali studi hanno rivelato notevoli divergenze nell'interpretazione e nell'applicazione del Regolamento, in particolare per quanto riguarda l'accesso e l'uso dei dati sanitari per scopi di ricerca, nonché le garanzie per la tutela dei diritti degli interessati. V., ad esempio, J. Hansen-P. Wilson-E. Verhoeven, et al. (su commissione della European Commission-Consumers, Health, Agriculture and Food Executive Agency), *Assessment of the EU Member States' rules on health data in the light of GDPR*, 2021, disponibile all'indirizzo <https://data.europa.eu>; E. Kindt-C.A. Fontanillo López-J. Czarnocki, et al. (su commissione dell'European Data Protection Board), *Study*, cit.

¹³¹ Definito alla stregua di un "puzzle" da G. Comandé, *Ricerca*, cit., 207.



fuori dell'Unione Europea, dove il sistema è meno regolamentato¹³².

Il “sistema giuridico multilivello”¹³³ delineato per la ricerca scientifica ha inoltre sollevato rilevanti criticità in termini di collaborazione transazionale. La ricerca scientifica collaborativa presuppone, infatti, lo scambio transfrontaliero di dati, un processo già complicato dalle disposizioni del Regolamento e ulteriormente aggravato dalla frammentazione delle normative nazionali. Tale situazione limita, pertanto, la realizzazione di progetti di ricerca internazionali e può influenzare le scelte strategiche relative ai partner dei consorzi¹³⁴.

Le difficoltà nella condivisione dei dati sono emerse in modo particolarmente evidente durante la pandemia di COVID-19, quando lo scambio dei dati sanitari per la ricerca in ambito di salute pubblica ha incontrato numerosi ostacoli a causa delle divergenze normative tra i vari Stati membri¹³⁵. Questo ha dimostrato come un contesto normativo frammentato all'interno dell'Unione possa ostacolare le attività di ricerca transazionale, con conseguenze significative sulla tutela della salute della collettività, sottolineando, di conseguenza, la necessità di un maggiore coordinamento normativo.

In risposta a tali sfide, l'Unione Europea si sta orientando verso la creazione di un contesto sicuro per la ricerca, favorendo un accesso e una condivisione più ampi dei dati sanitari attraverso un'integrazione tra il GDPR, la normativa sullo Spazio Europeo dei Dati Sanitari e quella sull'intelligenza artificiale¹³⁶.

4. – Le problematiche relative all'utilizzo dei dati sanitari a fini di ricerca scientifica e alla loro circolazione, anche a livello transfrontaliero, evidenziate nel paragrafo precedente, hanno sottolineato la necessità di un sistema più coerente, uniforme e integrato, per promuovere l'impiego di tali dati garantendo al contempo il rispetto dei diritti fondamentali degli individui¹³⁷. In risposta a queste criticità, nel maggio del 2022, la Commissione Europea ha presentato una proposta di Regolamento volta a istituire uno Spazio Europeo dei Dati Sanitari (*European Health Data Space – EHDS*)¹³⁸, un quadro normativo specificamente concepito per superare le difficoltà tecniche e regolatorie legate all'uso dei dati sanitari, in particolare per l'assistenza sanitaria e la ricerca scientifica¹³⁹. Lo scopo è quello di creare un ambiente comune per la condivisione delle in-

¹³² V. anche K. PORMEISTER, *Genetic data*, cit., 140, il quale aveva segnalato il rischio di *forum shopping* verso le legislazioni più favorevoli alla ricerca.

¹³³ In questo senso, tra gli altri, M.L. MANIS, *The processing*, cit., 326; M.C. SPENA, *La salute*, cit., 104. In generale, v. anche G. DI FEDERICO, *Fundamental Rights in the EU: Legal Pluralism and Multi-Level Protection after the Lisbon Treaty*, in D. GIACOMO (a cura di), *The EU Charter of Fundamental Rights. Ius Gentium: Comparative Perspectives on Law and Justice*, Springer, 2011, 15 ss.

¹³⁴ In argomento, v. anche T. SOKOL, *European Health Data Space, Use of Data and Data Subjects' Control over Their Own Health Data: Can an Opt-Out Restore the Balance?*, in *European Journal of Health Law*, 2024, 7; R. DUCATO, sub art. 89, cit., 974; E.B. VAN VEEN, *Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate*, in *European Journal of Cancer*, 2018, 75.

¹³⁵ Al riguardo, v., tra gli altri, P. TERZIS, *Compromises and asymmetries in the European Health Data Space*, in *European Journal of Health Law*, 2023, 347; R. BECKER-A. THOROGOOD-J. ORDISH, et al., *COVID-19 Research: Navigating the European General Data Protection Regulation*, in *Journal of Medical Internet Research*, 2020, 8, 4.

¹³⁶ Cfr. EUROPEAN COMMISSION, *European Health Union: A European Health Data Space for people and science*, 3 maggio 2022, disponibile all'indirizzo <<https://ec.europa.eu>>.

¹³⁷ Cfr. EUROPEAN COMMISSION, *Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, COM(2022) 197 final, SWD(2022) 131 final, 3 maggio 2022.

¹³⁸ EUROPEAN COMMISSION, *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space* (COM/2022/197 final), 3 maggio 2022.

¹³⁹ Da qui, anche la scelta dello strumento giuridico adottato, il Regolamento anziché la Direttiva, per garantire un'applicazione



formazioni sanitarie in Europa, dove cittadini, ricercatori, innovatori e decisori politici possano accedere e condividere queste risorse in modo sicuro e trasparente ¹⁴⁰.

In particolare, il Regolamento, prossimo all'adozione definitiva nel momento in cui si scrive ¹⁴¹, persegue due obiettivi principali ¹⁴². Da un lato, mira a rafforzare il controllo dei cittadini sui propri dati sanitari, facilitandone lo scambio per garantire la continuità dell'assistenza sanitaria in tutto il territorio dell'Unione. L'EHDS intende infatti creare un'infrastruttura che consenta a cittadini e operatori sanitari di accedere facilmente ai dati sanitari in formato elettronico, riconosciuto e accettato in tutta l'Unione Europea, facilitando così la continuità delle cure anche al di fuori del Paese di residenza.

Dall'altro lato, un obiettivo centrale dell'EHDS è quello di istituire un sistema coerente, affidabile ed efficiente per il riutilizzo dei dati sanitari in ambiti quali la ricerca scientifica, lo sviluppo e l'innovazione di prodotti e servizi, la formulazione di politiche sanitarie, la sicurezza dei pazienti e altre attività di interesse pubblico. Per raggiungere questo obiettivo, la nuova normativa stabilisce procedure centralizzate per garantire l'accesso a varie categorie di dati sanitari elettronici, imponendo ai soggetti detentori di questi dati l'obbligo di metterli a disposizione. Il Regolamento affronta in tal modo le problematiche interpretative e di frammentazione emerse nell'ambito del GDPR in relazione all'uso secondario dei dati sanitari, soprattutto per scopi di ricerca scientifica, introducendo un meccanismo comune di accesso ai dati in tutto il territorio europeo. Quest'ultimo aspetto risulta, dunque, particolarmente delicato, poiché implica un necessario bilanciamento tra la protezione dei diritti individuali e l'interesse collettivo a favore della salute pubblica e dell'innovazione.

In questa prospettiva, che comprende sia il rafforzamento del controllo dei cittadini sui propri dati sanitari sia l'istituzione di un sistema efficiente per il riutilizzo dei dati, il Regolamento distingue tra l'uso primario ¹⁴³ e secondario ¹⁴⁴ dei dati sanitari elettronici, riservando a ciascun ambito una disciplina specifica. Ai fini

omogenea della normativa e creare un clima di fiducia necessario ad assicurare il più ampio accesso e una condivisione diffusa dei dati sanitari elettronici (v. la Relazione che accompagna il testo della proposta di Regolamento). La nuova normativa si colloca nel più ampio contesto della strategia europea per i dati, adottata dalla Commissione Europea nel febbraio 2020, con l'obiettivo di creare uno spazio unico europeo per i dati, agevolando lo scambio e l'utilizzo dei dati in settori strategici, quali l'industria, l'energia, l'ambiente e la salute. Cfr. EUROPEAN COMMISSION, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data*, COM(2020) 66 final, 19 febbraio 2020.

¹⁴⁰ Cfr. EUROPEAN COMMISSION, *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, cit., *Explanatory Memorandum*, 1. La disciplina proposta si basa e integra il GDPR e interagisce con altre normative pertinenti, tra cui il Data Governance Act, il Data Act, e la normativa sull'intelligenza artificiale. Inoltre, il Regolamento non pregiudica altre normative rilevanti, come quelle relative alla sicurezza dei dispositivi medici e dei dispositivi medico-diagnostici in vitro.

¹⁴¹ Dopo la fase di trilatero tra i rappresentanti del Parlamento europeo, del Consiglio dell'Unione Europea e della Commissione europea, nel mese di aprile 2024 il testo del Regolamento è stato definitivamente approvato dal Parlamento Europeo. La pubblicazione del testo sulla Gazzetta Ufficiale dell'Unione Europea è prevista entro la fine del 2024, previa revisione linguistica e sistemazione della numerazione degli articoli. Per questo motivo, gli articoli citati nel presente contributo in merito al testo definitivo si riferiscono al testo approvato nell'aprile 2024 e potrebbero subire modifiche nella numerazione.

¹⁴² Cfr. il considerando n. 1, EUROPEAN PARLIAMENT, *Legislative Resolution of 24 April 2024 on the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, COM(2022) 0197 – C9-0167/2022 – 2022/0140(COD), 24 aprile 2024 (d'ora innanzi, per brevità: EHDS, testo adottato). Un ulteriore obiettivo perseguito è quello di migliorare il funzionamento del mercato interno, mediante la creazione di un quadro giuridico e tecnico uniforme, in particolare per lo sviluppo e la commercializzazione di sistemi di cartelle cliniche elettroniche.

¹⁴³ Per «uso primario» si intende l'accesso ai dati sanitari da parte degli operatori allo scopo di fornire assistenza sanitaria (cfr. art. 2, par. 2, lett. d, EHDS, testo adottato).

¹⁴⁴ Inteso, dunque, nella sua ultima formulazione, come il riutilizzo dei dati sanitari elettronici per le finalità indicate nel Capitolo IV del Regolamento, differenti da quelle iniziali per cui sono stati raccolti (sia nel contesto dell'uso primario che in quello dell'uso secondario) (cfr. art. 2, par. 2, lett. e, EHDS, testo adottato). La definizione iniziale di uso secondario è stata oggetto di numerose critiche. Nella Proposta presentata dalla Commissione, l'uso secondario faceva infatti riferimento all'impiego dei dati per le finalità in-



dell'indagine oggetto del presente contributo, l'attenzione si concentra sugli aspetti principali della disciplina dell'uso secondario dei dati, per verificare in che modo sia stato raggiunto l'equilibrio tra la tutela degli interessi individuali e la promozione della ricerca scientifica, e quali implicazioni ne derivino.

A tale riguardo, come si avrà modo di illustrare, la prima proposta presentata dalla Commissione europea, pur accolta positivamente per l'intento di promuovere un quadro giuridico unitario per la circolazione dei dati sanitari, aveva sollevato diverse critiche¹⁴⁵. Una delle questioni più controverse¹⁴⁶ riguardava il livello di controllo che gli interessati avrebbero dovuto mantenere sull'uso secondario dei propri dati sanitari nell'ambito dell'EHDS. Il testo iniziale aveva introdotto, infatti, significativi squilibri tra l'autodeterminazione degli interessati e la necessità di riutilizzare i dati raccolti per finalità diverse. Durante il processo di approvazione, il testo è stato oggetto di numerose modifiche, che hanno portato alla versione approvata dal Parlamento Europeo nell'aprile 2024. Nonostante alcune criticità permangano¹⁴⁷, questa versione rappresenta un significativo progresso nel bilanciare gli interessi individuali e collettivi, in particolare riguardo all'uso secondario dei dati sanitari per la ricerca scientifica.

L'uso dei dati sanitari elettronici per scopi secondari è disciplinato nel capitolo IV, il quale affronta diversi aspetti, come le categorie minime di dati che devono essere messi a disposizione per usi secondari, gli scopi per cui i dati possono essere utilizzati e le finalità vietate, nonché i meccanismi di accesso a livello nazionale ed europeo e gli organismi preposti.

In questo contesto, l'art. 33 stabilisce le categorie minime di dati sanitari elettronici che devono essere rese disponibili dai titolari dei dati¹⁴⁸ per l'uso secondario, tra cui rientra, dunque, la ricerca scientifica. Le categorie indicate sono molto ampie e comprendono, ad esempio, dati provenienti da cartelle cliniche elettroniche, dati sui fattori che influenzano la salute (quali determinanti sociali, ambientali e comportamentali), dati genetici, dati raccolti tramite dispositivi medici e quelli conservati nelle biobanche. Complessivamente, tali categorie coprono un'ampia gamma di dati provenienti da fonti diverse, includendo sia dati dell'amministrazione sanitaria e della salute pubblica, sia dati raccolti da fonti personali o volontarie, come dispositivi indossabili (*wearable*) e le relative applicazioni per il benessere¹⁴⁹. La flessibilità delle categorie di dati di-

dicato nel Capitolo IV, come la ricerca scientifica o lo sviluppo di prodotti e servizi, senza richiamare il concetto di riuso per finalità diverse. Questo approccio si basava sull'idea, in realtà presente anche nel testo finale, che i dati sanitari elettronici avessero primariamente uno scopo medico e che, quindi, il loro uso principale fosse quello sanitario. Tuttavia, ciò creava confusione rispetto al GDPR, il quale non prevede una distinzione simile, ma utilizza il concetto di "ulteriore trattamento dei dati" per indicare il riutilizzo dei dati per scopi diversi da quelli originari (v. sopra, *sub* par. 3.1). Con riferimento ai dubbi sollevati dalla definizione iniziale, cfr. EUROPEAN DATA PROTECTION BOARD e EUROPEAN DATA PROTECTION SUPERVISOR, *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*, 12 luglio 2022, par. 42.

¹⁴⁵ V., ad esempio, EUROPEAN DATA PROTECTION BOARD e EUROPEAN DATA PROTECTION SUPERVISOR, *EDPB-EDPS Joint Opinion 03/2022*, cit. In dottrina, M. SHABANI-S. YILMAZ, *Lawfulness*, cit., 133 s.; S. SLOKENBERGA, *Scientific Research*, cit., 146 s.; T. SOKOL, *European Health Data Space*, cit., 11 ss.

¹⁴⁶ Un'ulteriore criticità emersa riguarda, come detto (v. nt. 144), le definizioni proposte. Molte delle definizioni introdotte dalla Proposta, così come numerose delle sue disposizioni, non risultavano infatti armonizzate con quelle già presenti nel GDPR e in altre normative pertinenti, come il Data Governance Act e il Data Act, generando un quadro normativo incerto e di difficile applicazione. Al riguardo, v. EUROPEAN DATA PROTECTION BOARD e EUROPEAN DATA PROTECTION SUPERVISOR, *EDPB-EDPS Joint Opinion 03/2022*, cit.

¹⁴⁷ Le quali meriterebbero un'analisi separata e, pertanto, non vengono trattate nel presente contributo.

¹⁴⁸ Cfr. la definizione contenuta all'art. par. 2, lett. y, EHDS, testo adottato. Tra i soggetti che possono assumere la qualifica di titolari dei dati sanitari vi sono, tra l'altro, persone fisiche o giuridiche, autorità pubbliche, agenzie o altri organismi operanti nel settore sanitario o assistenziale, nonché persone fisiche e giuridiche che svolgono attività di ricerca o sviluppano prodotti e servizi destinati a tali settori, o che sviluppano e producono applicazioni per il benessere. Il considerando n. 40 del Regolamento precisa, inoltre, che tali soggetti possono essere enti pubblici, privati o senza scopo di lucro.

¹⁴⁹ Al riguardo, v. EUROPEAN DATA PROTECTION BOARD e EUROPEAN DATA PROTECTION SUPERVISOR, *EDPB-EDPS Joint Opinion*



spionabili per l'uso secondario risponde alle esigenze, in continua evoluzione, degli utenti dei dati e mira ad ampliare le risorse comuni¹⁵⁰. Inoltre, gli Stati membri possono introdurre ulteriori categorie di dati da rendere disponibili per l'uso secondario¹⁵¹.

Il Regolamento individua anche le finalità per le quali è consentito l'uso secondario dei dati sanitari elettronici¹⁵². Tra queste rientrano, tra le altre, il perseguimento dell'interesse pubblico nel settore della salute pubblica e professionale, lo sviluppo di politiche, l'elaborazione di statistiche e le attività di istruzione e formazione in ambito sanitario o assistenziale. È inoltre espressamente menzionata la finalità di ricerca scientifica relativa ai settori della salute e dell'assistenza, volta a contribuire alla salute pubblica, alla valutazione delle tecnologie sanitarie o al mantenimento di elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, a beneficio degli utenti finali, come pazienti, operatori sanitari e amministratori della sanità. Questa finalità di ricerca scientifica comprende anche lo sviluppo e l'innovazione di prodotti e servizi, nonché la formazione e la valutazione di algoritmi, inclusi quelli utilizzati in dispositivi medici, dispositivi diagnostici in vitro, sistemi di intelligenza artificiale e applicazioni di salute digitale.

La definizione di un elenco vincolante delle finalità per cui i dati possono essere trattati per scopi di uso secondario, accompagnata dalla precisazione che tali finalità devono contribuire all'interesse generale della società¹⁵³, è di particolare rilievo, tenuto conto dell'ampia platea di soggetti, sia pubblici che privati, che possono richiedere l'accesso a tali dati¹⁵⁴.

Oltre alle finalità consentite, il Regolamento precisa una serie di finalità espressamente vietate per l'uso secondario dei dati sanitari elettronici, come l'adozione di decisioni potenzialmente dannose per le persone fisiche cui tali dati si riferiscono¹⁵⁵ e le attività pubblicitarie e di *marketing*¹⁵⁶, contribuendo così a definire

03/2022, cit., par. 80, dove erano state espresse preoccupazioni riguardo all'inclusione dei dati provenienti da applicazioni per il benessere, evidenziando i rischi legati all'affidabilità e accuratezza di tali dati, nonché ai possibili usi impropri per finalità di profilazione o non trasparenti.

¹⁵⁰ Cfr. considerando n. 39, EHDS, testo adottato. V., inoltre, quanto osservato da P. TERZIS, *Compromises*, cit., 348 s, il quale evidenzia come l'ampio spettro di categorie di dati sanitari che possono essere trattati per uso secondario si giustifichi nel contesto della strategia dell'UE per la trasformazione digitale. Nell'ambito di questo progetto, il Regolamento mira ad ampliare le risorse comuni di dati, includendo non solo dati amministrativi, dati da dispositivi medici e dati genomici, ma anche, tra l'altro, dati elettronici provenienti da applicazioni digitali per la salute, oltre a dati relativi allo stato professionale, occupazionale e allo stile di vita.

¹⁵¹ Art. 33, par. 8, EHDS, testo adottato.

¹⁵² Cfr. art. 34, EHDS, testo adottato.

¹⁵³ Cfr. anche il considerando n. 41, EHDS, testo adottato. In particolare, per quanto riguarda il trattamento dei dati sanitari elettronici per finalità di ricerca e sviluppo, il testo finale della nuova normativa chiarisce che tale attività è ammessa solo se volta a generare benefici concreti per la società, come una maggiore disponibilità e accessibilità a farmaci, dispositivi medici e servizi sanitari, contribuendo così alla salute pubblica. Questa precisazione è fondamentale per prevenire l'uso improprio dei dati per fini puramente commerciali, non in linea con l'interesse pubblico e, di conseguenza, per mantenere un equilibrio tra gli obiettivi del Regolamento e la tutela dei soggetti coinvolti. L'esigenza di collegamento con la salute pubblica e la sicurezza sociale era stata altresì evidenziata dall'EDPB e dall'EDPS nella valutazione della Proposta iniziale: cfr. EUROPEAN DATA PROTECTION BOARD e EUROPEAN DATA PROTECTION SUPERVISOR, *EDPB-EDPS Joint Opinion 03/2022*, cit., par. 85. Inoltre, la precisazione risulta maggiormente in linea con l'eccezione contenuta nell'art. 9, par. 1, lett. j, GDPR.

¹⁵⁴ Cfr. anche il considerando n. 41, EHDS, testo adottato, in cui si chiarisce che il concetto di finalità di ricerca scientifica dovrebbe essere interpretato in senso ampio, includendo, tra l'altro, lo sviluppo tecnologico, la dimostrazione, la ricerca applicata e quella finanziata privatamente. Al riguardo, v. anche T. SOKOL, *European Health Data Space*, cit., 12; P. TERZIS, *Compromises*, cit., 354 s.

¹⁵⁵ Si osservi che, all'interno del cap. IV, dedicato all'uso secondario dei dati, il Regolamento non fa riferimento alle "persone interessate" ai sensi del GDPR, bensì alle persone fisiche, le quali possono coincidere o meno con i soggetti cui i dati sanitari si riferiscono. Questa scelta terminologica si giustifica in quanto l'approccio privilegiato all'interno dell'EHDS per gli usi secondari prevede la completa anonimizzazione dei dati (a questo proposito, si veda oltre). In particolare, il Regolamento considera sia i dati sanitari elettronici non personali che quelli personali.

¹⁵⁶ Cfr. art. 35 e il considerando n. 41aa, EHDS, testo adottato.



con maggiore chiarezza ciò che costituisce un utilizzo lecito dei dati sanitari per tale scopo¹⁵⁷.

Come anticipato, per l'accesso e l'uso secondario dei dati sanitari a livello europeo, il Regolamento introduce un meccanismo strutturato e armonizzato volto a garantirne un impiego sicuro e controllato¹⁵⁸. Questo sistema facilita la condivisione delle informazioni, assicurando al contempo un elevato livello di protezione. In questo contesto, un ruolo centrale è affidato agli organismi di accesso ai dati¹⁵⁹, mentre ruoli di rilievo sono assegnati anche ai titolari dei dati¹⁶⁰ e agli utenti dei dati¹⁶¹.

Per riassumere il funzionamento di questo meccanismo, gli organismi di accesso ai dati, istituiti a livello nazionale, sono responsabili del coordinamento e della gestione delle richieste di accesso ai dati sanitari elettronici per usi secondari, presentate dagli utenti dei dati. Questi organismi valutano le domande di accesso, verificando la conformità dell'uso proposto con le finalità autorizzate dal Regolamento e che siano adottate tutte le garanzie necessarie per la protezione dei dati. Nel caso in cui la richiesta venga approvata, il titolare dei dati interessato¹⁶² è tenuto a fornire i dati all'organismo di accesso¹⁶³, il quale li rende disponibili all'utente tramite una piattaforma centralizzata e sicura¹⁶⁴. L'accesso ai dati avviene, dunque, attraverso queste piattaforme nazionali, progettate per garantire che i dati siano accessibili solo agli utenti autorizzati e che tutte le operazioni siano tracciabili e protette¹⁶⁵. Inoltre, per facilitare l'accesso ai dati per uso secondario tra i diversi Stati membri, è prevista la creazione di HealthData@EU¹⁶⁶, un'infrastruttura che collegherà i "Punti

¹⁵⁷ V. anche M. SHABANI-S. YILMAZ, *Lawfulness*, cit., 132.

¹⁵⁸ Con riferimento al funzionamento del meccanismo proposto, v., più ampiamente, P. TERZIS, *Compromises*, cit., 349 ss.

¹⁵⁹ Cfr. considerando nn. 42-44 e art. 36, EHDS, testo adottato. Gli organismi di accesso ai dati sanitari sono istituiti da ogni Stato membro per autorizzare e regolamentare l'accesso ai dati sanitari per scopi di uso secondario in ambienti sicuri.

¹⁶⁰ V. sopra nt. 148.

¹⁶¹ Cfr. la definizione contenuta all'art. par. 2, lett. z, EHDS, testo adottato. Tra i soggetti che possono avere accesso ai dati sanitari elettronici vi sono persone fisiche e giuridiche, comprese le istituzioni, gli organismi e le agenzie dell'Unione. In particolare, il considerando n. 41 include enti pubblici, privati e senza scopo di lucro, nonché singoli ricercatori.

¹⁶² I titolari dei dati devono comunicare all'organismo responsabile dell'accesso ai dati sanitari una descrizione generale delle serie di dati in loro possesso. Sulla base delle informazioni ricevute, l'organismo pubblica un catalogo delle serie di dati disponibili a livello nazionale, con informazioni dettagliate sulle serie e sulle loro caratteristiche, affinché gli utenti possano valutare la rilevanza dei dati rispetto alle finalità che intendono perseguire (cfr. artt. 41 e 55, EHDS, testo adottato).

¹⁶³ Nella versione iniziale della Proposta, se la richiesta riguardava un singolo titolare in uno Stato membro, gli utenti potevano presentarla direttamente a quest'ultimo, il quale poteva rilasciare l'autorizzazione. Tuttavia, nel testo finale, è stata prevista una maggiore centralizzazione delle richieste attraverso gli organismi di accesso ai dati sanitari (cioè anche con riferimento alla procedura semplificata prevista ora dall'49, EHDS, testo adottato). Questa modifica sembra rispondere all'obiettivo di standardizzare e monitorare l'accesso ai dati, assicurando una maggiore coerenza tra i vari Stati membri e una protezione dei dati più solida.

¹⁶⁴ Per quanto concerne l'esigenza di garantire la protezione dei dati sanitari elettronici messi a disposizione attraverso la piattaforma dell'organismo responsabile, il Regolamento impone l'adozione di specifiche misure tecniche e organizzative, inclusi controlli periodici per verificarne l'efficacia. Inoltre, al fine di assicurare la massima sicurezza dei dati sanitari e la tutela dei diritti delle persone coinvolte, gli organismi devono limitare l'accesso esclusivamente ai dati pertinenti e strettamente necessari per il raggiungimento degli obiettivi indicati dagli utenti al momento della richiesta, in conformità ai principi di minimizzazione e limitazione delle finalità: cfr. artt. 44 e 50, EHDS, testo adottato.

¹⁶⁵ Al fine di assicurare il corretto utilizzo dei dati oggetto di accesso, in caso di inosservanza degli obblighi da parte dell'utente dei dati, gli organismi responsabili hanno il potere di revocare l'autorizzazione concessa e di interrompere il trattamento dei dati sanitari elettronici effettuato dallo stesso. Inoltre, tali organismi possono escludere l'utente da qualsiasi accesso ai dati sanitari elettronici per uso secondario nell'ambito dell'EHDS per un periodo determinato. In aggiunta o in alternativa a queste misure, l'organismo responsabile dell'accesso può comminare sanzioni amministrative pecuniarie, con importi massimi particolarmente elevati in caso di violazioni gravi, come l'uso secondario dei dati per finalità vietate o la mancata osservanza del divieto di re-identificazione (cfr. artt. 43 e 43a, EHDS, testo adottato).

¹⁶⁶ Cfr. considerando n. 55b e art. 52, EHDS, testo adottato. L'HealthData@EU rappresenta l'infrastruttura transfrontaliera prevista per facilitare lo scambio e l'interoperabilità dei dati sanitari elettronici tra gli Stati membri dell'UE. La sua funzione primaria è consentire l'uso secondario dei dati sanitari in un ambiente sicuro e conforme, favorendo la cooperazione e l'integrazione a livello europeo.



di contatto” nazionali responsabili della disponibilità dei dati sanitari elettronici ¹⁶⁷, creando così un sistema di interoperabilità a livello europeo ¹⁶⁸.

Il Regolamento stabilisce, inoltre, in via prioritaria, che gli organismi di accesso mettano a disposizione i dati richiesti per usi secondari in forma anonima, vietando qualsiasi tentativo di re-identificare le persone fisiche cui tali dati si riferiscono ¹⁶⁹. Tuttavia, qualora l’utente dei dati dimostri l’impossibilità di raggiungere la finalità del trattamento con dati anonimizzati, può essere concesso l’accesso ai dati in forma pseudonimizzata, con la conseguente necessità di rispettare il GDPR e le relative basi giuridiche ¹⁷⁰.

4.1. – Come anticipato, uno dei temi più dibattuti durante l’approvazione della Proposta ha riguardato il ruolo degli interessati nel decidere sull’uso secondario dei propri dati sanitari, in particolare per quanto riguarda il consenso. L’approccio generale delineato dal Regolamento sullo Spazio Europeo dei Dati Sanitari, infatti, non richiede il consenso degli interessati per la condivisione dei dati per usi secondari, ma prevede altre basi giuridiche ai sensi dell’art. 6 del GDPR, da considerarsi in combinazione con le eccezioni al divieto di trattare categorie particolari di dati personali di cui all’art. 9, par. 2, GDPR.

Al riguardo, lo stesso Regolamento costituisce una base giuridica per l’uso secondario dei dati sanitari elettronici personali, comprese le garanzie necessarie per consentire il trattamento di particolari categorie di dati, in conformità con l’art. 9, par. 2, lett. *g, h, i e j*, GDPR (e pertanto rappresenta la legge dell’Unione ivi menzionata). Di conseguenza, agli Stati membri non è più consentito mantenere o introdurre ulteriori condizioni, comprese limitazioni e disposizioni specifiche che richiedono il consenso dell’interessato ¹⁷¹.

Al contempo, il Regolamento introduce un regime distinto di basi giuridiche per la condivisione dei dati a seconda del ruolo del soggetto che effettua il trattamento ¹⁷². I titolari dei dati, ad esempio, mettono a disposizione i dati agli organismi di accesso in adempimento di un obbligo legale imposto dal Regolamento in esame, ai sensi dell’art. 6, par. 1, lett. *c*, GDPR ¹⁷³, che si distingue, dunque, dalla base giuridica impiegata per legittimare il trat-

¹⁶⁷ Cfr. art. 52, EHDS, testo adottato. Si tratta di strutture organizzative e tecniche designate a livello nazionale, incaricate di rendere disponibili e facilitare l’accesso ai dati sanitari elettronici per l’uso secondario ai vari partecipanti autorizzati all’infrastruttura transfrontaliera HealthData@EU.

¹⁶⁸ La responsabilità operativa e gestionale di HealthData@EU sarà condivisa tra la Commissione Europea, che si occuperà del coordinamento generale e della supervisione, e gli Stati membri, che attraverso i loro organismi nazionali garantiranno il corretto funzionamento della piattaforma. Cfr. art. 52, EHDS, testo adottato.

¹⁶⁹ Al riguardo, il Regolamento riconosce che alcune categorie di dati sanitari elettronici possano essere considerate particolarmente sensibili, e quindi personali, anche se fornite in formato anonimo. In determinate circostanze, come nel caso di dati relativi a malattie rare o di piccole aree geografiche, anche l’uso di tecniche avanzate di anonimizzazione potrebbe non eliminare del tutto il rischio di re-identificazione, che rimane elevato. Di conseguenza, si richiede l’adozione di misure di protezione adeguate e proporzionate a tale rischio. In particolare, per i trasferimenti verso Paesi terzi, si delega alla Commissione il compito di individuare condizioni specifiche proporzionate al rischio di re-identificazione, tenendo conto delle specificità delle categorie di dati e delle tecniche di anonimizzazione o aggregazione utilizzate. In questo senso, v. il considerando n. 64, EHDS, testo adottato.

¹⁷⁰ Cfr. art. 44, parr. 2 e 3 e art. 46, par. 1, lett. *c*, EHDS, testo adottato. In tal caso, si prevede che solo l’organismo di accesso, o un organismo che agisca come terza parte fidata in conformità con la legislazione nazionale, possa avere accesso alle informazioni necessarie per invertire la pseudonimizzazione.

¹⁷¹ Tuttavia, agli Stati membri è consentito introdurre misure più rigorose e ulteriori garanzie a livello nazionale per tutelare la sensibilità e il valore dei dati appartenenti a determinate categorie indicate (quali, ad esempio, dati genetici, epigenomici e genomici umani, dati provenienti dalle applicazioni per il benessere o dalle biobanche e dai database associati). Per evitare incertezze derivanti dalla potenziale frammentazione normativa tra gli Stati membri e promuovere un maggiore controllo a livello europeo, è richiesto loro di notificare tali misure aggiuntive alla Commissione (cfr. art. 33, par. 8b, EHDS, testo adottato).

¹⁷² Cfr. il considerando n. 37, EHDS, testo adottato.

¹⁷³ In conformità con l’art. 9, par. 2, lett. *i e j*, GDPR.



tamento iniziale (ad esempio, la fornitura di assistenza sanitaria). Gli organismi di accesso consentono, invece, l'accesso ai dati nello svolgimento di un compito di interesse pubblico assegnato dal medesimo Regolamento, ai sensi dell'art. 6, par. 1, lett. e, GDPR¹⁷⁴. Quanto agli utenti dei dati sanitari, per la richiesta di accesso possono basarsi su una delle basi giuridiche previste dall'art. 6, par. 1, GDPR, tra cui, in particolare, il legittimo interesse o l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri¹⁷⁵.

In tale quadro, la proposta iniziale della Commissione europea non attribuiva alcun ruolo agli interessati nel processo decisionale riguardante l'uso secondario dei loro dati, impedendo loro, altresì, di sottrarsi al trattamento¹⁷⁶; di conseguenza, questo approccio ha sollevato significative preoccupazioni, portando a revisioni successive durante il processo legislativo¹⁷⁷.

La versione finale adottata sembra aver trovato un miglior equilibrio tra l'interesse pubblico e quello individuale, introducendo un meccanismo di opt-out obbligatorio a livello europeo, non lasciato, dunque, alla discrezionalità degli Stati membri¹⁷⁸. Il Regolamento riconosce quindi agli interessati il diritto di rinunciare,

¹⁷⁴ Lo stesso Regolamento soddisfa inoltre i requisiti di cui all'art. 9, par. 2, lett. g, h, i, e j (a seconda dei casi), GDPR.

¹⁷⁵ In tal caso è il Regolamento a fornire le garanzie richieste dall'art. 9, par. 2, GDPR.

¹⁷⁶ In particolare, l'art. 33 stabiliva che, nelle ipotesi in cui il consenso per il trattamento dei dati sanitari fosse richiesto ai sensi della normativa nazionale applicabile, gli organismi responsabili per l'accesso ai dati avrebbero dovuto prescindere da tale consenso e agire in conformità con gli obblighi imposti dal Regolamento.

¹⁷⁷ Il rapporto preliminare elaborato dalle Commissioni ENVI e LIBE del Parlamento europeo ha cercato di ristabilire un equilibrio tra il diritto degli interessati a controllare i propri dati sanitari e l'obiettivo pubblico di facilitare la ricerca medica (V. EUROPEAN PARLIAMENT-COMMITTEE ON THE ENVIRONMENT, PUBLIC HEALTH AND FOOD SAFETY COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft report on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD))*, pubblicato il 10 febbraio 2023). In particolare, l'emendamento n. 84 aveva introdotto un meccanismo vincolante di opt-out, applicabile uniformemente a tutti gli Stati membri, consentendo agli interessati di escludere i propri dati dal trattamento per scopi secondari, senza obbligo di motivazione. Nel testo presentato nel dicembre 2023, frutto di lunghe negoziazioni tra i gruppi politici, il Parlamento aveva proposto una modifica rilevante: oltre a mantenere la possibilità di opt-out, veniva introdotto per alcuni tipi di dati sensibili (in particolare dati genetici, genomici, proteomici, dati di applicazioni per il benessere e dati sanitari elettronici di biobanche) un sistema di opt-in, richiedendo il consenso esplicito degli interessati (cfr. EUROPEAN PARLIAMENT, *European Health Data Space, Amendments adopted by the European Parliament on 13 December 2023 on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD))*, P9_TA(2023)0462, 13 dicembre 2023). Questa scelta, pur mirata a rafforzare l'autodeterminazione dei singoli, avrebbe tuttavia potuto ostacolare un settore importante della ricerca medica e lo sviluppo di nuove tecnologie sanitarie, a causa della mancanza di dati rappresentativi, con possibili ricadute negative sulla salute individuale e collettiva (si osserva infatti frequentemente che i tassi di partecipazione sono più bassi con un approccio di opt-in rispetto a quello di opt-out. Al riguardo, v., tra gli altri, Y. DE MAN-Y. WIELAND-JORNA-B. TORENSMA, et al., *Opt-In and Opt-Out Consent Procedures for the Reuse of Routinely Recorded Health Data in Scientific Research and Their Consequences for Consent Rate and Consent Bias: Systematic Review*, in *Journal of Medical Internet Research*, 2023, e42131, 16; T. SOKOL, *European Health Data Space*, cit., 22). Diversa è stata la soluzione proposta dal Consiglio dell'Unione Europea, che, pur evitando le problematiche dell'opt-in, ha sollevato altre questioni. Il testo del Consiglio lasciava agli Stati membri la facoltà di concedere agli interessati la possibilità di opporsi al trattamento dei dati personali in qualsiasi momento, senza doverne motivare la ragione, riconoscendo loro un diritto di opposizione liberamente esercitabile. Agli Stati membri veniva anche data anche la possibilità di prevedere eccezioni, in linea con l'art. 23 del GDPR, per motivi legati, tra l'altro, alla protezione della salute pubblica, alla sicurezza sul lavoro e alla qualità dell'assistenza sanitaria, inclusa la sicurezza di pazienti e dispositivi medici (cfr. COUNCIL OF THE EUROPEAN UNION, *Proposal for a Regulation on the European Health Data Space – Mandate for negotiations with the European Parliament*, 16048/1/23 REV 1, 7 dicembre 2023, articolo 35F). Questa maggiore autonomia concessa agli Stati membri avrebbe però potuto portare a una frammentazione all'interno dell'Unione Europea, con conseguenti differenze giuridiche tra i cittadini dei vari Paesi riguardo all'uso dei propri dati.

¹⁷⁸ Questa soluzione è stata introdotta nel testo adottato a marzo 2024, in seguito all'accordo raggiunto tra il Parlamento Europeo e il Consiglio dell'Unione Europea, e successivamente confermato nel testo finale approvato dal Parlamento europeo ad aprile 2024, *sub art. 48a*, che richiede agli Stati membri di introdurre meccanismi per consentire l'esercizio del diritto di opt-out da parte degli interessati. La soluzione adottata risulta, dunque, maggiormente coerente con le esigenze di armonizzazione perseguite dal Regolamento. In proposito, v. anche L. BOLOGNINI- S. ZIPPONI, *Prospettive future in sanità: Spazio Europeo dei Dati Sanitari e regolazione dei dati sintetici*, in ID.-ID. (a cura di), *Privacy e diritto dei dati sanitari*, cit., 272.



in qualsiasi momento e senza necessità di giustificazione, al trattamento dei dati sanitari elettronici che li riguardano per uso secondario. In tal caso, i dati in questione non saranno più resi disponibili né altrimenti trattati, senza pregiudicare la liceità dei trattamenti per uso secondario effettuati in precedenza. Gli Stati membri possono tuttavia consentire la disponibilità dei dati per i quali è stato esercitato l'opt-out qualora siano presenti circostanze eccezionali espressamente previste¹⁷⁹, stabilendo misure specifiche e adeguate per proteggere i diritti e le libertà fondamentali delle persone fisiche.

Il testo approvato introduce, dunque, un meccanismo *ex post* che consente agli interessati di impedire l'utilizzo dei propri dati per scopi di uso secondario, garantendo così una forma di controllo individuale. Al contempo, prevede eccezioni per tutelare l'interesse pubblico, in particolare nell'ambito della ricerca scientifica e della formulazione di politiche sanitarie. Tale soluzione mira, pertanto, a garantire la rappresentatività e la disponibilità dei dati per la ricerca, rispettando sia l'autodeterminazione individuale sia le competenze degli Stati membri in materia di assistenza sanitaria. Inoltre, l'approccio risulta coerente con i principi enunciati nell'art. 9, par. 2, lett. j, GDPR, che impone un equilibrio tra l'interesse pubblico e la tutela dei diritti fondamentali degli interessati nell'uso dei dati personali per scopi di ricerca scientifica¹⁸⁰.

Strettamente collegato al controllo degli interessati sui propri dati sanitari è il tema della trasparenza. La proposta iniziale della Commissione escludeva espressamente l'obbligo, per gli organismi responsabili dell'accesso ai dati – che, nell'adempimento dei compiti assegnati dall'EHDS, operano in qualità di titolari del trattamento¹⁸¹ – di fornire a ciascun interessato le informazioni previste dall'art. 14 del GDPR riguardo all'uso secondario dei propri dati, limitandosi, invece, a un obbligo di informazione generale al pubblico sulle condizioni di messa a disposizione di tali dati¹⁸². Questa deroga si giustificava, come chiarito nei considerando della Proposta, in ragione dell'onere amministrativo che l'adempimento dell'obbligo di informazione individuale avrebbe comportato, in conformità a quanto previsto dall'art. 14, par. 5, GDPR¹⁸³. Tuttavia, tale esclusione è stata oggetto di numerose critiche, poiché ritenuta suscettibile di compromettere la trasparenza e l'effettivo esercizio dei diritti da parte degli interessati¹⁸⁴.

Il testo finale del Regolamento, con l'eliminazione dell'espressa deroga presente nella versione originale¹⁸⁵,

¹⁷⁹ In particolare, il Regolamento stabilisce che gli Stati membri possono consentire la disponibilità dei dati esclusivamente in risposta a richieste presentate da: un ente pubblico o da un'istituzione, un organo, un ufficio o un'agenzia dell'Unione con il mandato di svolgere compiti nel settore della sanità pubblica, o da un altro soggetto incaricato di svolgere compiti pubblici nel settore della sanità pubblica, o che agisce per conto di un'autorità pubblica o su incarico di quest'ultima (cfr. art. 48a, EHDS, testo adottato).

¹⁸⁰ In questo senso, v. anche T. SOKOL, *European Health Data Space*, cit., 22.

¹⁸¹ Nello specifico, l'art. 51, nella formulazione da ultimo adottata, definisce espressamente la ripartizione dei ruoli rispetto al trattamento dei dati ai sensi del GDPR. In questo contesto, il titolare dei dati è considerato titolare del trattamento per la comunicazione dei dati richiesti dall'organismo di accesso. L'organismo di accesso agisce come titolare del trattamento nell'adempimento dei suoi compiti, ma diventa responsabile del trattamento per conto dell'utente, che assume il ruolo di titolare, nel momento in cui fornisce i dati a quest'ultimo a seguito dell'autorizzazione.

¹⁸² Cfr. art. 38, par. 2, EUROPEAN COMMISSION, *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, cit.

¹⁸³ Cfr. considerando n. 44, EUROPEAN COMMISSION, *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, cit.

¹⁸⁴ In dottrina cfr., tra gli altri S. SLOKENBERGA, *Scientific Research*, cit., 144; M. SHABANI e S. YILMAZ, *Lawfulness*, cit., 133. Anche il Comitato europeo per la protezione dei dati (EDPB) e il Garante europeo per la protezione dei dati (EDPS), nel loro parere congiunto sulla proposta di Regolamento, avevano evidenziato le criticità di tale soluzione, invitando il legislatore a individuare situazioni specifiche e circoscritte per l'applicazione di questa esenzione, al fine di evitare un'applicazione sistematica priva di adeguata valutazione e giustificazione (cfr. ID., *EDPB-EDPS Joint Opinion 03/2022*, cit., par. 95 e 96). Del resto, la trasparenza è fondamentale poiché, oltre a garantire l'autodeterminazione dell'interessato, costituisce una salvaguardia aggiuntiva quando le circostanze della ricerca non permettono di ottenere un consenso specifico. In questo senso, cfr. quanto evidenziato dall'EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 05/2020*, cit., 31.

¹⁸⁵ Cfr. considerando n. 44 e art. 37a, EHDS, testo adottato.



sembra indicare, invece, il permanere dell'obbligo per gli organismi di accesso di fornire le informazioni richieste dal GDPR. Questa interpretazione trova conferma nel nuovo considerando n. 44, che, a differenza della versione precedente, stabilisce che le informazioni pubbliche che gli organismi di accesso sono tenuti a fornire – incluse le misure di sicurezza adottate e i diritti degli interessati in relazione all'uso secondario dei dati¹⁸⁶ – “integrano” gli obblighi previsti dall'art. 14 del GDPR, garantendo un trattamento equo e trasparente anche qualora venga applicata l'eccezione di cui al par. 5 della medesima disposizione, ora limitata al ricorrere delle condizioni espressamente indicate¹⁸⁷.

Le recenti modifiche alla disciplina sull'uso secondario dei dati sanitari elettronici consentono pertanto di affermare che il legislatore europeo abbia cercato, per quanto possibile, di trovare un giusto equilibrio tra le esigenze della ricerca e i diritti degli interessati, anche in materia di trasparenza, alla luce delle nuove complessità poste dall'attuale contesto tecnologico-informatico.

5. – La ricerca scientifica in ambito medico, fondamentale per il miglioramento della salute individuale e collettiva, ha conosciuto un notevole sviluppo con l'introduzione delle tecnologie *data-intensive*. Tuttavia, con l'evoluzione dei metodi di ricerca, sono emersi i limiti del tradizionale modello di tutela, basato principalmente sul binomio consenso informato-anonimizzazione, nel garantire un'adeguata protezione degli interessati riguardo al trattamento dei loro dati sanitari.

In risposta a queste sfide, il GDPR ha introdotto nuovi meccanismi di *governance* e di gestione del rischio, spostando l'attenzione dal controllo individuale verso una maggiore responsabilizzazione dei titolari del trattamento dei dati. La recente crisi sanitaria globale ha nondimeno reso ancora più evidente la necessità di un intervento normativo che faciliti la condivisione dei dati sanitari a livello transfrontaliero, evidenziando i limiti normativi esistenti in materia di ricerca scientifica e la frammentazione tra gli Stati membri.

Il Regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS) intende superare tali criticità, delineando un sistema di condivisione obbligatoria dei dati sanitari elettronici che prescinde dal consenso individuale, a favore dell'interesse collettivo per la ricerca scientifica in ambito sanitario, ma che integra al contempo misure di controllo *ex post* da parte degli interessati e un meccanismo centralizzato per garantire un utilizzo sicuro e conforme dei dati.

Il nuovo modello di tutela non elimina, dunque, la centralità dell'individuo, ma ne ridefinisce i confini, adattando le misure di protezione alle nuove esigenze della ricerca scientifica, dell'innovazione tecnologica e della globalizzazione. La normativa di prossima adozione, pur presentando alcune criticità che esulano dal *focus* specifico di queste riflessioni conclusive, intende pertanto continuare a mantenere un adeguato equilibrio tra le esigenze della ricerca e la protezione della dignità e dei diritti fondamentali degli interessati, introducendo nuove soluzioni per garantirne una tutela efficace.

Sarà tuttavia necessario attendere la messa in atto del sistema di garanzia delineato dall'EHDS per verificare la capacità di tutelare adeguatamente la riservatezza dei dati sanitari, soprattutto alla luce delle problematiche legate alla sicurezza informatica e alla condivisione transfrontaliera delle informazioni.

¹⁸⁶ Cfr. art. 37a, EHDS, testo adottato, che dispone che gli organismi responsabili dell'accesso ai dati sanitari forniscano agli interessati determinate informazioni, tra cui: la base giuridica che legittima l'accesso per l'utente dei dati, le misure tecniche e organizzative adottate, i diritti delle persone fisiche in relazione all'uso secondario dei dati sanitari elettronici, le modalità di esercizio dei diritti da parte delle persone fisiche ai sensi del GDPR, l'identità e i dati di contatto dell'organismo responsabile, l'identità dei soggetti che hanno ottenuto l'accesso ai dati e l'autorizzazione riguardante le finalità del loro trattamento, nonché le modalità di esercizio del diritto di opt-out.

¹⁸⁷ In questo senso, cfr. anche le modifiche proposte dal Parlamento europeo nel testo pubblicato a dicembre 2023, in relazione al considerando n. 44 e all'art. 38 (EUROPEAN PARLIAMENT, *European Health Data Space, Amendments*, cit., emendamenti nn. 46 e 368).