Information Technology Law 01

Series Editors Fabio Bravo *and* Angelo Giuseppe Orofino

Prospettive civilistiche in ordine agli spazi di condivisione dei dati sanitari alla luce del Regolamento EHDS

Stefano Faillace

Wolters Kluwer

INFORMATION TECHNOLOGY LAW

The volumes published in this Series
have been subject to a double-blind peer review procedure

Information Technology Law 01

Series Editors Fabio Bravo *and* Angelo Giuseppe Orofino

Prospettive civilistiche in ordine agli spazi di condivisione dei dati sanitari alla luce del Regolamento EHDS

Stefano Faillace

Wolters Kluwer

The research is funded by the European Union – Next Generation EU, in the framework of the GRINS – Growing Resilient, Inclusive and Sustainable Project (GRINS PE00000018 – CUP J33C22002910001). The views and opinions expressed are solely those of the authors and do not necessarily reflect those of the European Union, and the European Union cannot be held responsible for them.

This volume, subjected to double-blind peer review, has been positively evaluated by Professors Francesco Di Ciommo and Fabrizio Piraino.

Printed by
GECA - Divisione Libri di CISCRA S.p.A., Via Belvedere, 42 - 20862 Arcore (MB)

A Daniela, Francesco e Chiara

INDICE

Capitolo I

DALLA NUOVA DISCIPLINA DEL «FASCICOLO SANITARIO ELETTRONICO 2.0» ALLA CREAZIONE DI UNO SPAZIO EUROPEO DI CONDIVISIONE DEI DATI SANITARI (EHDS)

Capitolo II

DIFFICOLTÀ INTERPRETATIVE E APPLICATIVE NELL'USO SECONDARIO DEI DATI SANITARI TRA GDPR, CODICE *PRIVACY* ED ELABORAZIONE DELLE CORTI E DELLE AUTORITÀ GARANTI

CAPITOLO III

NUOVI MODELLI DI INTERMEDIAZIONE PROPOSTI DAL *DATA GOVERNANCE ACT* PER UNA TUTELA SOSTANZIALE DEI DIRITTI DELL'INTERESSATO

CAPITOLO IV

LA TUTELA DELL'INTERESSATO NELL'USO PRIMARIO E SECONDARIO DEI DATI SANITARI SECONDO IL REGOLAMENTO EUROPEO CHE ISTITUISCE UN «*EUROPEAN HEALTH DATA SPACE*»

Capitolo I

DALLA NUOVA DISCIPLINA DEL «FASCICOLO SANITARIO ELETTRONICO 2.0» ALLA CREAZIONE DI UNO SPAZIO EUROPEO DI CONDIVISIONE DEI DATI SANITARI (EHDS)

Sommario: 1. Proliferazione di banche dati sanitarie nell'attuale contesto normativo europeo e nazionale. Una *matrioska* che parte dal fascicolo sanitario elettronico, passando per l'Ecosistema dati sanitari, sino al prospettato *European Health Data Space*. – 2. L'inquadramento del Fascicolo sanitario elettronico e della cartella clinica elettronica all'insegna del concetto di "*patient-centered care*". – 3. Il fascicolo sanitario elettronico e le scelte del legislatore in ordine al consenso come sua base giuridica – 4. (*segue*) Titolarità del trattamento, responsabilità della struttura ospedaliera ed eventuale concorso di colpa del paziente «interessato» in caso di *malpractice* medica. – 5. L'erigendo Ecosistema dei dati sanitari, i rapporti con il fascicolo sanitario elettronico e i ruoli del trattamento. – 6. L'elaborazione dei dati clinici presenti nel fascicolo sanitario elettronico attraverso l'utilizzo di strumenti di intelligenza artificiale. Profili di responsabilità del medico e della struttura.

1. *Proliferazione di banche dati sanitarie nell'attuale contesto normativo europeo e nazionale. Una matrioska che parte dal fascicolo sanitario elettronico, passando per l'Ecosistema dei dati sanitari, sino al prospettato European Health Data Space*

Come noto, lo sviluppo delle tecnologie informatiche e l'espandersi del cd. mercato digitale hanno determinato una crescita esponenziale dell'immagazzinamento, dell'accesso e dello scambio di dati e informazioni personali (i cosiddetti *big data*) [1], incrementando correla-

[1] Con la locuzione "*big data*" si fa riferimento alla raccolta, all'analisi e all'accu-

tivamente i rischi connessi all'attività di trattamento [2].

Così, pure nel settore sanitario il progresso scientifico richiede che le autorità sanitarie procedano a raccogliere, conservare ed elaborare i dati sanitari dei singoli, per poter così fornire prestazioni di prevenzione, diagnostiche e di cura aggiornate ed efficaci, anche con l'ausilio di *software* caratterizzati da forme di intelligenza artificiale [3]. Ed infatti,

---

mulo di ingenti quantità di dati, tra i quali possono essere ricompresi dati di natura personale (nell'accezione fornita dall'art. 4 del Reg. UE 2016/679) provenienti anche da fonti diverse. La natura massiva delle operazioni di trattamento reca con sé la necessità che tali insiemi di informazioni siano oggetto di trattamento automatizzato, mediante algoritmi e altre tecniche avanzate, al fine di individuare correlazioni di natura (per lo più) probabilistica, tendenze e/o modelli. I *big data* nel campo della salute stanno crescendo in percentuale maggiore rispetto ad altri settori, in virtù di 4 importanti fenomeni: 1) digitalizzazione della diagnostica per immagini; 2) tecniche di reportistica digitale in sostituzione delle cartelle cartacee; 3) sviluppo di biotecnologie impiegate nel campo delle cosiddette scienze omiche; 4) esplosione dell'*internet of things*.

[2] Cfr. A.C. NAZZARO, *L'utilizzo dei Big data e i problemi di tutela della persona*, in *Rassegna di diritto civile*, 2018, 1239 ss.; A. MANTELERO, *Big data and data protection*, in G. GONZÁLEZ-FUSTER, R. VAN BRAKEL, P. DE HERT (a cura di) *Research Handbook on Privacy and Data Protection Law*, Cheltenham, Edward Elgard Publishing, 2022, 335; U. PAGALLO, *The Legal Challenges of Big Data: putting Secondary Rules First in the Field of EU Data Protection*, in *European Data Protection Law Review*, 2017, 36; A. OTTOLIA, *Big Data e innovazione computazionale*, in *Quaderni AIDA* n. 28, Torino, Giappichelli 2017.

[3] Da anni il settore sanitario è fortemente interessato dall'utilizzo di tecnologie basate sull'intelligenza artificiale. Ciò è stato sicuramente favorito dall'incessante sviluppo di tecnologie basate su sofisticate tecniche di *machine learning* e dall'enorme disponibilità di informazioni che l'era dei *Big Data* consente. Per la Commissione Europea «i *Big Data* in sanità si riferiscono a grandi *set* di dati, raccolti periodicamente o automaticamente, che vengono archiviati elettronicamente, riutilizzabili allo scopo di migliorare le prestazioni del sistema sanitario». Cfr. *European Commission, Study on Big Data in Public Health, Telemedicine and Healthcare, December 2016,* in *https://op.europa.eu/en/publication-detail/-/publication/d504f34c-c104-11e6-a6db-01aa75ed71a1/language-en*. Le possibili fonti di dati in questo scenario sono le più disparate: FSE, letteratura medica, studi clinici, dati sui sinistri assicurativi, cartelle cliniche, dati inseriti dai pazienti o registrati su *fitness tracker*, ecc. La confluenza di questi fattori ha determinato una notevole spinta verso lo sviluppo e il perfezionamento di me-

nel contesto della ricerca scientifica, la tecnologia ha portato alla nascita di sempre più sofisticate banche dati e biobanche, reti telematiche e piattaforme digitali [4]. Non c'è dubbio che lo scambio di dati sanitari sia indispensabile nel settore medico e scientifico: poter accedere a dati aggiornati, affidabili e rispondenti ai principi FAIR (*Findable, Accessible, Interoperable, Reusable)*, nel rispetto del principio di minimiz-

todiche di medicina personalizzata, date le molte aspettative e speranze per l'applicazione delle tecniche di IA in campo medico, quali la possibilità di sviluppare modelli predittivi con evidenti vantaggi in termini di prevenzione e la capacità di fornire diagnosi tempestive, al fine di garantire una pronta reazione con le cure più appropriate. Pure l'introduzione di ambienti basati su *chatbot* promette di garantire un corretto livello di informazione ai pazienti, accompagnandoli nei loro processi di cura.

[4] La banca dati è definita dall'art. 4, comma 1, lett. p), Codice privacy, come «un qualsiasi complesso organizzato di dati personali ripartito in una o più unità dislocate in uno o più siti». Secondo F. Cardarelli, *Le banche dati pubbliche: una definizione*, in *Il diritto dell'informazione e dell'informatica*, 2002, 321, è possibile ricostruire la categoria delle banche dati pubbliche sulla base dei seguenti elementi strutturali: – sono realizzate e gestite, direttamente o indirettamente, da pubbliche amministrazioni ovvero da organismi di diritto pubblico, sulla base di finalità istituzionali proprie di detti enti, definite o previste dalla legge o da regolamenti;– sono generalmente accessibili dagli utenti in base ai principi generali sull'accesso ai documenti amministrativi, e possono essere sottratte al principio dell'accesso solo in caso di limiti legislativi afferenti al segreto, alla tutela dei dati personali ed in particolare di quelli sensibili, ed in caso di banche dati funzionali allo svolgimento di attività a carattere strettamente imprenditoriale o commerciale; – sono proteggibili, se ricorre il requisito della creatività, in forza del diritto d'autore ovvero sono proteggibili sulla base del diritto *sui generis* solo nel caso in cui l'investimento realizzato, direttamente o indirettamente, sia stato rilevante rispetto al normale svolgimento dell'attività amministrativa; - l'insieme dei dati e delle informazioni in esse contenuti, se rilevanti sotto il profilo commerciale, non possono essere resi disponibili in via esclusiva ad un soggetto privato, ma devono poter essere resi accessibili ai soggetti che ne facciano richiesta in base a condizioni eque, trasparenti e non discriminatorie, e sulla base di criteri di remunerativitá che siano orientati ai costi e che in ogni caso non siano di per sé ostacolo allo svolgimento di attività in regime di concorrenza. Con particolare riferimento alla protezione dei dati nelle banche dati sanitarie, si veda M. Campagna, *Il regolamento europeo 679/2016 e l'utilizzo delle banche dati in sanità*, in A. Monica, G. Balduzzi (a cura di), *Governare il cambiamento istituzionale e organizzativo nelle amministrazioni europee*, Pavia, Pavia University Press, 2019, 59 ss.

zazione, permette di fornire cure migliori al paziente e di far progredire in minor tempo i progetti di innovazione e ricerca connessi allo studio delle patologie e allo sviluppo di nuove cure. Fondamentale, ad esempio è stato il ruolo ricoperto dai cd. *big data*, durante l'epidemia da COVID-19, con riferimento sia alle strategie di contenimento del contagio, che alla verifica in merito all'efficacia e alla sicurezza delle soluzioni terapeutiche, non solo vaccinali, adottate per fronteggiare le sintomatologie associate alla suddetta patologia.

Stiamo assistendo, di conseguenza, anche in forza di una decisa politica europea in tal senso, alla creazione di una pluralità di regolamentazioni di derivazione nazionale e unionale, riguardanti la gestione dei dati sanitari, con diverse prospettive funzionali, sia a vocazione individuale che collettiva, che, a tratti, tendono pericolosamente a sovrapporsi, creando indubitabilmente notevoli e rilevanti difficoltà interpretative.

Nell'ambito dell'*European Strategy for data*, il Regolamento denominato *Data Governance act* (Reg. UE 2022/868), entrato in vigore il 24 settembre 2023, mira a promuovere la disponibilità di dati personali e non personali detenuti dal settore pubblico e a creare un ambiente affidabile per facilitarne l'uso per la ricerca e la creazione di nuovi servizi e prodotti innovativi [5]. All'interno di tale cornice, il 3 maggio 2022 la Commissione Europea ha presentato una proposta legislativa avente ad oggetto la creazione di uno Spazio europeo dei dati sanitari, an-

[5] La comunicazione della Commissione europea in data 19 febbraio 2020, denominata «Una strategia europea per i dati» (COM/2020/66 Final), ha avuto come obiettivo ultimo quello di «creare uno spazio unico europeo di dati — un autentico mercato unico di dati, aperto ai dati provenienti da tutto il mondo — nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore, riducendo nel contempo al minimo la nostra impronta di carbonio e ambientale». Cfr. in argomento, F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa/Europa*, 2021, 199 ss.; G. RESTA, *La regolazione digitale nell'Unione Europea. Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, 2022, 971 ss.

che noto come *European Health Data Space* (EHDS), poi divenuto il Regolamento UE 327/2025, che può essere interpretato, per certi versi, come *lex specialis* ed una delle prime applicazioni settoriali del sopra menzionato *Data Governance Act*[6]. È importante sottolineare che l'EHDS non è concepito come un deposito centralizzato di dati europei: piuttosto si configura come un'architettura condivisa per stabilire regole comuni, procedure, *standard* tecnologici e infrastrutture.

Parallelamente, sulla base dell'art. 12, comma 15-*quater*, della legge 17 dicembre 2012 n. 221, con decreto del Ministro della Salute del 31 dicembre 2024[7] è stata prevista la creazione di una banca dati a peri-

[6] Come vedremo più avanti, lo scopo di tale regolamento è quello di consentire alle persone di assumere il controllo dei propri dati sanitari, una migliore erogazione dell'assistenza sanitaria e di permettere all'UE di sfruttare appieno le potenzialità offerte da uno scambio, uso e riutilizzo sicuro e protetto dei dati sanitari, senza gli ostacoli esistenti. Le attuali problematiche legate al riutilizzo dei dati sanitari consistono nella difficoltà di accesso, da parte delle persone fisiche, ai propri dati sanitari mediante sistemi elettronici; nell'impossibilità di condividere i dati generati da ospedali e centri medici con altri operatori sanitari, spesso anche perché registrati su carta, non rintracciabili e disseminati in vari luoghi; nell'impossibilità di visualizzare i dati sanitari generati in un paese diverso da quello di appartenenza; nella difficoltà, nel settore privato, nell'utilizzo del consenso come unica base giuridica per l'utilizzo dei dati dei pazienti nei settori della ricerca e dello sviluppo, con conseguente incremento dei costi e riduzione dell'efficienza degli studi condotti; nella frammentazione normativa tra gli Stati membri, che ostacola la ricerca e l'innovazione da parte dei piccoli attori, e la ricerca transfrontaliera. Il costituendo EHDS, secondo le intenzioni della Commissione che lo ha proposto, dovrebbe permettere agli operatori sanitari di operare in modo più efficace grazie ad una migliore interoperabilità a livello transfrontaliero, e, conseguentemente, di disporre di dati più completi per le decisioni terapeutiche e diagnostiche, anche quando i dati dei pazienti sono ubicati in un altro paese dell'UE. Il potenziamento dell'interoperabilità per agevolare lo scambio di dati tra i prestatori di assistenza sanitaria all'interno dei paesi e a livello transfrontaliero dovrebbe consentire ai prestatori di assistenza sanitaria di evitare la ripetizione dei *tests*, con effetti positivi per i pazienti e la spesa sanitaria.

[7] L'istituzione dell'Ecosistema dati sanitari è stata decisa con decreto del 31 dicembre 2024, pubblicato in G.U. in data 5 marzo 2025.

metro nazionale denominata «Ecosistema Dati Sanitari» (EDS) [8], che dovrebbe raccogliere i dati e i documenti sanitari relativi alle prestazioni socio-sanitarie erogate sul territorio nazionale di tutti gli assistiti, una banca dati che acquisisce, memorizza e gestisce i dati, poi elaborati per offrire servizi agli esercenti le professioni sanitarie, al Ministero della Salute, alle regioni/province autonome e allo stesso interessato. Infine, alla base di tale piramide, appare il Fascicolo Sanitario Elettronico, banca dati a carattere individuale che gode di una regolamentazione stratificata e di un'applicazione ormai ultradecennale, seppur a macchia di leopardo, definito in dottrina come «un supporto informatico contenente dati personali di natura amministrativa, sociale e sanitaria che riflettono un'immagine passata, presente e futura dello stato di salute di una persona al fine di facilitarne l'accesso e l'utilizzo da parte dei terzi autorizzati» [9]. Esso costituisce «una nuova forma di comunicazione e gestione dei dati del paziente, che permette di far confluire in un unico documento informatizzato tutti i dati sanitari di quest'ultimo, in modo da facilitare l'accesso e

[8] Tale norma afferma che: «al fine di garantire il coordinamento informatico e assicurare servizi omogenei sul territorio nazionale per il perseguimento delle finalità di cui al comma 2, il Ministero della Salute, d'intesa con la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale, assicurando l'adeguatezza delle infrastrutture tecnologiche e la sicurezza cibernetica in raccordo con l'Agenzia per la cybersicurezza nazionale, cura la realizzazione dell'Ecosistema Dati Sanitari (di seguito EDS). L'EDS è alimentato dai dati trasmessi dalle strutture sanitarie e socio-sanitarie, dagli enti del Servizio sanitario nazionale e da quelli resi disponibili tramite il sistema Tessera Sanitaria. Il Ministero della Salute è titolare del trattamento dei dati raccolti e generati dall'EDS, la cui gestione operativa è affidata all'AGENAS, che la effettua in qualità' di responsabile del trattamento per conto del predetto Ministero. Con decreto del Ministro della Salute, sono individuati i contenuti dell'EDS, le modalità di alimentazione dell'EDS, nonchè i soggetti che hanno accesso all'EDS, le operazioni eseguibili e le misure di sicurezza per assicurare i diritti degli interessati».

[9] Cfr. V. PEIGNÉ, *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2011, 1519 ss.

l'utilizzo degli stessi da parte dei terzi autorizzati al momento del bisogno»[10].

Dopo un primo riconoscimento giuridico, concretizzatosi nell'emanazione delle Linee Guida del Garante per la protezione dei dati personali[11], cui seguirono, dopo un anno, quelle del Ministero della salute[12], tale strumento venne menzionato dal legislatore per la prima volta in una stesura non definitiva del c.d. Decreto Balduzzi, per poi

---

[10] Cfr. G.Comandé, L. Nocco,V. Peigné, *Il fascicolo sanitario elettronico: uno studio multidisciplinare*, in *Rivista italiana di medicina legale e del diritto in campo sanitario,* 105 s.

[11] Cfr. le «Linee guida in tema di Fascicolo Sanitario Elettronico (FSE) e di dossier sanitario», 16 luglio 2009 (G.U. n. 178 del 3 agosto 2009, *docweb* n. 1634116). In tale sede, l'Autorità Garante ha qualificato il fascicolo sanitario informatico come «condivisione informatica, da parte di distinti organismi o professionisti, di dati e documenti sanitari che vengono formati, integrati e aggiornati nel tempo da più soggetti, al fine di documentare, in modo unitario e in termini il più possibile completi, un'intera gamma di diversi eventi sanitari riguardanti un medesimo individuo, in prospettiva, l'intera sua storia clinica». In tale sede, vennero individuati i contenuti sia del FSE sia del dossier sanitario, che hanno come caratteristica comune il trattamento di dati sanitari relativi ad un medesimo soggetto e riportati in più documenti elettronici tra loro collegati, condivisibili da soggetti sanitari diversi: entrambi contengono informazioni inerenti lo stato di salute di un individuo, relative ad eventi clinici presenti e trascorsi (es. referti, documentazione clinica relativa a ricoveri, accessi al pronto soccorso, vaccinazioni,...) volte a documentare la storia clinica. La differenza tra FSE e dossier sanitario sta nell'ambito di operatività: infatti il FSE è formato da dati sanitari originati da diversi titolari del trattamento (es. aziende sanitarie, laboratori clinici privati, ...), mentre il dossier sanitario è costituito presso un organismo sanitario, unico titolare del trattamento (es. ospedale o clinica privata), al cui interno operino più professionisti. Il riferimento descrittivo e regolamentare di quest'ultimo strumento è dato dal provvedimento n. 331 del 4 giugno 2015, «Linee guida in materia di Dossier Sanitario» – 4 giugno 2015, Pubblicato su G.U. n. 164 del 17 luglio 2015 (*docweb* n. 4084632). In argomento, vedi L. Rufo, *Il dossier sanitario elettronico, Un approccio traslazionale alla disciplina del trattamento dei dati sanitari in ambito clinico*, Bologna, Il mulino, 2018, e, da ultimo, S. Melchionna, *Sanità digitale e innovazione*, in L. Bolognini, S. Zipponi (a cura di), *Privacy e diritto dei dati sanitari*, Milano, Lefebvre Giuffrè, 2024, 103 ss.

[12] Cfr. Ministero della salute, *Il Fascicolo Sanitario Elettronico. Linee guida nazionali*, in *www.salute.gov.it*, 11 novembre 2010.

trovare spazio nel D.L. 18 ottobre 2012, n. 179, convertito con modificazioni dall'art. 12 della legge 17 dicembre 2012 n. 221 [13], affidato alla responsabilità regionale e poi disciplinato con d.p.c.m. 29 settem-

[13] Cfr., in argomento, E. CATELANI, *La digitalizzazione dei dati sanitari: un percorso ad ostacoli*, in *Corti supreme e salute*, 2023, 423 ss.; M. R. NUCCIO, *Digitalizzazione e circolazione dei dati sanitari*, in *Tecnologie e diritto*, 2023, 357 ss.; C. SILVANO, *La digitalizzazione dei servizi sanitari alla luce del riparto di competenze tra Stato e Regioni. Il caso del Fascicolo Sanitario Elettronico*, in *federalismi.it*, 1 novembre 2023, n. 26, 228 ss.; G. CAPILLI, *Diritto privato sanitario. Fondamenti*, Pisa, Pacini, 2022, 5 ss.; L. FERRARO, *Il Regolamento UE 2016/679 tra Fascicolo Sanitario Elettronico e Cartella Clinica Elettronica: il trattamento dei dati di salute e l'autodeterminazione informativa della persona*, in *BioLaw Journal – Rivista di BioDiritto*, 2021, 91 ss.; A. PIOGGIA, *Il Fascicolo sanitario elettronico: opportunità e rischi dell'interoperabilità dei dati sanitari*, in R. CAVALLO PERIN (a cura di), *L'amministrazione pubblica con i* big data*: da Torino un dibattito sull'intelligenza artificiale*, Torino, Università degli studi di Torino, 2021, 215 ss.; N. POSTERARO, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *Federalismi.it* n. 26/2022, 189 ss. Per un'analisi approfondita della disciplina del Fascicolo sanitario elettronico, si veda C.C. GIARDINA, *Il fascicolo sanitario elettronico tra norme e prassi*, in *Azienditalia*, 2021, 2043 ss. Cfr., inoltre, E. SORRENTINO, M. T. GUAGLIANONE, E. CARDILLO, M.T. CHIARAVALLOTI, A. F. SPAGNUOLO, G.A. CAVARRETTA, *La conservazione dei documenti che alimentano il Fascicolo Sanitario Elettronico*, in *Rivista italiana di informatica e diritto*, 2020, 35; A. MARCHESE, *Profili civilistici dell'information technology in ambito sanitario*, Napoli, ESI, 2021; S. CORSO, *Il fascicolo sanitario elettronico fra e-Health, privacy ed emergenza sanitaria*, in *Responsabilità medica*, 2020, 393 ss. Per una panoramica sulla disciplina del fascicolo sanitario elettronico precedente alla sua formale istituzione, si veda P. GUARDA, voce *Civile – Fascicolo sanitario elettronico*, in *Digesto online*, 2011, P. GUARDA, *Fascicolo sanitario elettronico e protezione dei dati personali*, Trento, Università degli studi di Trento, 2011, 65 ss.; G. COMANDÉ, L. NOCCO, V. PEIGNÉ, *Il fascicolo sanitario elettronico: uno studio multidisciplinare*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2012, 105 ss.; G. GLIATTA, *Il diritto alla privacy in ambito medico: trattamento dei dati sensibili e fascicolo sanitario elettronico*, in *La responsabilità civile*, 2010, 682; ID., *Il trattamento dei dati sensibili e la responsabilità per la tenuta del fascicolo elettronico*, in M. FRANZONI (diretto da), *Le responsabilità nei servizi sanitari: responsabilità civile, responsabilità penale, diritto processuale, amministrativo e del lavoro, profili medico-legali e comparatistici, analisi economica*, Bologna, Zanichelli, 2011, 289 ss.; A. THIENE, *Salute, riserbo e rimedio risarcitorio*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2015, 1421.

bre 2015, n.178, che ha definito contenuti, responsabilità dei diversi soggetti che intervengono sul FSE, sistemi di sicurezza e modalità di accesso. Il D.L. 34/2020 ha poi disposto il collegamento del FSE, tramite il supporto dell'INI (Infrastruttura Nazionale per l'Interoperabilità) al Sistema Informativo Trapianti, alle Anagrafi vaccinali e ai CUP regionali, così da consentire l'estensione del patrimonio informativo del FSE ai dati relativi alla donazione degli organi, alle vaccinazioni e alle prenotazioni degli esami medici.

Di recente, la riforma delle disposizioni attuative in ordine all'implementazione del FSE, dopo aver subito una battuta d'arresto a causa del parere negativo dal Garante della privacy [14], è stata definitivamente approvata in data 7 settembre 2023 e pubblicata ed entrata in vigore il 24 ottobre 2023 [15].

Il FSE 2.0 si pone essenzialmente 3 obiettivi principali: l'adozione di un modello architetturale unificato a livello nazionale, di uno standard nazionale di riferimento e l'implementazione di servizi orientati al cittadino [16].

Nel frattempo, in attesa della creazione di uno spazio di condivisio-

---

[14] Lo schema di decreto, trasmesso al Garante *Privacy* con nota del 15 luglio 2022, era stato bocciato dal parere negativo di quest'ultimo, reso in data 22 agosto 2022 n. reg. 294 (*docweb* 9802729). Cfr. S. Corso, *Fascicolo sanitario elettronico ed ecosistema dati sanitari. I pareri critici del Garante per la protezione dei dati personali al Ministero della salute*, in *www.rivistaresponsabilitamedica.it*, 22 settembre 2022

[15] Il decreto è stato pubblicato in G.U., Serie Generale n.249, del 24 ottobre 2023, dopo aver infine ottenuto il parere favorevole del Garante Privacy, reg. provv. n. 256 del 8 giugno 2023 (*doc. web* n. 9900433). In argomento, vedi S. Corso, *Il fascicolo sanitario elettronico 2.0. Spunti per una lettura critica*, in *Le nuove leggi civili commentate*, 2024, 334; A. Thiene, S. Corso (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, Napoli, Jovene, 2023, 1 ss.; N. Posteraro, *Parere del Garante privacy sullo schema di decreto sul Fascicolo Sanitario Elettronico (FSE)*, in *federalismi.it*, *Osservatorio di diritto sanitario*, ottobre 2023.

[16] Sul piano tecnico, il salto di qualità del FSE 2.0 deriva: a) dalla trasformazione dei documenti in dati 'strutturati', che hanno un formato omogeneo e condiviso; b) dalla creazione di un'infrastruttura nazionale per l'interoperabilità (INI) che permette flussi informativi fra Regioni, permettendo la consultazione e l'uso del FSE rela-

ne comune, anche altri paesi europei stanno sviluppando il proprio sistema di *Electronic health records*[17]. È da tempo infatti percepita a livello europeo, sia dagli operatori sanitari sia dagli utenti del sistema sanitario, la necessità di una più agevole accessibilità alle informazioni sulla salute del paziente, per il miglior perseguimento dello scopo di cura[18]. Si possono citare «*Mon espace santé*» in Francia, «*Historia Clínica Digital del Sistema Nacional de Salud*» in Spagna e «*ePA – Die elektronische Patientenakte*" in Germania[19].

---

tivo a un assistito anche da parte di operatori sanitari di Regioni erogatrici della prestazione diverse dalla Regione di assistenza.

[17] Se il nostro modello di FSE è caratterizzato da un'infrastruttura basata su una rete nazionale di architetture regionali, V. PEIGNÉ, *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, cit., 1522 ss., riferisce di modelli differenti da quello italiano, il modello francese e quello inglese, pensati rispettivamente con un'architettura centralizzata a livello nazionale e con una mista. Cfr. anche V. PEIGNÈ, *Verso il Fascicolo Sanitario Elettronico: presentazione della riforma francese*, in *Diritto dell'internet*, 2007, 296.

[18] Cfr. le Comunicazioni della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni, COM/2004/0356, *Sanità elettronica – migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica*, 30 aprile 2004, e COM/2005/0229, *i2010 – Una società dell'informazione per la crescita e l'impiego*, 1° giugno 2005, entrambe consultabili in *www.eur-lex.europa.eu*. Vedi anche G. VICARELLI, M. BRONZINI, *La sanità digitale: dimensioni di analisi e prospettive di ricerca*, in *Politiche sociali*, 2018, 150.

[19] In Francia, la legge n. 2019-774 del 24 luglio 2019, relativa all'organizzazione e alla trasformazione del sistema sanitario (OTSS), prevede la formazione per ogni utente di un *Espace Numérique de Santé* (ENS) (rinominato «*Mon espace santé*»), che dà accesso ai propri dati e ai servizi digitali sanitari. Si tratta di una cartella clinica digitale individuale, la cui attivazione non è obbligatoria, messa a disposizione dei 69 milioni di assicurati in Francia dallo Stato e dall'assicurazione sanitaria, per consentire a ciascun cittadino di archiviare le proprie informazioni mediche e condividerle con gli operatori sanitari che lo curano. L'articolo 45 e l'articolo 50 della legge OTSS sono stati integrati dall'articolo 98 della legge n. 2020-1525 del 7 dicembre 2020, di accelerazione e semplificazione dell'azione pubblica, che pone il *Dossier Médical Partagé* (DMP) come una componente indissociabile del *Mon espace santé*. Inoltre, prevede la creazione automatica del DMP assieme all'apertura automatica del *Mon espace santé*, in applicazione dell'articolo L.1111-13 del codice della sanità pubblica. La Cartella Clinica Condivisa (*Dossier Medicale Partagê*) è una cartella clinica digitale, che con-

Allo stato attuale, poi, alcuni paesi europei stanno sperimentando un'embrionale interoperabilità dei dati. Ci si riferisce *all'European Union Patient Summary*, un documento che viene generato utilizzando le informazioni già presenti nella cartella clinica elettronica del paziente, progettato per consentire ai professionisti sanitari provenienti da altri Paesi dell'Unione Europea di fornire assistenza non programmata a cittadini che richiedano cure al di fuori del proprio Paese d'origine, fornendo informazioni cliniche essenziali sui pazienti (tale servizio risulta attivo in Spagna, Francia, Grecia, Portogallo, Olanda, Lussemburgo, Croazia, Repubblica Ceca). Dato questo panorama normativo alquanto complesso, il tentativo di questo studio è di approfondirne gli aspetti di rilevanza civilistica, segnatamente sulle basi giuridiche del trattamento, sui diritti dell'interessato e sulla responsabilità civile. Si tratta, infatti, di materia magmatica regolata da una disciplina di settore oggetto di plurime modifiche, talvolta lacunose e spesso scarsamente meditate.

2. *L'inquadramento del Fascicolo sanitario elettronico e della cartella clinica elettronica all'insegna del concetto di "patient-centered care"*

L'art. 12 della legge 17 dicembre 2012 n. 221 definisce il fascicolo sanitario elettronico come «l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, riferiti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale». Si tratta di un «archivio della salute dell'assistito», che, istituito dalle singole Regioni (e dalle Province Autonome), viene implementato nel tempo sia dai soggetti che prendono in cura il paziente, che dal paziente stesso. La medesima

sente di archiviare, centralizzare e proteggere le informazioni sanitarie di un paziente, come esami sanitari, allergie ai farmaci, rapporti di ricovero, ecc. È gratuita e confidenziale. Possono contribuire a creare tale cartella clinica condivisa sia il paziente che il medico. Essa archivia la storia medica dei pazienti francesi e consente la raccolta di tutti gli altri dati sanitari personali in aree specifiche.

norma prevede che il FSE sia alimentato con i dati degli eventi clinici, in maniera continuativa e tempestiva, dai soggetti e dagli esercenti le professioni sanitarie che prendono in cura l'assistito (comma 3). Il FSE è istituito per corrispondere a finalità di: a) prevenzione, diagnosi, cura e riabilitazione; b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico [20]; c) programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria, profilassi internazionale (art. 12, comma 2); c-*bis*) valutazioni e accertamenti sanitari per il riconoscimento di prestazioni assistenziali e previdenziali [21]. Esso è, dunque, un *set* strutturato di tutte le informazioni collegate alla sfera della salute di un soggetto – referti, visite mediche o ambulatoriali, accessi al pronto soccorso, prescrizioni, diagnosi, tratta-

[20] L'utilizzo dei dati di cui al fascicolo sanitario elettronico ai fini di ricerca medica è dai più considerato accettabile, poiché si percepisce l'utilità sociale e non lucrativa di questa attività. In argomento, cfr. G. COMANDÉ, *Ricerca in sanità e data protection un puzzle... risolvibile*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2019, 187 ss.. Le finalità di ricerca e di governo sono perseguite secondo livelli di accesso, modalità e logiche di organizzazione ed elaborazione dei dati definiti conformemente ai principi di proporzionalità, necessità e indispensabilità nel trattamento dei dati personali; ma il libero accesso da parte degli organi di governo ai dati (non condizionato dal previo consenso dell'interessato alla consultazione, contrariamente a quanto avviene con riguardo al caso in cui essi debbano essere utilizzati per le finalità di prevenzione, diagnosi, cura e riabilitazione) è garantito purché gli stessi siano pseudonimizzati. Ciò sul presupposto che, per tali finalità, diverse da quella della cura della persona, sia sufficiente utilizzare informazioni non identificative dei pazienti.

[21] Con la riforma della disciplina del FSE, ad opera del d.l. n. 4 del 2022, è previsto, infatti, che il Fascicolo, oltre alle finalità di cura, persegua anche finalità di prevenzione e profilassi internazionale. L'art. 12 del d.l. n. 179 del 2012 individua poi i soggetti che possono perseguire le predette finalità, specificando che quelle di diagnosi, cura e riabilitazione sono di pertinenza del Servizio sanitario nazionale e dei servizi socio-sanitari regionali e di tutti gli esercenti le professioni sanitarie; quelle di prevenzione, del Servizio sanitario nazionale e dei servizi socio-sanitari regionali, degli esercenti le professioni sanitarie, nonché dagli Uffici delle Regioni e delle Province autonome competenti in materia di prevenzione sanitaria e dal Ministero della salute; quelle di profilassi internazionale sono perseguite dal Ministero della Salute.

menti terapeutici, allergie, storia clinica, stile di vita, esami di laboratori, ecc. –, da intendersi in senso lato (può comprendere, ad esempio, dati amministrativi o informazioni fiscali concernenti esenzioni o condizioni di erogazione delle prestazioni sanitarie) [22]. Con il fascicolo sanitario elettronico, quindi, si possono visualizzare e stampare i documenti sanitari (prescrizioni, referti, ecc.), ma anche usufruire di una vasta gamma di servizi, quali, ad esempio: prenotare *on line* visite ed esami specialistici, modificare o disdire gli appuntamenti prenotati, pagare *on line* i ticket sanitari e visualizzare le ricevute dei pagamenti, cambiare o revocare il medico di famiglia, autocertificare le esenzioni per età e reddito. Il paziente, grazie a tale architettura digitale, è quindi messo in condizione di partecipare con maggiore consapevolezza alle decisioni inerenti il mantenimento e la cura della propria salute, diventando, almeno nelle intenzioni del legislatore, il «baricentro del sistema di gestione delle informazioni idonee a rivelare il suo stato di salute» [23]. Un mutamento, questo, che costituisce la caratteristica distintiva dei sistemi di *Personal Health Record* (PHR), attraverso i quali il paziente

---

[22] Tale nozione riprende il concetto, noto in ambiente anglosassone, di *Electronic Health Record* (EHR), che è generalmente definito come un "*repository of information regarding the health status of a subject of care, in computer processable form*", creato, gestito e consultato dagli operatori sanitari autorizzati. Si consideri che secondo il regolamento EHDS, all'art. 2 lett. m, per EHR si intende «una raccolta di dati sanitari elettronici relativi a una persona fisica e raccolti nel sistema sanitario, trattati ai fini della prestazione di assistenza sanitaria».

[23] Il concetto di *patient-centered care* (PCC) fa timidamente comparsa nella letteratura scientifica a partire dagli anni Cinquanta del secolo scorso (A. Leino, *Planning patient-centered care*, in *American Journal of Nursing*, vol. 52, n. 3, 1952, 324), per poi affermarsi, grazie all'avvento di Internet e delle tecnologie informatiche, come uno dei motori trainanti dello sviluppo dei servizi di assistenza sanitaria. A riguardo, vedi J.P. Tarte, C.C. Bogiages, *Patient-centered care delivery and the role of information systems*, in *Computer Health*, vol. 13, n. 2, 1992, 44; N. Calabretta, *Consumer-driven, patient-centered health care in the age of electronic information*, in *Journal of the Medical Library Association*, vol. 90, 1, 2002, 32; T. J. Thompson, D.G. Brailer, *The decade of health information technology: delivering consumer-centric and information-rich health care*, Washington, DC: US Department of Health and Human Services, 2004.

partecipa al controllo e alla gestione del flusso informativo relativo ai propri dati sanitari. I *Personal Health Record* possono anche essere integrati in un ecosistema di FSE, e rappresentano delle piattaforme di servizi *online* rivolte al cittadino, che si declinano in un'ampia gamma di applicazioni, modalità di accesso al FSE, di condivisione di dati tramite tale piattaforma, archiviazione diretta da parte del paziente di informazioni di carattere socio-sanitario che li riguardano. È uno strumento, quindi, che permette di costruire il processo di cura attorno al cittadino: questi, da spettatore passivo di decisioni a lui in larga misura inintelligibili, è messo in condizione di partecipare attivamente con una rinnovata autodeterminazione decisionale, la quale si lega a doppio filo ai profili di protezione dei dati personali. Il FSE nasce quindi come strumento per la persona e subordinato alla sua volontà [24].

Il FSE, inoltre, tende a favorire la coordinazione, la qualità e la

---

[24] Cfr. G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, Zanichelli, 2012, 305, secondo cui «molte sarebbero state le scelte possibili nel delineare l'architettura giuridica del fascicolo sanitario elettronico, come pure del *dossier* sanitario: lo si sarebbe potuto incentrare sul medico, garantendo la completezza delle informazioni, o sulla struttura sanitaria, conferendo maggiore rilevanza agli aspetti amministrativi. Si è scelto, invece, di incentrarlo sull'individuo e di garantire l'autodeterminazione del medesimo. Il fascicolo sanitario elettronico, in questa concezione, è dell'individuo e questi ne gestisce le informazioni. Può decidere, quindi, non solo se costituirlo o meno, ma anche quali eventi sanitari rendere visibili, quali oscurare e quali deoscurare. Il principio di autodeterminazione prevale quindi su altre diverse esigenze, quali appunto quella già citata della completezza delle informazioni contenute nel fascicolo». Anche nella nuova normativa sull'EHDS, su cui *infra*, tale tendenza sembra confermata, visto che, secondo l'art. 5: «Le persone fisiche o i loro rappresentanti di cui all'articolo 4, paragrafo 2, hanno il diritto di inserire informazioni nella propria cartella clinica elettronica attraverso servizi o applicazioni di accesso ai dati sanitari elettronici collegati a tali servizi come indicato al medesimo articolo». Analogamente cfr. Considerando n.12 Reg. EHDS; S. CORSO, *Il fascicolo sanitario elettronico 2.0. Spunti per una lettura critica*, in *Nuove Leggi civili commentate*, 2024, 334, sottolinea però che, negli ultimi anni, un'azione normativa, condotta su più fronti, ha determinato un mutamento del modo di intendere il FSE: da strumento *principalmente per la persona* e la tutela dei suoi diritti fondamentali, su tutti quello alla sua salute, a strumento *primariamente per la pubblica amministrazione* e

continuità delle cure con una migliore informazione e comunicazione sia tra professionisti, che nel rapporto professionista-paziente.[25].

La disponibilità dei dati che transitano attraverso il fascicolo sanitario elettronico incide anche sulle politiche sanitarie a tutti i livelli di *governance* (regionale, nazionale e sovranazionale), consentendo di acquisire elementi utili alla conoscenza di specifici profili del quadro sanitario, così da poter adottare misure idonee a prevenire la diffusione di certe patologie, tenere sotto controllo alcuni fattori di rischio o porre attenzione alla capacità predittiva propria di elementi informativi apparentemente irrilevanti e marginali. Pare opportuno, poi, distin-

---

la garanzia di maggiore efficienza, nel contesto del funzionamento del Sistema sanitario nazionale.

[25] Sono molteplici i benefici che il FSE può apportare a supporto di un sistema di sanità integrata. Le informazioni possono essere agevolmente condivise tra gli operatori autorizzati e il processo decisionale relativo alle scelte terapeutiche può essere gestito in maniera coordinata dalle strutture che, a vario titolo, hanno in cura un medesimo soggetto. Naturalmente, più sarà accurata la raccolta dei dati, garantita la fruibilità degli stessi e contestualizzata la loro trasposizione, maggiori saranno gli obiettivi che il sistema sarà in grado di raggiungere. Cfr., a riguardo, P.G. Shekelle, S. C. Morton, E. B. Keeler, *Costs and benefits of health information technology*, in *Evidence report/technology assessment* (Full Rep), n. 132, 2006, 1 ss.. Ovviamente, anche in questo campo, l'errore umano può causare danni concreti o potenziali. Ad esempio, il Garante *Privacy*, con provvedimento del 24 giugno 2021, reg. n. 251 (*doc. web n.* 9709119), ha sanzionato l'I.R.C.C.S. Burlo Garofolo di Trieste, per l'errore di un suo dipendente – operatore sanitario, che, all'atto della registrazione del consenso al trattamento dati personali della figlia della ricorrente, aveva associato, nel sistema dell'anagrafica sanitaria, ai dati della medesima quelli di una minore omonima della figlia. La ricorrente, quindi, aveva avuto la possibilità di visualizzare, attraverso la sua utenza, il Fascicolo Sanitario Elettronico (FSE) di una minore nei cui confronti non aveva potestà legale. Tale comportamento ha violato i principi di «esattezza», di «integrità e riservatezza» del trattamento, di «liceità, correttezza e trasparenza» (art. 5, par. 1, lett. a), d) e f) del Regolamento), nonché le disposizioni relative al trattamento delle categorie particolari di dati personali (art. 9 del Regolamento). Per fattispecie analoghe, vedi Provvedimento del Garante nei confronti del Centro diagnostico italiano di Milano in data 25 marzo 2021, reg. provv. n. 118 (*doc. web n. 9586906)* e il Provvedimento del Garante del 9 luglio 2020 (*doc. web n. 9440117*) nei confronti della Fondazione IRCCS Policlinico San Matteo –reg. provv. n. 141 del 9 luglio 2020.

guere il FSE dalla Cartella Clinica Elettronica (CCE) [26]. Quest'ultima è stata definita dall'art. 47 bis, comma 1, D.L. 9 febbraio 2012, n. 5, come un documento in formato digitale, elaborato dalla struttura che ha in cura il paziente, contenente i dati medico-sanitari riferiti al singolo episodio di ricovero che lo riguarda. Essa mira ad assicurare continuità all'intrapreso percorso di cura e di assistenza [27]. La cartella clinica,

---

[26] Riguardo al ruolo della cartella clinica elettronica per la tutela giurisdizionale dei pazienti, specialmente sul fronte dell'azione risarcitoria nei confronti della struttura sanitaria e del medico, recentemente, vedi N. POSTERARO, *Danni da responsabilità medica*, in G. CASSANO (a cura di), *Il danno alla persona*, Milano, Lefebvre Giuffrè, 2021, 831 ss. La giurisprudenza in materia si è occupata dell'ipotesi di conflitto fra il diritto alla riservatezza del titolare della cartella clinica e il diritto del coniuge di ottenere l'annullamento del matrimonio concordatario, sancendo la parità di rango delle due situazioni e, quindi, ritenendo legittimo l'accesso alla cartella clinica da parte di costui (Cfr. Cons. Stato 28 settembre 2010, n.7166, in *Ragiusan*, 2011, 321-322; TAR Catania 7 maggio 2008 n. 878, in *Foro Amministrativo Tar*, 2009, 1609; Cons. Stato 28 ottobre 2010, n. 5374, in *Ragiusan* 2009, 303-304; Cons. Stato 14 novembre 2006, n. 6681, *Riv. Amministrativa Rep. It.*, 2008, 98).

[27] Nel regolamento EHDS (all'art. 2 lett. j), la cartella clinica elettronica è definita come «una raccolta di dati sanitari elettronici relativi a una persona fisica e rilevati nell'ambito del sistema sanitario, il cui trattamento avviene ai fini della prestazione di assistenza sanitaria», e all'art. 2 lett. k), un «sistema di cartelle cliniche elettroniche»: qualsiasi sistema in cui il *software* oppure la combinazione tra l'*hardware* e il *software* del sistema consente ai dati sanitari elettronici personali rientranti nelle categorie prioritarie di dati sanitari elettronici personali stabilite a norma del presente regolamento di essere conservati, intermediati, esportati, importati, convertiti, modificati o visualizzati e destinato dal fabbricante a essere utilizzato dai prestatori di assistenza sanitaria nel fornire cure assistenziali ai pazienti o dai pazienti nell'accedere ai loro dati sanitari elettronici. (In argomento, vedi C. INGENITO, *La rete di assistenza sanitaria on-line: la cartella clinica elettronica*, in *www.federalismi.it.*, n.5, 2021, 80-82; S. CORSO, *Salute e riserbo del paziente: questioni aperte in tema di cartella clinica*, in *Rivista responsabilità medica*, 2017, 395 e ss.; F. BOCCHINI, *Le cartelle cliniche. Funzioni, documento, prova*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2018, 35 ss.; P. GUARDA, *I dati sanitari*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 591; F. FILAURO, *Telemedicina, cartella clinica elettronica e tutela della privacy*, in *Danno e responsabilità*, 2011, 472; Con riferimento alla letteratura sulle cartelle cliniche elettroniche, vedi, *ex plurimis*, H. GLENNIE, *Electronic*

secondo l'impostazione prevalente, è considerata, dal punto di vista probatorio, un atto pubblico di fede privilegiata, in quanto redatta da parte del medico che riveste la qualifica di pubblico ufficiale nel momento in cui compie attività di assistenza sanitaria all'interno di ASL ovvero di Enti Ospedalieri, nell'esercizio di una potestà di certificazione ed attestazione [28]. Il FSE, invece, non assume la natura di at-

---

Health Records: Where They Are Now and Where They Need to Be, in R. MA (a cura di),- *Clinical Costing Techniques and Analysis in Modern Healthcare Systems*, Hershey, 2019, 87 ss.; R.S. Evans, *Electronic Health Records: Then, Now, and in the Future*, in *Yearbook of Medical Informatics*, 2016, *Special 25 Anniversary Edition*, 48 ss.; S. Hoffman, *Electronic Health Records and Medical Big Data. Law and policy*, Cambridge University press, 2016; G. De Minico, *Electronic health record: political issues and privacy*, in *www.apertacontrada.it*, 18 dicembre 2015; M. Turk, *Electronic Health Records: How to Suture the Gap Between Privacy and Efficient Delivery of Healthcare*, in *Brooklyn Law review*, vol. 80, 2015, 565 ss.; C. K. Wang, *Security and privacy of personal health record, electronic medical record and health information*, in *Problems and Perspectives in Management*, 2015, vol.13, n.4, 19 ss.; L.B. Harman, C.A. Flite, K.. Bond, *Electronic Health Records: Privacy, Confidentiality, and Security*, in *Virtual Mentor. American Medical Association Journal of Ethics*, 2012, vol. 14, n. 9, 712 ss.; T. Miron-Shatz, G. Elwyn, *To serve and protect? Electronic health records pose challenges for privacy, autonomy and person-centered medicine*, in *The International Journal of Person Centered Medicine*, 2011, vol. 1, 405 ss.

[28] La prevalente giurisprudenza di merito e di legittimità (*ex multis*, Cass. pen. 22 ottobre 2018, n. 55385, in *Responsabilità civile e previdenza,* 2019, 668; Cass. civ., 8 novembre 2016, n. 22639, in *Responsabilità civile e previdenza*, 2016, 2025; Cass. pen. 10 dicembre 2014, n. 5635, in *Ragiusan*, 2015, 371-373; ma già Cass. Pen. 26 novembre 1997, n. 1098, in *Giustizia penale*, 1999, II, 45; Cass. pen. 8 febbraio 1990, in *Giustizia penale*, 1991, II, 76), definisce appunto la cartella clinica quale atto pubblico di fede privilegiata, in quanto redatta da parte del medico che riveste la qualifica di pubblico ufficiale, nel momento in cui compie attività di assistenza sanitaria all'interno di ASL ovvero di Enti Ospedalieri, nell'esercizio di una potestà di certificazione ed attestazione. Un'impostazione dottrinaria, invece, definisce la cartella clinica quale atto di certificazione, dichiarazione di scienza e di verità da parte del medico, non suscettibile in quanto tale di modificare le situazioni giuridiche ad essa preesistenti. Sarebbe infatti un atto inidoneo ad esplicare un'efficacia costitutiva di nuove situazioni giuridiche, ciò che invece costituirebbe la funzione distintiva e peculiare dell'atto pubblico (Cfr. O. De Pietro, L. D'Ancora, *La cartella clinica. Problemi procedurali e aspetti medico-legali*, Napoli, Martinucci, 1985, 39; A. De Marsico, *Natura giuridica del verbale di ricovero d'urgenza in ospedale e cartella clinica. I controlli e la loro influenza in atti*, in *Giustizia penale*, 1971, 97-

to pubblico, in quanto non certifica lo stato di salute di un individuo, bensì fornisce, in maniera potenzialmente incompleta, informazioni sanitarie che possono agevolare il percorso di cura. A normativa vigente, infatti, mentre non è richiesto il consenso alla compilazione della cartella clinica, all'interessato è riconosciuto il diritto di non acconsentire all'utilizzo del FSE per determinate finalità. Analogamente, non è possibile richiedere l'oscuramento dei dati inseriti nella cartella clinica, mentre è previsto che taluni dati e documenti (c.d. a maggior tutela di anonimato) siano di regola oscurati attraverso il Fascicolo e che l'interessato possa comunque decidere di non renderne consultabili altri (diritto di oscuramento). Va infine rimarcato come, al comma 4 dell'art. 1 della legge 22 dicembre 2017 n. 219 (Norme in materia di consenso informato e disposizioni anticipate di trattamento), venga espressamente specificato che «il consenso informato, in qualunque forma espresso, è inserito nella cartella clinica e nel fascicolo sanitario elettronico». Entrambi tali documenti, il fascicolo sanitario e la cartella clinica, diventano, pertanto, serbatoi da cui attingere per verificare la presenza del consenso informato al trattamento sanitario in caso di controversia giudiziaria.

Peraltro, l'irregolare tenuta della cartella clinica del paziente può causare una responsabilità del medico, e ciò è desumibile dal Codice di Deontologia Medica, che, all'art. 26, comma 1, precisa che: «Il medico redige la cartella clinica, quale documento essenziale dell'evento ricovero, con completezza, chiarezza e diligenza e ne tutela la riservatezza; le eventuali correzioni vanno motivate e sottoscritte»[29]; in essa

105). Se, poi, le cartelle cliniche provengono da strutture private, che non operano in rapporto di convenzionamento, si atteggiano come semplice promemoria privato dell'attività diagnostica e terapeutica svolta, superabile con gli ordinari mezzi di prova.

[29] Cfr. poi Cass. Civ., 17 gennaio 2020, n.852, in *Giustiziacivile.com*, 2020, con nota di E. A. EMILIOZZI, *Esiste la responsabilità per l'incompleta compilazione della cartella clinica?*, in cui si afferma che l'irregolare formazione della cartella clinica può determinare una responsabilità contrattuale, e, ai fini del riparto dell'onere della prova tra il paziente danneggiato da un lato e la struttura sanitaria o il medico danneggiante dall'altro, il primo deve limitarsi a provare l'esistenza del contratto, ovvero, il contatto sociale, l'insorgenza o l'aggravamento della patologia e l'inadempimento del debito-

il medico riporta i dati anamnestici e quelli obiettivi relativi alla condizione clinica e alle attività diagnostico-terapeutiche a tal fine pratica-

---

re astrattamente idoneo a provocare il danno lamentato, mentre sul secondo grava l'onere di dimostrare che non vi è stato inadempimento, ovvero, che esso, se vi è stato, non è eziologicamente rilevante nei confronti dell'evento dannoso. L'incompletezza della cartella deve essere tale da impedire la ricostruzione fattuale sul piano concreto, e, in particolare nel suo nucleo centrale, identificabile nella connessione materialmente eziologica fra condotta sanitaria commissiva od omissiva ed evento. Sotto quest'ultimo profilo, la valenza della incompletezza della cartella si pone, attraverso il mezzo presuntivo – su cui, a ben guardare, si riflette in concreto il principio della prossimità della prova –, a favore di chi adduce di essere stato danneggiato, giacché diversamente verrebbe a giovare proprio a colui che, inadempiendo al proprio obbligo di diligenza, tale incompletezza ha creato (Cass., 14 novembre 2019, n. 29498, in *Dejure*). Tuttavia, non si deve pensare che la responsabilità contrattuale della struttura sanitaria derivi *tout court* dall'irregolare compilazione della cartella clinica del paziente, bensì essa sussiste: «quando, attraverso un criterio necessariamente probabilistico, si possa ritenere che l'opera del medico, se correttamente e prontamente prestata, avrebbe avuto fondate possibilità di evitare il danno» (Cass., 27 aprile 2010, n. 10060, in *Dejure*). Pertanto, le irregolarità nella tenuta della cartella clinica non escludono l'onere della prova a carico del paziente di dimostrare l'astratta idoneità della condotta del medico alla produzione del danno lamentato, bensì impediscono al medico stesso di fornire la prova della interruzione del presunto nesso eziologico tra la condotta e l'evento di danno invocando proprio le lacune della cartella clinica (Cass., 13 settembre 2000, n. 12103, in *Dejure*). Il fatto che la cartella clinica sia redatta dalla stessa parte che svolge la prestazione sanitaria comporta un'assoluta posizione di dominio del medico sulla principale prova documentale della propria condotta. In quest'ottica, non è accettabile che il difetto di compilazione della cartella clinica possa tradursi in uno svantaggio processuale per il paziente, anziché per la parte cui il difetto di annotazione è imputabile. Le lacune nella tenuta della cartella clinica consentono «il ricorso alle presunzioni, come avviene in ogni caso in cui la prova non possa essere data per un comportamento ascrivibile alla stessa parte contro la quale il fatto da provare avrebbe potuto essere invocato, nel quadro dei principi in ordine alla distribuzione dell'onere della prova ed al rilievo che assume a tal fine la «vicinanza della prova» e cioè la effettiva possibilità per l'una o per l'altra di offrirla» (cfr. Cass., 21 luglio 2003, n. 11316. In senso analogo, vedi Cass. civ., sez. III, 23 marzo 2018, n. 7250; Cass. civ., sez. III, 18 febbraio 2021, n. 4424; Cass. civ., sez. III, 21 novembre 2017, n. 27561, Cass. civ., sez. III, 12 giugno 2015, n. 12218; Cass. civ., sez. III, 31 marzo 2016, n. 6209, tutte in *Dejure*).

te; registra il decorso clinico assistenziale nel suo contestuale manifestarsi o nell'eventuale pianificazione anticipata delle cure, nel caso di paziente con malattia progressiva, garantendo la tracciabilità della sua redazione (Cfr. art. 26, comma 2 del codice deontologico). L'obbligo di conservazione della cartella clinica, distinto dall'obbligo di tenuta della medesima, è invece a carico della struttura sanitaria [30].

3. *Il fascicolo sanitario elettronico e le scelte del legislatore in ordine al consenso come sua base giuridica*

Nella formulazione originaria del D.L. 179/2012, il FSE prevedeva la raccolta di due consensi da parte dell'assistito: un consenso «libero e informato» per l'alimentazione del medesimo (art. 12, comma 3-*bis*), potendo il cittadino decidere se e quali dati relativi alla propria salute far inserire nel fascicolo, ed un consenso alla consultazione dei dati e documenti da parte del curante, con il relativo richiamo al rispetto del segreto professionale e prevedendo modalità da individuarsi nei casi di emergenza sanitaria. Il comma 5 dell'art. 12, L. 221/2012 precisa tuttora tra l'altro che il mancato consenso «non pregiudica il diritto all'erogazione della prestazione sanitaria». Il D. L. 19 maggio 2020, n. 34 (c.d. Decreto Rilancio), convertito nella L. 17 luglio 2020, n. 77, all'art. 11, ha però abrogato il suddetto comma 3-*bis*, per cui

[30] Va, infatti, tenuta in considerazione la distinzione tra l'obbligo di compilazione e l'obbligo di conservazione della cartella clinica. Cass. Civ., sez III, 13 luglio 2018 n. 18567, in *Foro it.*, 2018, 1, 10, c. 3048, ha stabilito, infatti, che, ai sensi dell'art. 7 del d.p.r. n. 128/1969, il primario è responsabile della compilazione e conservazione della cartella clinica per tutta la durata del ricovero e ha il dovere di consegnare l'atto all'archivio centrale; una volta avvenuto questo passaggio, l'obbligo di conservazione si trasferisce però, in via esclusiva e a tempo indeterminato, sulla struttura sanitaria e più precisamente sul direttore sanitario, su cui ricadranno eventuali omissioni, quali lo smarrimento della cartella.

non è più necessario il consenso per l'alimentazione del FSE [31]. Permane invece la necessità di un consenso per la consultazione dei dati e documenti da parte dei sanitari. [32]

---

[31] Cfr., in argomento, Cfr. A. Gambino, V. Maggio, E. Occorsio, *La riforma del fascicolo sanitario elettronico*, in *Diritto Mercato Tecnologia*, 22 luglio 2020, 10 e ss.; A. Piogia, *Il decreto "rilancio". sanità e sicurezza*, in *Giornale di diritto amministrativo*, 2020, 560. La scelta appare in linea con l'indirizzo del Garante *privacy,* espresso con provvedimento del 7 marzo 2019, n. 55, «Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario», consultabile in *www.garanteprivacy.it*. Cfr., in argomento, N. Busca, *Chiarimenti sull'applicazione della disciplina di protezione dei dati in ambito sanitario*, in *www.rivistaresponsabilitamedica.it*, 8 aprile 2019; M. D'Agostino Panebianco, *Il trattamento dei dati nel Sistema Sanitario Nazionale italiano alla luce del Provvedimento del Garante del 7 marzo 2019*, in *Ciberspazio e diritto*, 2019, 241 ss.; F.G. Cuttaia, *The impact of EU Regulation 2016/679 on the Italian health system*, in G.M. Fares (a cura di), *The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis*, Torino, 2021, 200 s.; M. Foglia, *Patients and privacy: GDPR compliance for healthcare organizations*, in *European Journal of Privacy Law & Technologies*, 2020, Special Issue, 43 ss.; R.M. Colangelo, *App mediche e protezione dei dati personali. Alcuni spunti giuridici tra Gdpr, codice privacy novellato e chiarimenti del Garante*, in *Autonomie locali e servizi sociali*, 2019, 275 ss.

[32] Da quel che emerge leggendo il numero di fascicoli attivati nel sito istituzionale dedicato, si ricava inoltre che non solo l'alimentazione, ma anche l'attivazione del FSE avviene senza il consenso degli interessati. La possibilità di attivare automaticamente il FSE di ciascun singolo è stata dedotta in via interpretativa dall'eliminazione della regola che richiedeva il consenso per l'alimentazione (Si veda, al riguardo, la circolare del Ministero della salute e del Ministero dell'economia e delle finanze 17 febbraio 2021, in *www.trovanorme.salute.gov.it*.). Cfr. però l'art. 11, Reg. EHDS, secondo cui «nel trattare i dati in formato elettronico, i professionisti sanitari hanno accesso ai dati sanitari elettronici personali pertinenti e necessari delle persone fisiche in cura presso di loro attraverso i servizi di accesso per professionisti sanitari di cui all'articolo 12, indipendentemente dallo Stato membro di affiliazione e dallo Stato membro di cura». Se lo Stato membro di affiliazione e lo Stato membro di cura della persona fisica in cura differiscono, l'accesso transfrontaliero ai suoi dati sanitari elettronici personali è fornito attraverso l'infrastruttura transfrontaliera di cui all'articolo 23. L'accesso di cui ai paragrafi 1 e 2 del presente articolo include almeno le categorie prioritarie dei dati sanitari elettronici personali di cui all'articolo 14. Nel trattare i dati in formato elettronico, i prestatori di assistenza sanitaria garantiscono che i dati sanitari elettronici personali delle persone fisiche che hanno in cura siano

A seguito di tale modifica, il FSE è alimentato «in maniera continuativa e tempestiva» dagli esercenti le professioni sanitarie che prendono in cura l'assistito, esercenti operanti ora anche al di fuori del Servizio sanitario nazionale [33], nonché, su iniziativa dello stesso interessato, con i dati a sua disposizione nella partizione del FSE denominata Taccuino personale (cfr. art. 4, DPCM n. 178/2015). Solo però con l'entrata in vigore del decreto, denominato «fascicolo sanitario elettronico 2.0» del 24 ottobre 2023, come vedremo, il margine di responsabilità per l'inadempimento di tale obbligo di alimentazione è stato disciplinato, seppur in maniera scarna e lacunosa.

Una volta che l'assistito abbia espresso il proprio consenso, libero, specifico, informato e inequivocabile, alla consultazione del fascicolo, che deve essere reso *una tantum* e può essere sempre revocato, il personale sanitario che lo ha in cura può accedere al di lui FSE. Va peraltro evidenziato che tale consenso esplicito dell'interessato è richiesto per le finalità di diagnosi, cura e riabilitazione, prevenzione e profilassi internazionale (art. 8 decreto FSE 2.0), e sempre nel rispetto del segreto professionale (art. 12, c. 5, d.l.n.179/2012), mentre il consenso non è richiesto per finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico, per le finalità di programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria e per valutazioni e accertamenti sanitari per il riconoscimento di prestazioni assistenziali e previdenziali. A cosa si deve questa prevalenza del consenso come base giuridica? Ebbene, se è vero che nello stabilire un generale divieto al trattamento delle categorie particolari di dati personali, il GDPR prevede alcune deroghe, tra cui rientrano

---

aggiornati con informazioni relative all'assistenza sanitaria prestata. In questa nuova normativa di derivazione comunitaria, quindi, in linea di principio e salvo il diritto di esclusione, di cui si parlerà nel capitolo IV, non è contemplato un consenso dell'interessato per l'uso primario dei dati sanitari da parte degli operatori sanitari.

[33] Peraltro, l'art. 11 del codice deontologico del Consiglio dell'Ordine dei Medici Chirurghi e degli Odontoiatri del 2006 vieta al medico di collaborare alla costituzione di banche di dati sanitari, ove non esistano garanzie di tutela della riservatezza, della sicurezza e della vita privata della persona.

quelle relative alla salute di cui all'art. 9 GDPR, di queste ultime non fa parte la materia di cui si tratta [34]. Insomma, come correttamente

[34] Tali deroghe sono riconducibili, in via generale, ai trattamenti necessari per: motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (art. 9, par. 2, lett. g) del Regolamento), individuati dall'art. 2-*sexies* del Codice privacy; motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. i) del Regolamento e Considerando n. 54) (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare); finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali («finalità di cura») sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità, (art. 9, par. 2, lett. h) e par. 3 del Regolamento e considerando n. 53; art. 75 del Codice) effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza. In argomento, vedi G. Garofalo, *Trattamento e protezione dei dati personali, spunti rimediali in ambito sanitario*, in *Diritto di famiglia e delle persone*, 2021, 1392 ss.; G. Comandè, *Ricerca in sanità e data protection un puzzle.. risolvibile*, in *Rivista italiana di medicina legale e del diritto in campo sanitario,* 2019, 187 ss. A titolo esemplificativo, oltre ai trattamenti relativi al FSE, non rientrano nelle sopradescritte ipotesi, e richiedono il consenso dell'interessato o altra idonea condizione legittimante, secondo quanto stabilito dal Garante privacy nel provv. GPDP 7 marzo 2019, n. 55 (*docweb* n. 9091942) recante «Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario»), anche le seguenti categorie: a) trattamenti connessi all'utilizzo di *app* mediche, attraverso le quali autonomi titolari raccolgono dati, anche sanitari dell'interessato, per finalità diverse dalla telemedicina oppure quando, indipendentemente dalla finalità dell'applicazione, ai dati dell'interessato possano avere accesso soggetti diversi dai professionisti sanitari o altri soggetti tenuti al segreto professionale (cfr. Faq CNIL del 17 agosto 2018 sulle applicazioni mobili in sanità); b) trattamenti preordinati alla fidelizzazione della clientela, effettuati dalle farmacie attraverso programmi di accumulo punti, al fine di fruire di servizi o prestazioni accessorie, attinenti al settore farmaceutico-sanitario, aggiuntivi rispetto alle attività di assistenza farmaceutica tradizionalmente svolta dalle farmacie territoriali pubbliche e private nell'ambito del Servizio sanitario nazionale (SSN); c) trattamenti effettuati in campo sanitario da persone giuridiche private per

precisato dal Garante per la protezione dei dati personali, ai sensi dell'art. 9, par. 2, lett. h) e par. 3 del GDPR, il professionista sanitario, soggetto al segreto professionale, può trattare i dati sanitari del paziente anche senza il suo consenso, per i trattamenti necessari alla prestazione sanitaria richiesta dall'interessato (indipendentemente dal fatto che questi operi in qualità di libero professionista, ovvero all'interno di una struttura pubblica o privata), ma i trattamenti effettuati attraverso il FSE per finalità di cura richiedono comunque, quale condizione di liceità, l'acquisizione del consenso, posto che lo stesso è richiesto da disposizioni di settore «che sono precedenti all'applicazione del regolamento», disposizioni il cui rispetto è poi stato espressamente previsto dall'art. 75 del Codice privacy [35].

Tale consenso, peraltro, deve essere reso a seguito della visione della relativa informativa che illustri al cittadino il tipo di trattamento, i dati che vengono trattati, le finalità e la titolarità del trattamento [36].

---

finalità promozionali o commerciali (es. promozioni su programmi di screening, contratto di fornitura di servizi ammnistrativi, come quelli alberghieri di degenza); d) trattamenti effettuati da professionisti sanitari per finalità commerciali o elettorali (cfr. provv. del 6 marzo 2014, *doc. web* n. 3013267).

[35] Cfr., sul punto, il provvedimento del Garante privacy, «Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario», 7 marzo 2019 (*docweb* 9091942), in *www.garanteprivacy.it*.

[36] Sulla tradizionale qualificazione del consenso quale atto autorizzativo di diritto privato, specificazione della più ampia figura del consenso dell'avente diritto, a carattere non negoziale, cfr., S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in *Rivista di diritto civile*, 1999, II, 455 s.; S. VICIANI, *Strategie contrattuali del consenso al trattamento dei dati personali*, in *Rivista critica di diritto privato*, 1999, 159 s.; A. FICI, E. PELLECCHIA, *Il consenso al trattamento*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003, 502; A. DI MAJO, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela,* in V. CUFFARO, V. RICCIUTO, V. ZENO ZENCOVICH, *Trattamento dei dati personali e tutela della persona*, Milano, Giuffrè, 1999, 230, il quale osserva che il consenso dell'interessato «negoziale o meno che possa definirsi, non equivale certo ad un atto di disposizione, una volta per tutte, di un proprio bene o diritto ma ad un elemento che rende lecito un comportamento di altri, che interferisca in qualche modo nella sfera giuridica dell'interessato. Tale esclusione vale *hic et nunc*, non impegna per il futuro». Secondo A. THIENE, *Com-*

A seguito dell'entrata in vigore del GDPR, l'informativa deve esse-

mento all'art. 9, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della privacy e data protection*, Milano, Giuffrè, 2021, 245, il consenso è investito di una funzione autorizzativa/permissiva perché ha l'effetto di rimuovere quel dovere generale di astensione che protegge il riserbo della persona, rendendo così lecita l'attività di trattamento che altrimenti sarebbe vietata (cfr., in tal senso, pure D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Rivista critica di diritto privato,* 1998, 351 ss.). In termini più generali, sulla centralità della figura del consenso nell'ambito della disposizione del sé, cfr. C. Castronovo, *Il negozio giuridico dal patrimonio alla persona*, in *Europa e diritto privato*, 2009, 87 s. e, in particolare, 100 s.; A. Nicolussi, *Lo sviluppo della persona umana come valore costituzionale e il cosiddetto biodiritto*, in *Europa e diritto privato*, 2009, 1 s.; Id., *Autonomia privata e diritti della persona*, in *Enc. dir.*, Annali, IV, Milano, Giuffrè, 2011, 133 s. Invero, come è noto, una parte della dottrina attribuisce (in ogni caso) al consenso natura di atto dispositivo: cfr. G. Oppo, *Sul consenso dell'interessato,* in V. Cuffaro, V. Ricciuto, V. Zeno Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, , 1993, 123 s.; V. Zeno Zencovich, *Una lettura comparatistica della l. 675/96 sul trattamento dei dati personali*, ivi, 169 s.; Bilotta, *Consenso e condizioni generali di contratto,* in V. Cuffaro, V. Ricciuto (a cura di) *Il Trattamento dei dati personali*, Milano, Giuffrè, 1993, 87 s., con la conseguenza che le informazioni rilevano quali veri e propri beni giuridici. Cfr. poi, F. Bravo, *Il consenso e le altre condizioni di liceità del trattamento dei dati personali*, in G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 152-157, che ritiene che il dibattito sulla natura giuridica del consenso sia sterile, in ragione del fatto che esso può assumere diversi connotati a seconda delle circostanze e delle fattispecie. La constatazione della difficoltà di una ricostruzione univoca del consenso viene confermata pure da V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Diritto dell'informazione e dell'informatica*, 2018, 689 ss.; Id, *L'equivoco della privacy. Persona vs dato personale*, Napoli, ESI, 2022, 180. Sulle possibili diverse qualificazioni giuridiche del consenso, cfr., ampiamente, il contributo di S. Thobani, *I requisiti del consenso al trattamento dei dati personali*, Rimini, Maggioli, 2016, 2 ss. Sulla circostanza che spesso l'utente sia posto di fronte alla scelta di prestare il consenso al trattamento dei dati personali o di non poter fruire del servizio, vedi E. Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, 2018, 113. Sulla circostanza che oggi il rilascio del consenso sia spesso un mero esercizio routinario di selezione della casella, L. Moerel, *Big data protection, How to Make the Draft EU Regulation on Data Protection Future Proof*, 2014, 9, in *www.debrauw.com/wpcontent/uploads/NEWS-PUBLICATIONS/Moerel_oratie.pdf*, 24, ove afferma che: "(...) *the granting of consent becomes a mechanical matter of "thicking the box", i.e., becomes*

re formulata con linguaggio chiaro e indicare, oltre a tutti gli elementi richiesti dall'art. 13 del Regolamento (titolare, finalità del trattamento, etc.), che i dati che confluiscono nel fascicolo sono relativi allo stato di salute attuale ed eventualmente pregresso dell'interessato. L'informativa deve, inoltre, indicare il diritto di conoscere quali accessi sono stati effettuati al proprio FSE [37]. Il consenso può essere manifestato (o revocato) direttamente dall'assistito, sia utilizzando strumenti telematici messi a disposizione della regione/PA, previa autenticazione, che mediante dichiarazione resa ad un soggetto delegato dalle Aziende Sanitarie della regione/PA (ad es. MMG/PLS o altri operatori preposti) [38]. La possibilità per le persone fisiche di delegare l'accesso ai pro-

---

subject to 'routinisation' and therefore meaningless"; A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, ESI, 2017, 59; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *I dati personali nel diritto europeo*, a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, Torino, Giappichelli, 2019, 38; C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contratto e impresa*, 2020, 882.

[37] Il nuovo decreto denominato «Fascicolo sanitario elettronico 2.0», entrato in vigore il 24 ottobre 2023, prevede che il Ministero della salute predisponga, in collaborazione con le regioni e province autonome, un modello di informativa (art. 7, comma 4, dello schema di decreto). Tale modello di informativa dovrà tener conto delle peculiarità proprie delle due soluzioni architetturali del FSE individuate nell'allegato C o dell'eventuale supporto in sussidiarietà del sistema FSE-INI offerto dal MEF, assicurando che, come indicato dallo schema di decreto, la regione/provincia autonoma dia adeguata pubblicità alla scelta del modello architetturale del FSE adottato (cfr. artt. 4, comma 5 e 5, comma 4. dello schema di decreto), nonché alle modalità di alimentazione e consultazione del FSE (art. 27, comma 1, dello schema di decreto). Il predetto modello dovrà poi essere aggiornato a seguito dell'attuazione alle disposizioni relative, in particolare, al FSE, alla medicina predittiva, all'interconnessione dei sistemi informativi, al ruolo del Sistema TS, ai servi resi da EDS e all'interconnessione del FSE con le infrastrutture nazionali e regionali di telemedicina.

[38] L'art. 11 del decreto Fascicolo sanitario elettronico 2.0 contempla la possibilità per l'interessato di delegare altri soggetti alla consultazione del FSE, «come risultanti dall'Anagrafe consensi e revoche, nelle more della disponibilità del Sistema di gestione deleghe». Nel decreto 24 ottobre 2023, sempre all'art. 11, sono descritti i trattamenti di dati connessi all'esercizio dell'istituto della delega, individuando le rispettive titolarità del trattamento, le fattispecie legate all'accesso di un FSE di un

pri dati sanitari a rappresentanti autorizzati, garantisce che anche i soggetti che necessitano di assistenza possano beneficiare dei servizi digitali di gestione delle informazioni mediche. Questo aspetto è di particolare rilevanza per le persone con disabilità, gli anziani o coloro

---

minore o di soggetto sottoposto alle forme di tutela previste dal codice civile, definendo puntualmente, nelle more della realizzazione del Sistema Gestione Deleghe di cui all'articolo 64-*ter* del CAD, il numero massimo di deleghe consentite sia al delegante che al delegato, le procedure utilizzabili per effettuare la delega, il suo rinnovo e revoca, la durata di validità e l'ambito di operatività della delega che – in ogni caso – esclude l'accesso ai dati soggetti a maggior tutela. Viene definito insomma in modo puntuale l'intero processo della delega nell'ambito del quale prevedere moduli o procedure *on-line standard* a supporto degli interessati. Il Garante, già nel 2017, aveva formulato, nel senso poi adottato nel nuovo decreto, specifiche osservazione sull'istituto della delega connesso alla consultazione del FSE (nota del 12 giugno 2017, prot. n. 20885). La delega può essere modulata, in modo che al delegato possa essere conferito il potere massimo, cioè i medesimi privilegi dell'assistito sul proprio FSE, oppure, in modo singolo o combinato, diversi poteri e facoltà di operare sul FSE. In nessun caso, il delegato accede ai dati di cui all'art. 6. Cfr. poi, sulla stessa direttrice, il Considerando 21 del Regolamento EHDS, di cui si tratterà *infra* al capitolo IV, secondo cui «Le persone fisiche dovrebbero poter fornire un'autorizzazione ad altre persone fisiche di loro scelta, come a parenti o ad altre persone fisiche loro vicine, che permetta a queste persone di loro scelta di accedere ai dati sanitari elettronici personali delle persone fisiche che forniscono l'autorizzazione o di controllarne l'accesso, oppure di utilizzare servizi di sanità digitale per loro conto. Tali autorizzazioni potrebbero anche risultare utili per altri usi alle persone fisiche che ricevono l'autorizzazione. Per consentire e attuare tali autorizzazioni è opportuno che gli Stati membri istituiscano servizi di delega che dovrebbero essere collegati a servizi di accesso ai dati sanitari elettronici personali, quali portali per i pazienti o applicazioni per dispositivi mobili rivolte ai pazienti. I servizi di delega dovrebbero anche permettere ai tutori di agire per conto dei loro tutelati, compresi i minori; in tali situazioni le autorizzazioni potrebbero essere automatiche. Oltre ai servizi di delega, gli Stati membri dovrebbero istituire anche servizi di assistenza facilmente accessibili forniti da personale adeguatamente formato per assistere le persone fisiche nell'esercizio dei propri diritti. Al fine di tenere conto dei casi in cui la visualizzazione, da parte dei tutori, di alcuni dati sanitari elettronici personali dei loro tutelati possa essere contraria agli interessi o alla volontà dei tutelati, compresi i minori, gli Stati membri dovrebbero poter prevedere nel diritto nazionale limitazioni e garanzie, nonché meccanismi per la loro attuazione tecnica».

che necessitano di un supporto nella gestione delle proprie cure. La possibilità di nominare un rappresentante offre maggiore flessibilità e garantisce che le informazioni sanitarie possano essere consultate e utilizzate nel rispetto delle esigenze del paziente. Il citato regolamento prevede, poi, che sia «responsabilità dei professionisti o degli operatori sanitari che erogano la prestazione acquisire l'esplicito consenso dell'assistito» (art. 5, comma 2).

Il tutto deve ovviamente avvenire in modo conforme alle previsioni del Regolamento relative ai requisiti del consenso richiamate anche dal Comitato europeo per la protezione dei dati [39]. La specificità del consenso è strettamente correlata alla particolare finalità perseguita e alla «granularità» delle richieste previste, anche al fine di scongiurare il rischio noto come "*function creep*", ovvero di uso non previsto di dati personali da parte del titolare del trattamento o di terzi e la perdita del controllo da parte dell'interessato (cfr. punto 3.2 delle predette Linee guida). In caso di «consenso per finalità diverse», precisa l'EPDB, si deve «prevedere una possibilità di adesione distinta per ciascuna finalità, in modo da consentire all'utente di esprimere un consenso specifico per le finalità specifiche». Il rispetto di tali requisiti impone quindi che le manifestazioni di volontà richieste dal citato art. 12 del D.L. n. 179/2012 siano esprimibili disgiuntamente nei confronti dei trattamenti effettuati per finalità di diagnosi, cura e riabilitazione (art. 12, comma 2, lett. a)), di prevenzione (successiva lett. a-*bis*)) e di profilassi internazionale (successiva, lett. a-*ter*)). Alla luce di tali direttive, fatte proprie dal Garante privacy nel proprio parere negativo del 22 agosto

[39] Cfr., art. 7 del Regolamento e Linee guida n. 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, Versione 1.1, adottate dal Comitato europeo per la protezione dei dati il 4 maggio 2020. Tali linee guida sono consultabili in *www.edpb.europa.eu*. Con riguardo alla revoca del consenso nello specifico contesto in esame, cfr., *ex multis*, S. MAZZAMUTO, *Il principio del consenso e il problema della revoca,* in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, I, Milano, Giuffrè, 2006, 993 ss.; G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Rivista critica di diritto privato,* 2000, 299 s.

2022[40], la disposizione sul consenso nel decreto Fascicolo sanitario elettronico 2.0 è stata quindi completamente riformulata, disponendo che le manifestazioni di volontà richieste siano appunto esprimibili disgiuntamente nei confronti dei trattamenti effettuati per diverse finalità. Come richiesto dall'Autorità, sono state, inoltre, definite – per ciascuna manifestazione di volontà – le conseguenze della revoca del consenso, le modalità di espressione, anche in relazione ai minori e ai soggetti sottoposti a tutela, e di alimentazione dell'anagrafe dei consensi[41].

---

[40] Cfr. Parere Garante Privacy 22 agosto 2022, n. 294, in *www.garanteprivacy.it* (*doc-web 9802729*). In merito alla previsione dell'art. 12, comma 2, lett. a-*bis*, del D.L. n. 179/2012, secondo cui il consenso dell'interessato è richiesto per il trattamento dei dati del FSE per finalità di prevenzione perseguibili dagli Uffici delle Regioni e delle Province autonome competenti in materia di prevenzione sanitaria e dal Ministero della salute e per finalità di profilassi internazionale (successiva lettera a-*ter*)) perseguibili dal solo Ministero della Salute, il Garante *privacy* aveva richiamato quanto indicato nel Considerando n. 43 del GDPR, ribadito anche dal Comitato europeo nelle citate linee guida (cfr. punto 3.1, n. 15), secondo cui «per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. Al riguardo, il Comitato, nel ricordare l'esistenza di basi giuridiche più appropriate per i trattamenti effettuati da autorità pubbliche, evidenzia che quando il trattamento è effettuato da tali soggetti «sussiste spesso un evidente squilibrio di potere nella relazione tra il titolare del trattamento e l'interessato, non disponendo quest'ultimo di «alternative realistiche all'accettazione (dei termini) del trattamento».

[41] In merito al trattamento dei dati effettuato per la tutela di un interesse vitale dell'interessato incapace di prestare il proprio consenso (art. 9, par. 1, lett. c) del Regolamento), nei casi di emergenza sanitaria (art. 12, comma 5, D.L. n. 179/2012) e nei casi in cui l'interessato sia in pericolo di vita, si evidenzia che i professionisti dell'emergenza che hanno in cura il paziente, verificata la sua incapacità fisica o giuridica di esprimere il consenso, possono accedere alla partizione del FSE denominata Profilo sanitario sintetico (o *patient summary*), ovvero a quella sezione del Fascicolo redatta e aggiornata dal medico di base o dal pediatra di libera scelta, che «riassume la storia clinica dell'assistito e la sua situazione corrente conosciuta» al fine «di

Il nuovo regolamento FSE 2.0, inoltre, nel distinguere le diverse tipologie di trattamenti, cioè per finalità di cura, per finalità di ricerca e per finalità di governo, definisce anche regole diverse per l'accesso alle informazioni contenute nel FSE e sui dati che possono essere trattati, proprio sulla base della finalità e quindi del soggetto che vi accede [42]. A ben vedere, il progetto di sanità digitale che ruota attorno

favorire la continuità di cura, permettendo un rapido inquadramento dell'assistito al momento di un contatto con il SSN» (art. 4 del decreto Fascicolo sanitario elettronico 2.0). Tale partizione del FSE consente di recuperare in un unico documento informazioni complete circa gli aspetti clinici e sanitari rilevanti dell'interessato relativi, ad esempio, all'attuale situazione clinica, per inquadrare prontamente lo stato di salute di un interessato. La formulazione in ordine all'accesso in emergenza al FSE è risultata convincente anche per il Garante (parere Garante *Privacy* 8 giugno 2023 n. 256, *docweb 9900433*, in *www.garanteprivacy.it*), essendo stata redatta sulla base di una valutazione tecnico scientifica, e avendo previsto, anche tecnicamente, un accesso al FSE in emergenza graduale, ovvero dapprima al solo PSS e, nel caso in cui questo non sia sufficiente, all'intero FSE, limitatamente al tempo strettamente necessario ad assicurare le cure emergenziali all'interessato e sempre nel rispetto del diritto di oscuramento eventualmente esercitato.

[42] È stato ora previsto nel decreto denominato «Fascicolo sanitario elettronico 2.0» che, nell'ambito del perseguimento delle finalità di prevenzione da parte delle regioni/province autonome e del Ministero, l'accesso al FSE sia limitato, mediante livelli diversificati di accesso, solo al personale sanitario sottoposto alle regole del segreto professionale non coincidente con quello che, per altre finalità, accede a flussi di dati pseudonimizzati, al fine di ridurre il rischio di re-identificazione dell'interessato (art. 16 del decreto e dell'allegato A). Con riferimento al profilo oggettivo dell'accesso, come richiesto dal Garante, alla luce dei principi di minimizzazione e trasparenza, è stato previsto che gli Uffici della Direzione generale del Ministero della salute competente e gli Uffici delle Regioni competenti possano accedere esclusivamente ai metadati dei documenti del FSE, privati degli elementi identificativi diretti e pseudonimizzati, al fine di pianificare, rispettivamente, le attività di prevenzione in ambito nazionale e quelle di prevenzione nel relativo ambito territoriale che saranno in ogni caso attuate dalle competenti ASL (art. 17 decreto). Si dà conto che, nel rispetto dei predetti principi, è stato previsto che siano comunque sottratti all'accesso, per le finalità di prevenzione, i dati per i quali l'assistito abbia richiesto l'oscuramento, nonché i metadati relativi al PSS e al TP dell'assistito (art. 17 decreto). Anche per le finalità di profilassi internazionale perseguite dal Ministero della salute, non erano state indicate le modalità e i livelli diversificati di accesso ai dati

al FSE, e di cui il decreto FSE 2.0 è parte fondante, mantiene un mo-

---

e ai documenti del FSE. La disposizione sul perseguimento delle finalità di profilassi internazionale da parte del Ministero della salute è stata pertanto interamente riformulata indicando, come richiesto dal Garante, la tipologia di soggetti tenuti al «segreto professionale» che possono trattare i dati ed i documenti del FSE, sulla base di uno specifico e valido consenso dell'interessato, nonché le misure idonee a scongiurare il rischio di re-identificazione dell'interessato. In merito a tali profili, è stato in particolare previsto che possa accedere al FSE esclusivamente il personale medico sottoposto alle regole del segreto professionale operante presso la Direzione generale del Ministero competente in materia di profilassi internazionale (designata quale Centro Nazionale Italiano per il Regolamento sanitario internazionale) che non sia coincidente con il personale che accede, per altre finalità, ai flussi di dati pseudonimizzati di cui è destinatario lo stesso Ministero (art. 18 del decreto e allegato A). È stato pertanto previsto che, per assicurare la massima sicurezza contro la diffusione internazionale delle malattie infettive e fronteggiare eventi di sanità pubblica inaspettati, il personale sanitario operante presso la predetta Direzione generale del Ministero della salute, previo consenso espresso dell'interessato, possa trattare i soli dati e documenti del FSE rilevanti al fine di individuare: a) la circolazione di nuovi patogeni o l'emergere di sintomatologie sconosciute o di fattori di rischio ambientale e/o alimentare; b) nuovi fattori di rischio legati a patologie correlate come coinfezioni; c) lo sviluppo di nuovi casi di farmacoresistenza verso specifici gruppi di patogeni; d) possibili nuove complicanze non conosciute di alcune malattie infettive che possono portare al decesso (art. 19 del decreto). I predetti medici, ivi compresi quelli operanti presso gli Uffici di Sanità Marittima e Aerea e di Frontiera, possono accedere ai dati e ai documenti del FSE solo se la consultazione risulti necessaria per la valutazione della situazione sanitaria dei soggetti destinatari delle seguenti azioni di competenza del Ministero: a) somministrare vaccinazioni o profilassi obbligatorie o raccomandate per soggetti diretti all'estero, su richiesta degli interessati; b) somministrare vaccinazioni o profilassi obbligatorie o raccomandate per soggetti provenienti dall'estero segnalandoli alle ASL territorialmente competenti; c) sottoporre a misure di quarantena o isolamento segnalandoli alle ASL territorialmente competenti; d) effettuare attività di contact tracing internazionale segnalandoli alle ASL territorialmente competenti; e) disporre misure di profilassi conseguenti a esposizioni ad agenti patogeni relative a soggetti che abbiano utilizzato mezzi di trasporto collettivi o soggiornato in comunità chiuse segnalandoli alle ASL territorialmente competenti (art. 19 del decreto). Nei casi di cui alle precedenti lettere b), c), d) ed e), su richiesta dell'Ufficio, è stato previsto che il Ministero della salute definisca preventivamente e documenti i criteri e le modalità per l'identificazione dei soggetti esposti o che espongono terzi a gravi minacce per la salute e che siano comunque sottratti all'ac-

dello volontaristico e «consensocentrico», perlomeno per la consultazione dei dati da parte degli operatori sanitari, per finalità specifiche quali diagnosi, cura e riabilitazione, oltre che finalità di prevenzione e profilassi internazionale. Quello del «consenso», peraltro, è più un mito o una parvenza di tutela, quantomeno lo è il consenso inteso nel senso di base giuridica per la legittimità del trattamento dei dati personali, e sono pertanto stati individuati altri strumenti, forse più funzionali, diversi da esso [43]. E la scelta, nell'ambito del GDPR, è ri-

---

cesso i dati per i quali l'interessato abbia richiesto l'oscuramento (art. 19 del decreto). In merito ai trattamenti effettuati per finalità di governo sanitario, il Ministero ha ritenuto di espungerne dal decreto la disciplina. E per essi rimangono in vigore le relative disposizioni di cui al d.P.C.M. n. 178/2015, fino all'adozione di ulteriori e specifici decreti che saranno adottati ai sensi dell'art. 12, comma 7, del D.L. n. 179 del 2012.

[43] Cfr. A.M. GAROFALO, *Regolare l'irregolabile: il consenso al trattamento dei dati nel GDPR*, in S. ORLANDO, G. CAPALDO (a cura di), Annuario 2021, Osservatorio Giuridico sulla innovazione Digitale, Roma, Sapienza Università editrice, 2021, 122 ss. Ma vedi già G. ALPA, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in V. CUFFARO, V. RICCIUTO, V. ZENO ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffrè, 1999, 26; F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 101 ss.; G. FINOCCHIARO, *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, in G.F. FERRARI (a cura di), *La legge sulla privacy dieci anni dopo*, Milano, Egea, 2008, 213.; V. ZAMBRANO, *Dati sanitari e tutela della sfera privata*, in *Diritto dell'informazione e dell'informatica*, 1999, 27. Esprimono peraltro perplessità verso il progressivo generale abbandono della regola del consenso, A. THIENE, *La regola e l'eccezione. Il ruolo del consenso in relazione al trattamento dei dati sanitari alla luce dell'art. 9 GDPR* , in A. THIENE, S. CORSO, *La protezione dei dati sanitari privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, Napoli, Jovene, 2023, 7 ss. Sul consenso dell'interessato e sul rapporto fra consenso al trattamento di dati comuni e consenso al trattamento di dati sensibili, vedi G. DE CRISTOFARO, *Die datenschutzrechtliche Einwilligung als Gegenstand des Leistungsversprechens*, in F. PADOVINI, T. PERTOT, M. SCHMIDT KESSEL, (a cura di), *Rechte an Daten*, Tübingen, Mohr Siebrek, 2020, 151 ss. Critico verso un modo tradizionale di intendere la *privacy* in ambito sanitario, E. MAESTRI, *Il feticcio della privacy nella sanità. Cura del paziente e biobanking genetico prima e dopo l'entrata in vigore del GDPR*, in A. THIENE, S. CORSO (a cura di), *La*

caduta su una serie di misure e accorgimenti, anche di natura tecnica, che poi si sono tradotti in principi e regole che possono, in larga parte, ricondursi al concetto di sicurezza. Si pensi al principio di *accountability*, la responsabilizzazione dei soggetti che operano il trattamento dei dati; alle nozioni di *privacy by design* e *privacy by default*; alle procedure di pseudonimizzazione e ai meccanismi di valutazione del rischio. Peraltro, sin dagli albori della riflessione in tema di protezione dei dati personali, si era colta l'inconsistenza del consenso dell'interessato al trattamento come dispositivo di controllo nella circolazione dei dati. È stato messo in luce, infatti, come il più delle volte il consenso sia prestato senza nessuna consapevolezza, con disattenzione. E, ancora, qualora tale consapevolezza vi sia, la scelta viene ad essere vincolata, pena la non erogazione del servizio connesso al trattamento. Del consenso si è parlato in termini di paradosso. E tutto ciò assume tratti forse anche più marcati nel contesto sanitario, se si considera che non può aversi trattamento sanitario, in assenza di trattamento di dati relativi alla salute del paziente, da parte del medico [44].

Gli interventi del legislatore, soprattutto i più recenti, sembrano comunque aver sancito il passaggio del FSE, da strumento principalmente per la persona e per la tutela dei suoi diritti fondamentali, primo fra tutti quello alla sua salute, a strumento votato anche a garantire

---

protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza, cit., 23 ss.

[44] La Suprema Corte ha affermato che il consenso al trattamento non è libero se prestato per ottenere un servizio infungibile e irrinunciabile (Cass. civ., 2 luglio 2018 n. 17278, in *Dejure*. Nello stesso senso, *ex multis*, C. Irti, *Consenso "negoziato" e circolazione dei dati personali*, Torino, Giappichelli, 2021, 96, e P. Gallo, *Il consenso al trattamento dei dati personali come prestazione*, in *Rivista di diritto civile*, 2022, 1079). Secondo tale arresto, per "infungibile" s'intende un servizio inaccessibile senza trattamento dei dati. Il servizio deve essere anche irrinunciabile senza un gravoso sacrificio da parte dell'utente, in quanto "essenziale" (come nel caso di servizi sanitari e bancari), giacché il mero desiderio di un servizio rinunciabile non può essere ritenuto sufficiente a coartare il consenso. In tal senso, vedi V. Bachelet, *Il contratto di scambio di "servizi contro dati" (o contro prezzo)*, in *Rivista di diritto civile*., 2024, 1130.

una maggiore efficienza, nel contesto del funzionamento del Servizio sanitario nazionale.

E ciò si denota dalla scelta di superare il consenso, laddove l'utilizzo del FSE abbia finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico, o di programmazione sanitaria, verifica di qualità delle cure e valutazione dell'assistenza sanitaria. La protezione dei dati è concepita, in tali casi, secondo un paradigma circolatorio differente, informato al principio di solidarietà [45], oltre la dicotomia persona e mercato, sottesa alla doppia anima del regolamento generale sulla protezione dei dati [46], si realizza così la funzione sociale del diritto alla protezione dei dati personali, che, come espresso al *considerando* n. 4, GDPR, non è prerogativa assoluta e va contemperato con altri diritti fondamentali [47].

In questo sistema, massima rilevanza acquisisce il potere di controllo in capo all'interessato sui propri dati personali, che si esprime attraverso tre diritti: il diritto di accesso ai dati e documenti, esercitabile utilizzando i servizi del portale nazionale FSE 2.0, i diritti di integrazione, rettifica e aggiornamento dei propri dati, il diritto di oscuramento dei propri dati nel FSE 2.0. In linea generale, l'interessato, ai

---

[45] Cfr. M. CIANCIMINO, *Circolazione "secondaria" di dati sanitari e biobanche. Nuovi paradigmi contrattuali e istanze personalistiche*, in *Diritto di famiglia e delle persone*, 2022, 68; C. RAPISARDA, *Ricerca scientifica e circolazione dei dati personali. Verso il definitivo superamento del paradigma privatistico?*, in *Europa e diritto privato*, 2021, 335 ss. Sul principio di solidarietà, *ex plurimis*, G. ALPA, *Solidarietà. Un principio normativo*, Bologna, Il Mulino, 2022.

[46] N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla* privacy, in ID. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, Wolters Kluwer, 2019, 35 ss. Cfr. E. TOSI, *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del* nuovo *Codice Privacy*, in ID. (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Lefebvre Giuffrè, 2019, 1 ss.

[47] Cfr. A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2017, 586 ss. In dottrina, è stato rilevato che, con «funzione sociale», il GDPR fa riferimento ad esigenze di «interesse pubblico» (Cfr., a proposito, F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e impresa*, 2018, 6).

sensi dell'art, 9, commi 3-7, del regolamento FSE 2.0, ha il diritto di richiedere l'oscuramento dei dati e dei documenti sanitari e sociosanitari sia prima dell'alimentazione del FSE, che successivamente. In quest'ultimo caso, i dati e i documenti oscurati potranno essere consultati esclusivamente dall'interessato e dai titolari che hanno generato i predetti documenti.

Si consideri peraltro che, come tutela preventiva, i dati particolarmente sensibili o «a maggior tutela» sono caricati automaticamente in forma oscurata nel fascicolo (Cfr. anche art. 6 del decreto FSE 2.0) [48]. L'art. 6 del decreto FSE 2.0, rubricato così come l'art. 5, d.p.c.m. n. 178/2015 «Dati soggetti a maggiore tutela dell'anonimato», sancisce, infatti, che siano resi visibili solo all'assistito «i dati e i documenti sanitari e socio-sanitari disciplinati dalle disposizioni normative a tutela delle persone sieropositive, delle donne che si sottopongono a un'interruzione volontaria di gravidanza, delle vittime di atti di violenza sessuale o di pedofilia, delle persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, delle donne che decidono di partorire in anonimato, nonché i dati e i documenti riferiti ai servizi offerti dai consultori familiari» [49]. L'assistito potrà decidere liberamente di rendere tali dati visibili a terzi, esercitando i diritti di cui all'art. 9,

---

[48] La distinzione fra dati soggetti a maggior tutela dell'anonimato e gli altri dati – distinzione che il decreto FSE 2.0 eredita dal precedente impianto normativo – merita di essere valorizzata. Se è vero che non tutti i dati personali sono sensibili e che non tutti i dati sensibili sono sensibili allo stesso modo, è vero anche che non tutti i dati relativi alla salute – dati supersensibili – presentano lo stesso livello di sensibilità (Nella giurisprudenza di legittimità, vedi Cass. civ., sez. un., 27 dicembre 2017, n. 30984, in *Giurisprudenza italiana*, 2018, 2639 ss., con nota di A. Ricci; Cass. civ. 11 gennaio 2016, n. 222, in *www.ridare.it*, 10 maggio 2016, con nota di P. Ziviz; Cass. civ. 8 luglio 2005, n. 14390, in *Corriere giuridico*, 2006, 39 ss., con nota di Cirillo. In quella amministrativa, *ex multis*, Cons. Stato 28 marzo 2023, n. 3160, in *Dejure*; Cons. Stato 27 novembre 2015, n. 5378, *ivi*; Cons. Stato, ad. plen., 25 settembre 2020, n. 19, in *www.dirittoegiustizia.it*, 12 ottobre 2020.

[49] Importante anche il novero dei soggetti che mai, in nessun caso, possono consultare il FSE 2.0 di un assistito: periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, organismi amministrativi anche

mediante un consenso esplicito, informato e specifico reso al soggetto che eroga la prestazione.

Nei casi in cui l'oscuramento di dati e documenti avvenga successivamente all'alimentazione del FSE, l'assistito è informato del fatto che le informazioni del dato o documento oscurato possono essere state utilizzate prima dell'oscuramento per la realizzazione di altri documenti, quali il Profilo sanitario sintetico di cui all'art. 4, rispetto ai quali può autonomamente esercitare il medesimo diritto [50].

---

operanti in ambito sanitario, medici legali che devono accertare l'idoneità lavorativa o rilasciare certificazioni necessarie al conferimento di permessi o abilitazioni.

[50] Cfr. Ordinanza-ingiunzione nei confronti di Azienda Usl della Romagna, 27 maggio 2021(*doc. web n. 9682619*), in un caso in cui il Garante privacy è intervenuto a seguito di una notifica della Usl della Romagna, per aver trasmesso quest'ultima ad un medico di famiglia il referto di una paziente che, al momento del ricovero per interruzione farmacologica della gravidanza, ne aveva richiesto l'oscuramento attraverso la compilazione di un apposito modulo. La comunicazione dei dati era avvenuta accidentalmente a causa di un *bug* nel *software* che gestiva l'accettazione, la dimissione e il trasferimento degli assistiti. La comunicazione illecita di dati sulla salute, contro la volontà espressa dai pazienti, aveva interessato 48 persone nell'arco temporale intercorrente tra il mese di aprile 2018 e l'agosto 2019. Cfr., poi, Ordinanza-ingiunzione nei confronti di Azienda provinciale per i servizi sanitari di Trento, 27 maggio 2021 (*doc. web n. 9682641*), in cui l'Azienda Provinciale per i Servizi Sanitari di Trento ha notificato al Garante *privacy* una violazione di dati personali per aver messo a disposizione dei medici di famiglia, per errore, 293 referti di 175 pazienti, tra cui 2 minorenni e alcune donne sottoposte ad interruzione di gravidanza, sebbene questi avessero esercitato il diritto di oscuramento. Anche in questo caso, la violazione è risultata imputabile esclusivamente ad un errore del *software*, che non ha associato ai documenti la richiesta di oscuramento, correttamente inserita dagli operatori sanitari nel Sistema informativo ospedaliero. Pure nel provvedimento nei confronti di Azienda Usl di Bologna - 29 aprile 2021, Reg. provv. n. 175 del 29 aprile 2021 (*doc. web n. 9676172*), tale ente è stato sanzionato dal Garante *privacy* per via dell'inserimento nel FSE di una minore dei documenti relativi alla prestazione erogata da un centro di consultazione per adolescenti, in contrasto con una esplicita richiesta di oscuramento avanzata dall'interessata stessa. Al minore fra i 14 e i 18 anni, peraltro, il legislatore ha riservato la possibilità di operare in autonomia e senza il consenso parentale, in alcune fattispecie tassativamente predeterminate legate alla gestione della propria sfera esistenziale. La *ratio* di questa previsione è lungimirante: in alcuni casi, relativi alla sfera più intima e personale, infatti, il minore può essere

4. *(segue) Titolarità del trattamento, responsabilità della struttura ospedaliera ed eventuale concorso di colpa del paziente «interessato» in caso di malpractice medica*

Il decreto denominato Fascicolo sanitario elettronico 2.0, come richiesto dal Garante, ha delineato, seppur in maniera generica, le responsabilità in caso di mancato oscuramento del dato o documento da parte del soggetto che eroga la prestazione (art. 6, comma 2,: «In assenza del consenso, l'erogatore della prestazione è responsabile dell'eventuale mancato oscuramento del dato o documento mediante l'apposita funzionalità di cui all'art. 9, comma 4)», evidentemente rinviando implicitamente alla disciplina generale di cui all'art. 82 GDPR, disciplina che, a sua volta, risulta non pacifica nella sua interpretazione [51].

Al di là dei casi in cui il singolo professionista opera in via auto-

---

indotto ad evitare di rivolgersi al servizio sanitario, nel timore che il genitore venga a conoscenza di determinate informazioni (in argomento, vedi R. Ducato, U. Izzo, *Diritto all'autodeterminazione informativa del minore e gestione dei dati "supersensibili" nel contesto del Fascicolo Sanitario Elettronico*, in *Diritto dell'informazione e dell'informatica*, 2013, 703 ss.). In queste ipotesi, la tutela della *privacy* del minore è, quindi, intimamente legata alla tutela della sua salute e di quella delle persone che potrebbero venire in contatto con lui. È bene precisare che l'oscuramento dei dati supersensibili non può essere inteso come un muro invalicabile: fonte e limite di questa sfera di autonomia del minore è pur sempre il diritto alla salute. I genitori, quindi, devono essere informati se il proprio figlio minore versa in una situazione patologica tale da necessitare terapie prolungate o interventi suscettibili di diminuire in modo permanente la sua integrità psicofisica ovvero di rappresentare un pericolo potenziale per le persone che vengano in contatto con quest'ultimo (si pensi al caso di sieropositività al virus HIV o ad altra malattia infettiva di rilievo). È all'operatore sanitario che in questi frangenti compete l'obbligo di avvisare il minore di non poter rispettare il vincolo di segretezza, per l'esigenza di fare in modo che il genitore sia pienamente coinvolto nel processo decisionale riguardante la salute del minore.

[51] Si consenta il rinvio, per un riepilogo delle diverse posizioni sulla natura della responsabilità in caso di illecito trattamento dei dati personali, a S. Faillace, *La natura e la disciplina delle obbligazioni di cui all'art. 25 del GDPR, espressione dei principi di privacy by design e di privacy by default*, in *Contratto e impresa*, 2022, 1123 ss.

noma (es. studio professionale), con riferimento ai quali lo stesso riveste la qualifica di titolare dei trattamenti effettuati, quando il sanitario agisce come operatore di una struttura sanitaria, lo stesso non agisce come titolare, bensì come soggetto autorizzato al trattamento dei dati (art. 29 del GDPR). Le pertinenti disposizioni del nuovo decreto FSE 2.0, in conformità a quanto richiesto dall'art. 12, comma 7, del d. l. n. 179/2012, prevedono una distinzione del profilo della titolarità del trattamento da quello legato all'alimentazione del FSE. La chiara indicazione della titolarità di tali trattamenti è del resto un elemento prodromico per delineare le responsabilità in ordine al rispetto dei principi generali e degli adempimenti in materia di protezione dei dati personali, nonché a garantire l'effettivo esercizio dei diritti da parte degli interessati [52]. La valutazione circa il rispetto dei principi generali del GDPR impone, infatti, con un approccio di responsabilizzazione, l'analisi disgiunta di ciascuna delle operazioni effettuate dai diversi soggetti a vario titolo coinvolti nel trattamento per il perseguimento delle finalità loro attribuite dalla normativa primaria. Ciò, soprattutto in considerazione del fatto che, come si vedrà nel prossimo paragrafo, la nuova architettura del FSE/EDS dovrebbe evitare una duplicazione di dati sanitari di tutta la popolazione assistita sul territorio nazionale, e su tale punto si impone il rigoroso rispetto di specifiche misure volte a garantire in concreto l'esattezza, l'integrità e l'aggiornamento dei dati e soprattutto la tutela dei diritti fondamentali degli interessati. Appare evidente, peraltro, come il singolo professionista sanitario, operante all'interno di una struttura sanitaria, nell'alimentare il FSE con i documenti sanitari dallo stesso prodotti nell'ambito del processo di cura dell'interessato, non possa essere qualificato come titolare del trattamento, non determinando le finalità e i mezzi dello stesso, né tantomeno possano essere allo stesso attribuiti i compiti e le responsabilità derivanti dall'assunzione di tale ruolo. Sono, invece, tito-

[52] Cfr. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version* 1.0, adottate il 2 settembre 2020 dal Comitato Europeo per la protezione dei dati.

lari del trattamento per finalità di cura le aziende sanitarie locali, le strutture sanitarie pubbliche del SSN, i servizi sociali sanitari regionali e del SSN e le strutture sanitarie autorizzate ed esercenti le professioni sanitarie.

Si è quindi rimediato alla confusione presente nello schema di decreto tra titolare del trattamento (inteso come fonte di determinazione delle finalità e dei mezzi del trattamento) e soggetto autorizzato ad alimentare e consultare il fascicolo, con particolare riferimento alla disciplina relativa al profilo sanitario sintetico (PSS), alle prescrizioni farmaceutiche e specialistiche, al dossier farmaceutico [53] e al taccuino personale [54].

---

[53] Il dossier farmaceutico è una sezione del FSE, aggiornata a cura della farmacia, che consente di tracciare ed eventualmente ricostruire la storia farmacologica dell'assistito, oltre che di monitorare l'appropriatezza nella dispensazione dei medicinali e l'aderenza alle terapie. Con specifico riferimento a tale documento, nel parere del 7 aprile 2022, l'Autorità Garante aveva rappresentato la necessità che lo schema di decreto evidenziasse la titolarità dei trattamenti, ove risiedessero i dati e i documenti e i soggetti che possono accedervi e per quali finalità. L'art. 6 dello schema di decreto sul FSE risultava invece privo di tutti i predetti elementi. All'art. 5 del decreto EDS si stabilisce poi che l'EDS medesimo gestirà il dossier farmaceutico, estraendo dati relativi a prescrizioni ed erogazioni di farmaci per migliorare l'assistenza al paziente. L'accesso a questi dati sarà consentito solo su richiesta e non costituirà una banca dati permanente, garantendo così un utilizzo mirato e sicuro delle informazioni.

[54] Il Taccuino personale è un'area specifica del FSE nella quale ciascun paziente o un suo delegato può inserire modificare ed eliminare dati e documenti relativi al proprio percorso di cura, garantendone l'esattezza e l'eventuale aggiornamento. Si tratta di un elemento integrativo che assicura la partecipazione attiva dell'assistito alla costruzione del proprio *database* sanitario, soprattutto tramite inserimento di informazioni riguardanti prestazioni pregresse. La disposizione, inoltre, precisa, come richiesto dal Garante, che, indipendentemente dal modello architetturale di FSE adottato, la Regione di assistenza sia considerata titolare del trattamento dei documenti del TP, ivi compresa l'adozione delle relative misure di sicurezza, fermo restando che al predetto titolare non è consentita la consultazione dei dati ivi contenuti. Nel taccuino personale, con il decreto sul FSE 2.0, potranno confluire i dati generati da dispositivi medici e *wearable*. Il FSE si apre quindi alla c.d. *m-Health* e

L'assenza di una disciplina organica in ordine agli obblighi di alimentazione e consultazione del FSE da parte dei professionisti sanitari poneva pure la necessità di definire nel decreto, come del resto indicato anche nell'art. 12, comma 7, del d.l. n. 179/2012, il quadro delle responsabilità in caso di mancato aggiornamento o rettifica dei dati. Tali elementi, infatti, incidono in merito al rispetto dei principi di protezione dei dati, in particolare di quelli di completezza, esattezza, aggiornamento e sicurezza previsti dal GDPR (art. 5). E su tale ultimo aspetto l'art. 12, comma 3, del decreto «fascicolo sanitario elettronico 2.0» prevede un onere in capo alle strutture sanitarie di alimentare il FSE entro cinque giorni dall'erogazione della prestazione sanitaria, affiancato da una connessa responsabilità in caso di mancata, intempestiva o inesatta alimentazione [55]. Appare chiaro come tale ultima condotta, così come la violazione dell'obbligo di controllare la completezza e la correttezza del fascicolo sanitario elettronico possano configurare un inesatto adempimento della prestazione sanitaria, da parte della struttura ospedaliera [56], per mano del personale suo au-

---

al connesso uso di *App*, per *smartphone*, *smartwatch* e *tablet*. Vedi la ricostruzione critica, a riguardo, di C. IRTI, *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano*, in *Persona e mercato*, 2023, 32 ss. Cfr. C. RAPISARDA, *La* privacy *sanitaria alla prova del* mobile ecosystem. *Il caso delle* app *mediche*, in *Le nuove leggi civili commentate*, 2023, 184 ss.

[55] L'introduzione di uno specifico onere e delle connesse responsabilità in capo ai soggetti alimentanti risponde anche alla generale osservazione formulata dall'Autorità Garante nel citato parere dell'agosto 2022 in ordine al rispetto del principio di proporzionalità del trattamento. Il Garante aveva infatti segnalato che non risultava proporzionata la scelta di realizzare uno strumento informativo, come il FSE, in cui rendere disponibili tutti i dati e i documenti relativi alla storia sanitaria di un individuo, con lo scopo di fornire uno scenario generale della salute dello stesso ai professionisti sanitari che lo prendono in cura, senza che gli stessi fossero tenuti ad alimentarlo.

[56] Secondo Cass. civ., sez. III, 5 luglio 2004, n. 12273, in *Giurisprudenza italiana*, 2005, 1409 ss., il medico ha, tra i suoi diversi obblighi, quello di controllare la completezza e l'esattezza della cartella clinica, la cui violazione configura difetto di diligenza ex art. 1176, comma 2, c.c. ed inesatto adempimento della corrispondente prestazione medica (conf. Cass. civ., sez. III, 18 settembre 2009, n. 20101, in *Giu-*

siliario, ex art. 1228 c.c. [57]. Nel caso di specie, ritengo possa configurarsi, infatti, un inadempimento del contratto di «spedalità» tra paziente e struttura sanitaria, vale a dire quel contratto atipico, pacificamente riconosciuto dalla giurisprudenza, che pone a carico della struttura sanitaria, oltre alla prestazione principale di tipo diagnostico-terapeutico, una serie di altre prestazioni che, contribuendo a riempire di contenuto il concetto di «efficiente *standard* organizzativo», influiscono sulla delimitazione dei confini della responsabilità. La struttura sanitaria, infatti, oltre e anche a prescindere dalla responsabilità indiretta per le condotte del personale medico operante al suo interno, ha una diretta e autonoma responsabilità per c.d. difetto di organizzazione. Pertanto, le obbligazioni della struttura sono estese alla sicurezza delle attrezzature, dei macchinari, alla vigilanza, alla custodia dei pazienti (oltre a prestazioni più propriamente riconducibili al contratto d'albergo per-

---

stizia civile Mass., 2009, 9, 1329; si vedano, in merito, anche gli artt. 5 e 7 del d.P.R. 27 marzo 1969 n. 128, in tema di soggetti responsabili della compilazione e conservazione della cartella clinica).

[57] Diverso il discorso invece nel caso in cui venga ritardato l'accesso al fascicolo sanitario elettronico per un periodo di tempo limitato, ad esempio, fino al momento in cui il paziente e l'operatore entrino in contatto, avendo mente al fatto che potrebbe non essere etico informare un paziente attraverso un canale elettronico di una diagnosi di una malattia incurabile, che probabilmente porterà alla sua rapida scomparsa, invece di fornire prima queste informazioni in una consultazione con il paziente. Di tale ipotesi, si occupa in maniera dubitativa il Considerando n. 10 reg. EHDS, secondo cui: «l'accesso immediato delle persone fisiche ad alcune categorie dei propri dati sanitari elettronici personali potrebbe essere dannoso per la loro sicurezza o non etico. Ad esempio potrebbe non essere etico informare un paziente attraverso un canale elettronico in merito alla diagnosi di una malattia incurabile che probabilmente sarà terminale anziché prima comunicare tale informazione in un colloquio con il paziente. Pertanto, in tali situazioni, dovrebbe essere possibile ritardare la fornitura dell'accesso ai dati sanitari elettronici personali per un periodo limitato, ad esempio fino al momento in cui il professionista sanitario possa spiegare la situazione al paziente. Gli Stati membri dovrebbero essere in grado di fissare tale eccezione laddove costituisca una misura necessaria e proporzionata in una società democratica, in linea con le limitazioni previste all'articolo 23 del regolamento (UE) 2016/679».

ché attinenti a vitto-riscaldamento-alloggio) e, perché no, anche alle prestazioni di corretta tenuta del fascicolo sanitario elettronico e della cartella clinica. [58]

Sotto altro profilo, vi è da aggiungere che, nell'ipotesi in cui il paziente non conceda o revochi l'assenso al medico curante e/o alla struttura alla consultazione del proprio fascicolo sanitario elettronico, ciò potrebbe impedire al medico che prende in cura il paziente di acquisire informazioni utili per una terapia appropriata.

---

[58] L'accettazione del paziente in ospedale, ai fini del ricovero o di una visita ambulatoriale, comporta la conclusione di un contratto, il contratto atipico di spedalità. La struttura sanitaria può essere chiamata a rispondere sia per fatto proprio – nei casi di danno al paziente derivante da disfunzione o carenze strutturali e/o organizzative inerenti alla struttura stessa – sia per fatto del personale sanitario – nei casi di negligenza e imperizia del personale sanitario/parasanitario nell'ambito dell'esecuzione della prestazione. In quest'ultima ipotesi, la struttura sanitaria risponde dell'attività attuata dall'operatore sanitario, laddove in questa sia ravvisabile almeno la colpa. Tale impostazione è stata confermata dal legislatore, con la L. 8 marzo 2017, n. 24 (c.d. Legge Gelli-Bianco), che, appunto, prevede una responsabilità per inadempimento della struttura sanitaria – pubblica o privata – per fatto proprio, sia in termini di organizzazione sia per grave *malpractice* del medico di cui si avvale, ed extracontrattuale per gli esercenti le professioni sanitarie. Secondo i rinnovati criteri, la struttura è tenuta quindi a corrispondere al paziente le somme a titolo di risarcimento danni ai sensi degli artt. 1218 e 1228 c.c. per *medical malpractice* (art.7, L. 17 marzo 2017, n. 24). Sul punto, vedi M. FACCIOLI, *La responsabilità civile per difetto di organizzazione delle strutture sanitarie*, Pisa, Pacini, 2018; A. ASTONE, *Responsabilità sanitaria ed emergenza pandemica*, in *Diritto di famiglia e delle persone*, 2022, 731. La natura complessa della prestazione che sorge dal contratto di spedalità è stata sottolineata in dottrina anche da M. BIONDI, *Contratto di spedalità e responsabilità della struttura sanitaria*, in *Contratti*, 2022, 447. Ma la tesi del contratto atipico di spedalità era stata sostenuta in passato già da F. GALGANO, *Contratto e responsabilità contrattuale nell'attività sanitaria* in *Rivista trimestrale di diritto e procedura civile*, 1984, 710, che richiamò lo schema della *locatio operis;* M. BILANCETTI, *La responsabilità penale e civile del medico*, Padova, Cedam, 1996, 312 ss.; R. DE MATTEIS, *La responsabilità medica tra prospettive comunitarie e nuove tendenze giurisprudenziali*, in *Contratto e impresa,* 1995, 488. Tale ricostruzione è seguita pure dalla giurisprudenza della Suprema Corte. Cfr., *ex multis*, Cass. civ., Sez. un., 11 gennaio 2008, n. 577, in *altalex.it*, e da ultimo, vedi Cass. Civ. 3 marzo 2023 n.6386, in *Dejure*.

Se poi le cure non fossero risolutive e il paziente dovesse invocare una responsabilità del medico e/o della struttura, è lecito chiedersi se la struttura ospedaliera possa eccepire un concorso di colpa del paziente, ove dimostri di non aver potuto accedere ad informazioni sulla salute del paziente che avrebbero potuto modificare l'anamnesi e/o la diagnosi e, quindi, il trattamento terapeutico programmato. [59] Non è inoltre da escludere che, in applicazione dei principi generali della responsabilità civile, il comportamento del paziente possa sollevare da ogni responsabilità il medico, qualora il suddetto comportamento sia tale da elidere la rilevanza casuale della condotta del sanitario nella produzione dell'evento lesivo subito dal malato. [60]

---

[59] Sull'argomento, vedi N. Bortolotti, A. Verzeletti, A. Antonietti, *Il concorso di colpa del paziente in ipotesi di responsabilità professionale medica*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2018, 1343 ss. In generale sul concorso di colpa del creditore, vedi V. Caredda, *Concorso del fatto colposo del creditore, art. 1227, Il codice civile commentario*, già diretto da P. Schlesinger e continuato da F.D. Busnelli e G. Ponzanelli, Milano, Giuffrè Lefebvre, 2020.

[60] In senso contrario, però, in fattispecie solo per certi versi analoghe, cfr. Cass. 20 novembre 2020, n. 26426, in *Dejure*, che afferma che il paziente, eccetto omissioni a fronte di specifiche richieste del medico in sede di anamnesi, non può ritenersi avere responsabilità per le carenze della medesima, non rientrando tra i propri obblighi né avere specifiche cognizioni di scienza medica, né sopperire ad accertate mancanze investigative del professionista (Nella specie, la S.C. ha cassato la decisione di merito che, accertata la responsabilità dei sanitari per omessa diagnosi della condizione di portatrice sana di talassemia in capo ad una donna in stato di gravidanza, divenuta madre di due gemelle affette da talassemia *maior*, aveva affermato la concorrente responsabilità di quest'ultima e del di lei marito, perché, consapevoli della condizione di portatore sano in capo a quest'ultimo, si erano rivolti ai medici per assicurarsi che non fosse tale anche lei ma, pur essendo a conoscenza di una patologia ematica, definita microcitemia, tra i collaterali della donna, non ne avevano parlato durante l'anamnesi). Tale principio era già stato, peraltro, affermato dalla Cassazione nella sentenza in data 12 settembre 2013 n. 20904, in *Dejure*, ove si legge che: «Una volta iniziato il rapporto curativo, la ricerca della situazione effettivamente esistente in capo al paziente, almeno per quanto attiene alle evidenze del suo stato psico-fisico, è affidata interamente al sanitario, che deve condurla in piena autonomia anche rispetto alle dichiarazioni rese dal paziente in sede di anamnesi, integran-

Tale problematica non è aliena nemmeno al legislatore europeo, se si pone mente al fatto che, al Considerando 17 del Regolamento EHDS 327/2025, si afferma che «è possibile che le persone fisiche non vogliano concedere l'accesso ad alcune parti dei loro dati sanitari elettronici personali, permettendo al contempo l'accesso ad altre parti. Tale aspetto potrebbe assumere particolare rilevanza in caso di questioni di salute come quelle legate alla salute mentale o sessuale, a procedure sensibili quali l'aborto o a dati su medicinali specifici che po-

---

do un diverso operare una palese mancanza di diligenza. Ne consegue, pertanto, che l'incompletezza o reticenza delle informazioni fornite dall'interessato sulle proprie condizioni psico-fisiche, ove esse siano accertabili – dal sanitario e\o dalla struttura in cui il medesimo opera – attraverso l'esecuzione, secondo la "*lex artis*", della prestazione iniziale del rapporto curativo, non costituisce ragione giustificativa per l'applicazione della limitazione di responsabilità, ai soli casi di dolo e colpa grave, di cui all'art. 2236 cod. civ». Con riferimento all'impossibilità di configurare un concorso colposo nel caso in cui il paziente eserciti un proprio diritto, vedi poi Cass. civ., 15 gennaio 2020 n. 515, in *Dejure*, che richiama il consolidato principio giurisprudenziale secondo cui «in tema di liquidazione del danno alla persona, è da considerarsi irrilevante il rifiuto del danneggiato di sottoporsi ad intervento chirurgico al fine di diminuire l'entità del danno, atteso che non può essere configurato alcun obbligo a suo carico di sottoporsi all'intervento stesso, non essendo quel rifiuto inquadrabile nell'ipotesi di concorso colposo del creditore, previsto dall'art. 1227 c.c., intendendosi comprese nell'ambito dell'ordinaria diligenza di cui al secondo comma dell'art. 1227 c.c. soltanto quelle attività che non siano gravose o eccezionali, o tali da comportare notevoli rischi o rilevanti sacrifici». Ad avviso della Suprema Corte, non è giustificata la possibilità di impiegare la valutazione equitativa per contenere l'esposizione risarcitoria dell'autore del comportamento illecito, perché significherebbe arrecare, sia pure in via indiretta, un *vulnus* ad un diritto che, invece, trova ampio riconoscimento e garanzia di tutela. La natura del diritto esercitato, cioè il rifiuto dell'emotrasfusione, ha acquistato una tale rilevanza anche nella coscienza sociale da non ammettere limitazioni di sorta al suo esercizio; e, per la Cassazione, intervenire sul contenimento delle conseguenze risarcitorie a carico dell'offensore significherebbe indirettamente intervenire sulla intensità e sulla qualità del suo riconoscimento. Con gli stessi criteri, seguiti da tale orientamento, allora, si potrebbe sostenere che pure la volontà di esercitare il diritto ad oscurare all'interno del fascicolo elettronico determinati eventi sanitari non potrebbe essere valutata ai fini di una colpa concorrente nella causazione del danno da *malpractice* medica.

trebbero rivelare altre questioni sensibili. È pertanto opportuno sostenere e attuare questa condivisione selettiva dei dati sanitari elettronici personali mediante limitazioni stabilite dalla persona fisica interessata con le stesse modalità all'interno del territorio di un dato Stato membro e per la condivisione transfrontaliera dei dati. Tali limitazioni dovrebbero consentire un livello di dettaglio sufficiente a limitare talune parti delle serie di dati, ad esempio componenti dei profili sanitari sintetici dei pazienti. Prima di definire dette limitazioni, le persone fisiche dovrebbero essere informate dei rischi per la sicurezza dei pazienti legati alla limitazione dell'accesso ai dati sanitari. Poiché l'indisponibilità dei dati sanitari elettronici personali soggetti a tali limitazioni può influire sull'erogazione o sulla qualità dei servizi sanitari erogati alla persona fisica, le persone fisiche che si avvalgono delle limitazioni dovrebbero assumersi la responsabilità del fatto che il prestatore di assistenza sanitaria non può tenere conto dei dati al momento dell'erogazione dei servizi sanitari. Le limitazioni all'accesso ai dati sanitari elettronici personali potrebbero mettere a repentaglio la vita delle persone e pertanto è opportuno che sia comunque possibile accedere a tali dati quando ciò è necessario per proteggere gli interessi vitali in situazioni di emergenza. Gli Stati membri potrebbero prevedere nel diritto interno disposizioni giuridiche più specifiche sui meccanismi delle limitazioni poste dalle persone fisiche su parti dei dati sanitari elettronici personali, in particolare per quanto riguarda la responsabilità medica nei casi in cui le persone fisiche interessate abbiano posto limitazioni»[61].

[61] Ancora, all'art. 8 del Reg. EHDS, si afferma che «le persone fisiche hanno il diritto di limitare l'accesso degli operatori sanitari e dei prestatori di assistenza sanitaria a tutti o a parte dei loro dati sanitari elettronici personali di cui all'articolo 3. Nell'esercizio di tale diritto, le persone fisiche sono informate del fatto che la limitazione dell'accesso può incidere sulla prestazione dell'assistenza sanitaria loro prestata. Il fatto che la persona fisica abbia effettuato una restrizione non è visibile ai prestatori di assistenza sanitaria. Gli Stati membri stabiliscono le norme e le garanzie specifiche relative a tali meccanismi di restrizione.»

5. *L'erigendo Ecosistema dei Dati Sanitari, i rapporti con il fascicolo sanitario elettronico e i ruoli del trattamento*

Tracciata la regolamentazione normativa relativa alla raccolta di dati sanitari all'interno del fascicolo sanitario elettronico, va considerata la prospettiva che tali dati divengano la base informativa dell'erigendo «Ecosistema dei dati sanitari», previsto dall'art. 15-*quater* della Legge 17 dicembre 2012 n. 179, ed istituito con decreto del 31 dicembre 2024 [62], infrastruttura che dovrebbe «acquisire, memorizzare e gestire (tal)i dati» per svolgere analisi avanzate e supporto decisionale, e dovrebbe diventare operativa entro il 31 marzo 2026. La finalità principale perseguita dall'ecosistema dei dati sanitari è quella di garantire servizi omogenei e una gestione centralizzata dei dati sanitari su tutto il territorio nazionale con il consenso espresso e preventivo dell'interessato, l'accesso tempestivo a dati sanitari esatti, aggiornati, sempre e comunque allineati con la volontà dell'assistito. L'EDS, una volta creato, si alimenterà, come detto, dei dati provenienti dal FSE, dalle strutture sanitarie e sociosanitarie, e dal Sistema Tessera Sanitaria, rendendo disponibili informazioni vitali per una gestione più efficiente della salute pubblica [63]. L'EDS non solo raccoglierà dati, ma li elaborerà per fornire servizi specifici a professionisti sanitari, regioni e cittadini, assicurando che le informazioni sanitarie siano trattate con il massimo rispetto dei diritti e le libertà dei cittadini [64]. I servizi, però, sono rea-

---

[62] Tale decreto è stato pubblicato nella Gazzetta ufficiale del 5 marzo 2025, dopo che il suo schema aveva avuto parere positivo, con provvedimento n. 605 del Garante privacy in data 26 settembre 2024, consultabile in *www.garanteprivacy.it* (*doc. web n. 10062302*).

[63] L'architettura dell'ecosistema dei dati sanitari garantisce la separazione dei dati in chiaro, pseudonimizzati e anonimizzati, il pieno allineamento tra i documenti sanitari pubblicati nei FSE regionali e i dati resi disponibili nell'EDS, la non duplicazione dei dati estratti dai documenti sanitari, la piena interoperabilità delle diverse unità di archiviazione contenenti i dati in chiaro e la facoltà per le regioni e le province autonome di gestire in proprio l'unità di archiviazione dei dati in chiaro.

[64] Secondo l'art. 2, comma 3, del decreto, i dati sono elaborati dall'EDS al fine

lizzati solo su richiesta (*on demand*), non essendo ammissibile l'elaborazione automatica dei dati e delle informazioni del FSE 2.0 (art. 3, comma 1) e l'utilizzo di sistemi di intelligenza artificiale (IA). Tuttavia, permangono sfide significative, come l'attuazione delle misure di protezione dei dati e la garanzia dell'applicabilità di diritti dell'interessato come l'oscuramento e la consultazione degli accessi ai propri dati. Ai sensi dell'art. 8, decreto EDS, il trattamento dei dati tramite tale strumento istituzionale richiede un consenso informato e specifico da parte degli assistiti, che deve essere espresso in modo chiaro per le finalità legate alla cura, alla prevenzione o alla profilassi internazionale [65]. Per le finalità di studio e ricerca scientifica, nonché di governo, l'accesso ai dati sarà limitato e sono previste specifiche misure tecniche a tutela degli utenti. Si potranno estrarre esclusivamente dati anonimizzati e, per le finalità di governo, solo dati aggregati privati degli elementi identificativi diretti e pseudonimizzati. Non potrà essere ritenuto valido, anche per i trattamenti effettuati attraverso l'EDS, il consenso reso (in passato) per il FSE. Solo i soggetti abilitati, previo consenso dell'interessato, potranno accedere all'EDS per finalità di cura,

---

assicurare, su richiesta, appositi servizi mediante la ricerca, consultazione, estrazione e analisi dei dati, nonché specifici servizi di supporto alla compilazione del Profilo Sanitario Sintetico, al processo di cura e per la realizzazione del dossier farmaceutico specificatamente individuati.

[65] Secondo l'art 7 del decreto EDS, in attuazione degli articoli 13 e 14 del Regolamento UE 2016/679 relativo alla protezione dei dati personali, quale presupposto di liceità del trattamento, deve essere fornita all'assistito, da parte del Ministero della salute, delle regioni e province autonome, idonea informativa che espliciti i trattamenti dei dati effettuati attraverso l'EDS. La revoca dei consensi all'elaborazione dei dati attraverso l'EDS determina, nel caso di revoca del consenso espresso per le finalità di cura, prevenzione e profilassi, la disabilitazione dell'accesso ai servizi del medesimo Ecosistema. La disabilitazione all'elaborazione dei dati attraverso l'EDS da parte di terzi per le specifiche finalità per le quali sono stati revocati i consensi, così come il mancato consenso, non pregiudicano il diritto all'erogazione della prestazione sanitaria. L'assistito può, successivamente, esprimere nuovi consensi all'elaborazione dei dati attraverso l'EDS, rendendo nuovamente disponibile l'elaborazione dei propri dati all'EDS, per le specifiche finalità per le quali sono stati espressi nuovi consensi.

vale a dire le strutture sanitarie e socio-sanitarie e i medici convenzionati, nonché gli esercenti le professioni sanitarie che prendono in cura l'interessato, anche al di fuori del servizio sanitario nazionale (SSN). E saranno resi disponibili una serie di servizi pertinenti alla finalità di cura, cui gli stessi accederanno su propria iniziativa, nel rispetto dei principi di minimizzazione, necessità e pertinenza dei dati. Viene prevista, all'art. 18 del decreto, l'eccezione di accesso in emergenza per finalità di cura, anche in assenza di un consenso dell'interessato, per gli operatori del SSN e dei servizi sociosanitari regionali, nonché gli esercenti le professioni sanitarie. Agli interessati è poi consentito di accedere, rettificare e oscurare i propri dati personali direttamente sul fascicolo sanitario elettronico, garantendo l'aggiornamento esatto ed immediato anche dell'EDS. Così come per il fascicolo sanitario elettronico, l'accesso ai servizi dell'EDS è sempre escluso ai soggetti operanti in ambito sanitario che non perseguono finalità di cura quali periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, organismi amministrativi anche operanti in ambito sanitario, personale medico nell'esercizio di attività medico-legale, quale quella per l'accertamento dell'idoneità lavorativa o per il rilascio di certificazioni necessarie al conferimento di permessi o abilitazioni.

Il decreto stabilisce che per la finalità di prevenzione, previo consenso dell'assistito, l'EDS renderà disponibili ai soggetti del SSN e dei servizi sociosanitari regionali della Regione di Assistenza (RdA), agli esercenti le professioni sanitarie che hanno in cura l'interessato, o comunque gli prestano assistenza, un insieme di servizi, descritti nell'allegato A, pertinenti alla finalità di prevenzione, cui gli stessi accedono su propria iniziativa, nel rispetto dei principi di minimizzazione, necessità e pertinenza, secondo livelli diversificati di accesso. Il decreto prevede che le regioni/province autonome e il Ministero della salute potranno accedere solo ai dati privati degli elementi identificativi diretti e pseudonimizzati [66]. L'accesso sarà possibile esclusivamente

[66] Si aggiunge che i soggetti del SSN e dei servizi sociosanitari regionali della RdA, gli esercenti le professioni sanitarie che hanno in cura l'assistito o comunque

per il personale sanitario autorizzato, soggetto alle regole del segreto professionale, e che non acceda anche ad altri flussi di dati pseudonimizzati per altre finalità [67]. Analogamente, per la finalità di profilassi internazionale il decreto stabilisce che, previo consenso dell'interessato, l'EDS renderà disponibili alla Direzione generale competente in materia di profilassi internazionale del Ministero della salute un insieme di servizi omogenei sul territorio nazionale [68]. Potranno accedere a questi servizi i soggetti operanti presso la Direzione generale del Ministero della salute, secondo livelli diversificati di accesso determinati sulla base delle relative attività di competenza, debitamente autorizzati

---

gli prestano assistenza sanitaria sono titolari del trattamento per finalità di prevenzione. Sono altresì titolari del trattamento per finalità di prevenzione le regioni attraverso gli uffici competenti in materia di prevenzione sanitaria nonché il Ministero della salute attraverso la Direzione generale competente in materia di prevenzione sanitaria.

[67] L'art. 18 del decreto prevede che, in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere e di rischio grave, imminente e irreparabile per la salute o l'incolumità fisica dell'interessato, che non abbia espresso il consenso al FSE e all'EDS, gli operatori del SSN e dei servizi socio-sanitari regionali, nonché gli esercenti le professioni sanitarie, secondo quanto previsto nell'articolo 20 del decreto FSE 2.0, potranno accedere, prioritariamente al PSS ed eventualmente al resto del FSE e, ove ritenuto necessario, ai servizi resi disponibili dall'EDS per finalità di cura. L'accesso ai servizi dell'EDS potrà avvenire solo nel caso in cui il professionista sanitario, verificata l'incapacità fisica o giuridica dell'interessato di esprimere il consenso, non riterrà sufficiente l'accesso al PSS e comunque solo per il tempo strettamente necessario ad assicurare all'interessato le cure indispensabili e fino a quando lo stesso non sia nuovamente in grado di esprimere la propria volontà al riguardo.

[68] Il Ministero della salute accede ai servizi dell'EDS se necessario per la valutazione della situazione sanitaria dei soggetti destinatari delle seguenti azioni di competenza del Ministero: somministrare vaccinazioni o profilassi obbligatorie o raccomandate per soggetti diretti all'estero, su richiesta degli interessati; somministrare vaccinazioni o profilassi obbligatorie o raccomandate per soggetti provenienti dall'estero; sottoporre a misure di quarantena o isolamento; effettuare attività di *contact tracing* internazionale; disporre misure di profilassi conseguenti a esposizioni ad agenti patogeni relative a soggetti che abbiano utilizzato mezzi di trasporto collettivi o soggiornato in comunità chiuse.

e da individuare esclusivamente in personale medico soggetto alle regole del segreto professionale che non accederà, per altre finalità, a flussi di dati pseudonimizzati [69]. La finalità di governo viene poi perseguita – a regime – esclusivamente attraverso i servizi che l'EDS renderà disponibili al personale dei competenti Uffici del Ministero della salute, di Agenas e delle regioni e delle province autonome competenti in materia di governo, a cui gli stessi accederanno sempre secondo i livelli diversificati di accesso indicati nell'allegato A (art. 16). Potranno accedere a questi servizi i soggetti abilitati che forniranno dati privati degli elementi identificativi diretti, pseudonimizzati, nonché dati aggregati. Il decreto prevede inoltre che il personale del Ministero della salute e delle Regioni e delle Province autonome, che, per altre finalità, ha accesso a flussi di dati pseudonimizzati, non accederà ai dati messi a disposizione dai servizi dell'EDS per finalità di governo. L'art. 17 del decreto disciplina l'accesso ai servizi dell'EDS per finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico. Il servizio previsto consiste esclusivamente nel rendere disponibile l'estrazione dall'EDS di dati anonimizzati secondo le tecniche indicate nell'allegato B, al personale dei competenti Uffici del Ministero della salute, di Agenas e delle regioni e province autonome (comma 1) [70].

---

[69] Il fine è quello di individuare: 1) la circolazione di nuovi patogeni o l'emergere di sintomatologie sconosciute o di fattori di rischio ambientale e/o alimentare; 2) nuovi fattori di rischio legati a patologie correlate come co-infezioni; 3) lo sviluppo di nuovi casi di farmacoresistenza verso specifici gruppi di patogeni; 4) possibili nuove complicanze non conosciute di alcune malattie infettive che possono portare al decesso del caso.

[70] Molto interessante la previsione legislativa secondo cui lo stesso soggetto (Ministero della Salute che opera attraverso Agenas) è titolare di dati in chiaro, di dati pseudonimizzati e degli stessi dati che hanno subito un processo di anonimizzazione (le cui tecniche sono elencate in Allegato B). Sembra dunque di poter affermare che attraverso il D.M. sull'EDS sia ammesso trattare dati in chiaro, applicare tecniche di anonimizzazione e poter quindi considerare gli stessi dati come anonimi (pur avendo piena contezza delle tecniche attraverso le quali i dati sono stati anonimizzati). Oppure si potrebbe ritenere che tali dati siano considerati anonimi solo per coloro che accedono: ciò in linea con la sentenza Tribunale UE 27 aprile 2023 557/2020 e

Questo servizio potrà essere erogato ai soggetti pubblici e privati che istituzionalmente perseguono finalità di studio e di ricerca scientifica in campo medico, biomedico ed epidemiologico per il tramite di Agenas, previa valutazione da parte della predetta Agenzia di una richiesta di estrazione di dati anonimizzati, corredata da un progetto di ricerca conforme alle regole metodologiche ed etiche, e, se del caso, alle regole deontologiche per trattamenti a fini statistici e di ricerca scientifica, nonché al Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. n. 101/2018 (comma 2). Inoltre, i servizi dell'EDS, che consentiranno trattamenti di dati di natura personale per le finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico, nel rispetto delle garanzie di cui all'art. 89 del Regolamento, saranno disciplinati nell'ambito di successivi decreti (comma 4).

Considerata tale normativa, si deve porre attenzione al fatto che il titolare del trattamento di quest'ultima banca dati sarà il Ministero della Salute, mentre Agenas, in qualità di responsabile del trattamento, avrà compiti di gestione operativa, assicurando che vengano rispettati i diritti degli interessati e le misure di sicurezza necessarie (art. 12 comma 2, decreto EDS). I titolari del trattamento del FSE, invece, in quanto soggetti preposti all'alimentazione dei dati e documenti relativi all'assistito sono, a secondo delle relative finalità: le aziende sanitarie locali, le strutture sanitarie pubbliche del SSN e dei servizi sociosanitari regionali, nonché i Servizi territoriali per l'Assistenza Sanitaria al personale Navigante (SASN); le strutture sanitarie accreditate al SSN e con i servizi sanitari regionali; le strutture sanitarie autorizzate; gli esercenti le professioni sanitarie operanti in autonomia. La titolarità è attribuita poi alle Regioni e alle Provincie autonome nel successivo trattamento per finalità di verifica formale e semantica dei dati e documenti ivi contenuti, rilevante in sede di alimentazione del FSE.

---

con il relativo recente parere dell'Avvocato Generale dello stato nel giudizio di appello CGCE C-413/23 (cfr., in tal senso, S. Stefanelli, *Ecosistema Dati Sanitari, c'è la norma: cos'è e come funziona la banca dati per la Salute in Italia*, in *www.agendadigitale.eu* del 7 marzo 2025).

Ciò considerato, all'evidenza, si prospetta un'estrazione e trasmissione di dati sanitari da tali ultimi soggetti al Ministero della Salute, titolare, come anticipato, dell'Ecosistema dati sanitari, con ogni inerente eventuale responsabilità di parte mittente e di parte ricevente, in caso di deviazione dalla condotta *standard*.

6. *L'elaborazione dei dati clinici presenti nel fascicolo sanitario elettronico attraverso l'utilizzo di strumenti di intelligenza artificiale. Profili di responsabilità del medico e della struttura*

Le Linee guida del 2022 per l'attuazione del FSE prevedono, all'interno dell'*executive summary* (punto 1), tra i vari requisiti obbligatori e raccomandati da attuare per perseguire gli obiettivi delineati entro la durata del PNRR, l'adozione di strumenti di *Advanced Analytics*, anche basati su tecniche di intelligenza artificiale per l'elaborazione dei dati clinici [71].

---

[71] Tali Linee guida sono pubblicate nella G.U. dell'11 luglio 2022. In relazione all'utilizzo dell'AI nell'ambito sanitario, *ex multis*, vedi M. CIANCIMINO, *AI-Based Decision-Making Process in Healthcare*, in *Journal of European Consumer and Market Law*, vol. 11, n. 5, 2022, 173 ss.; ID., *Protezione e controllo dei dati in àmbito sanitario e intelligenza artificiale. I dati relativi alla salute tra novità normative e innovazioni tecnologiche*, Napoli, ESI, 2020; M. FACCIOLI, (a cura di), *Profili giuridici dell'utilizzo della robotica e dell'intelligenza artificiale in medicina*, Napoli, ESI, 2022; D. MORANA, T. BALDUZZI, F. MORGANTI, *La salute "intelligente":* eHealth*, consenso informato e principio di non-discriminazione*, in *federalismi.it*, 28 dicembre 2022, n. 34, 127 ss.; B. VIVARELLI, *Profilazione dei dati e aziende sanitarie*, in A. ADINOLFI, A. SIMONCINI (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, ESI, 2022, 363 ss.; G. FIORIGLIO, *La protezione dei dati sanitari nella Società algoritmica. Profili informatico-giuridici*, in *Journal of Ethics and Legal Technologies*, vol. 3, n. 2, 2021, 79 ss.; F. LAGIOIA, *L'intelligenza artificiale in sanità: un'analisi giuridica*, Torino, Giappichelli, 2020; F. ROSA, *The use of IT tools and artificial intelligence in the health sector: the patient as a vulnerable subject*, in *European Journal of Privacy Law & Technologies*, 2020, 224 ss.; A. SPINA, *La medicina degli algoritmi: Intelligenza Artificiale, medicina digitale e regolazione dei dati personali*, in F. PIZZETTI (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018, 319 ss.; cfr. pure S. CORSO, *L'in-*

Pure i recenti interventi legislativi rendono evidente come il futuro della sanità sia orientato all'impiego di tecniche algoritmiche e di IA a supporto delle decisioni cliniche e governative sanitarie [72]. Ad esempio, il decreto-legge n. 19/2024 (convertito con modificazioni dalla L. 29 aprile 2024, n. 56), all'art. 42, prevede la gestione da parte di AGENAS di una piattaforma di intelligenza artificiale e valutazione delle tecnologie sanitarie (*Health Technology Assessment* – HTA) relative ai dispositivi medici (modifica all'art. 12, comma 15-*undecies* del d.l. n. 179/2012).

Molto chiaro appare l'orientamento che traspare anche dalla legge n. 132/2025, denominata "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", e pubblicata nella Gazzetta Ufficiale n. 223 del 25 settembre 2025, che intende attuare e integrare l'*AI Act*, proponendo un approccio antropocentrico [73]. All'art. 7, si afferma che «l'utilizzo di sistemi di intelligenza artificiale contribuisce al miglioramento del sistema sanitario, alla prevenzione, alla diagnosi e alla cura delle malattie, nel rispetto dei diritti, delle libertà e degli interessi della persona, anche in materia di protezione dei dati personali. L'introduzione di sistemi di intelligenza artificiale nel sistema sanitario non può selezionare e condizionare l'accesso alle prestazioni sanitarie secondo criteri discriminatori. L'interessato ha diritto di essere informato sull'impiego di tecnologie di intelligenza artificiale. I sistemi di intelligenza artificiale in ambito sanitario costituiscono un supporto nei processi di prevenzione, diagnosi, cura e scelta terapeutica, lasciando impregiudicata la decisione, che è sempre rimessa agli esercenti la professione medica. I sistemi di intelligenza artificiale utilizzati in ambito sanitario e i relativi dati impiegati devono essere affidabili, periodicamente verificati e aggiornati al fi-

---

telligenza artificiale e il trattamento dei dati relativi alla salute, in *Responsabilità medica*, 2023, 317 ss.

[72] In merito alla differenza tra algoritmi e tecniche di IA, cfr. Cons. Stato, 4-25 novembre 2021, n.7891, con commento di F. Fidanza, *Sulla distinzione tra intelligenza artificiale e algoritmi*, in *Rivista di diritto dell'impresa*, 2022, 389; G. Gallone, *Il Consiglio di Stato marca distinzione tra algoritmo, automazione ed intelligenza artificiale*, in *Diritto di internet*, 2022, 1.

[73] Vedi, per una prima lettura della norma, G. Resta, G.M. Riccio, *Il DDL AI è legge: primi spunti di riflessione*, pubblicato il 18 settembre 2025 in *www.altalex.com*.

ne di minimizzare il rischio di errori e migliorare la sicurezza dei pazienti». L'art.10 della medesima legge aggiunge poi alla normativa di cui alla legge 17 dicembre 2012, n. 221, in ordine alla disciplina sul fascicolo sanitario elettronico, l'art. 12-*bis*, che prevede che, per garantire strumenti e tecnologie avanzate nel settore sanitario, con uno o più decreti del Ministro della salute siano disciplinate le soluzioni di intelligenza artificiale aventi funzione di supporto alle finalità previste dall'articolo 12, comma 2. Per il supporto alle finalità di cura, e in particolare per l'assistenza territoriale, si prevede, inoltre, l'istituzione di una piattaforma di intelligenza artificiale, la cui progettazione, realizzazione, messa in servizio e titolarità sono attribuite all'AGENAS. Tale piattaforma dovrebbe erogare servizi di supporto: a) ai professionisti sanitari per la presa in carico della popolazione assistita con suggerimenti non vincolanti; b) ai medici nella pratica clinica quotidiana con suggerimenti non vincolanti; c) agli utenti per l'accesso ai servizi sanitari delle Case della comunità.

Vale, peraltro, la pena evidenziare come per l'addestramento dei modelli di IA ad alto rischio il Regolamento europeo sull'IA preveda come ipotesi eccezionale l'uso delle categorie particolari di dati personali. Tali dati devono, per la normativa unionale, essere soggetti a limitazioni tecniche relative al riutilizzo dei dati personali, nonché a misure più avanzate di sicurezza e di tutela della vita privata, compresa la pseudonimizzazione [74]. Deve, inoltre, essere garantita la validazione e la gestione dei sistemi di qualità, oltre che misure idonee ad assicurare

[74] Si precisa che nell'allegato III al Reg. UE 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, consultabile in https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=OJ%3AL_202401689, sono stati classificati, ai sensi dell'art. 6, par. 2, come ad alto rischio i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi (punto 5, lett. a). Parimenti sono considerati ad alto rischio i sistemi di IA di selezione dei pazienti per quanto concerne l'assistenza sanitaria di emergenza (punto 5, lett. d). In argomento, vedi C. PERLINGIERI, *Intelligenza artificiale in*

la sicurezza, ivi compresi i controlli e la tenuta di documentazione rigorosa sull'accesso, al fine di evitare abusi e garantire che solo le persone autorizzate sottostanti a opportuni obblighi di riservatezza abbiano accesso a tali dati personali. Per i dati personali appartenenti alle categorie particolari si richiamano principi e regole specifiche sulla preferenza circa l'uso dei dati sintetici o anonimi, sulle particolari limitazioni relative alla trasmissione, trasferimento o comunicazione delle informazioni, nonché sul tema della limitazione della conservazione dei dati. Peraltro, l'EDPS aveva raccomandato, nel caso di utilizzo di sistemi di IA ad alto rischio, che fosse previsto il diritto per l'interessato di ottenere l'intervento umano nell'ambito del processo decisionale che lo riguarda [75]. Ed il Regolamento sull'IA non si limita ad un richiamo generico a tale principio, ma individua, sulla base di un approccio basato sul rischio, specifiche e concrete misure di sorveglianza e di intervento correttivo (art. 14 del Reg. IA). Ciò, in particolare, nella fase di addestramento degli algoritmi, in quanto la qualità delle informazioni utilizzate e di esperienze immagazzinate in tale fase condiziona la capacità del sistema di effettuare elaborazioni e previsioni e ciò assume rischi specifici e significativi, soprattutto quando i sistemi di IA intendono intervenire sulla definizione del rischio di sviluppare malattie, sull'individuazione del percorso diagnostico e terapeutico o all'accesso alle cure o alla quota di partecipazione al costo delle stesse in carico all'assistito [76]. I rischi di discriminazione algoritmica sono infatti evidenti e possono incidere sull'equità e sull'inclusi-

ambito medico-sanitario: profili di ricostruzione normativa a seguito dell'AI Act, in *Rassegna di diritto civile*, 2024, 907 ss.

[75] Cfr. *EDPS Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments*, consultabile al seguente link: https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2023-10-23-edps-opinion-442023-artificial-intelligence-act-light-legislative-developments_en

[76] Sul punto cfr. CNIL, *Artificial intelligence: CNIL unveils its first answers for innovative and cy-friendly AI*, del 16 ottobre 2023, con cui la CNIL sottopone a consultazione pubblica alcune schede sulla creazione di *set* di dati per lo sviluppo di sistemi di intelligenza artificiale, consultabile in *www.cnil.fr/en/artificial-intelligence-cnil-unveils-its-first-answers-innovative-and-pri-friendly-ai*.

vità alle cure, potendo potenzialmente aumentare il divario e le disuguaglianze socio-sanitarie e minare l'attuazione di valori e principi costituzionali. Il rispetto del richiamato principio di non discriminazione algoritmica, affermato anche dalla nostra giurisprudenza, impone che siano adottati sistemi di IA affidabili, come ora richiede anche il Regolamento europeo sull'IA, che riducano le opacità, gli errori dovuti a cause tecnologiche e/o umane, verificandone periodicamente l'efficacia anche alla luce della rapida evoluzione delle tecnologie impiegate, delle procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate [77]. Ed è ai profili di responsabilità che il diritto civile ha guardato, avvicinandosi allo studio dei problemi che solleva l'intelligenza artificiale [78], anche in attesa di capire quali saranno i prossimi passi del Legi-

---

[77] Cfr., in particolare, Cons. Stato, sent., sez. VI, n. 2270/2019 in *Foro it*., 2019, 11, III, c. 606, Cons. Stato 8472/2019, in *Nuova giurisprudenza civile commentata*, 2020, I, 809 ss., con nota di MATTERA, *Decisioni algoritmiche. Il Consiglio di Stato fissa i limiti*, e Cons. Stato, 8473/2019, 8474/2019, e 1206/2021, su cui A. L. RUM, *Il provvedimento amministrativo adottato mediante algoritmo: il ruolo dell'intelligenza artificiale nel processo decisionale della P.A.*", in *Diritto amministrativo*, 2021. Come rilevato dal Considerando n. 69 dell'*AI Act*, «per quanto riguarda la salute, lo spazio europeo di dati sanitari agevolerà l'accesso non discriminatorio ai dati sanitari e l'addestramento di algoritmi di IA a partire da tali set di dati in modo sicuro, tempestivo, trasparente, affidabile e tale da tutelare la vita privata, nonché con un'adeguata governance istituzionale». Sulla discriminazione algoritmica, vedi G. CARAPEZZA FIGLIA, *Decisioni algoritmiche tra diritto alla spiegazione e divieto di discriminare*, in S. ORLANDO (a cura di), *Libertà e liceità del consenso nel trattamento dei dati personali*, Firenze, Persona e mercato ed., 2024, 64 ss. V. pure S. CORSO, *Alla frontiera del diritto privato. Nuove tecnologie e persona anziana*, in *Nuova giurisprudenza civile commentata*, 2024, II, 1253 ss.

[78] Sulla responsabilità civile legata all'intelligenza artificiale vedi A. FUSARO, *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo*, in *Nuova giurisprudenza civile commentata*, 2020, II, 1344 ss. Cfr. A. BECKERS, G. TEUBNER, *Three Liability Regimes for Artificial Intelligence*, Londra, Hart, 2022; M. GRONDONA, *Intelligenza artificiale e responsabilità da attività pericolose. Una prospettiva ideologicamente orientata e un inventario di problemi*, in V. CUOCCI, F.P. LOPS, C. MOTTI (a cura di), *La responsabilità civile nell'era digitale. Atti della Summer school 2021*, Bari, Cacucci, 2022, 181 ss.; L. DI DONNA, *Intelligenza artificiale e rimedi risarcitori*, Milano, Wolters Kluwer, 2022; V.

slatore europeo dopo il ritiro della proposta di direttiva relativa alla responsabilità extracontrattuale derivante dall'uso dell'intelligenza artificiale [79], considerata però anche l'esistenza di una proposta di direttiva

---

Di Gregorio, *Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie?*, in *Danno e responsabilità*, 2022, 51 ss.; D. Locatello, *Osservazioni sulla costruzione di un regime europeo di responsabilità civile per l'Intelligenza artificiale*, in *Jus civile*, 2022, 130 ss.; M. Mazzuca, *Note minime sulla responsabilità per i danni scaturenti dall'uso dei sistemi di IA*, in *Teoria e prassi del diritto*, 2022, 399 ss.; C. Iorio, *Intelligenza artificiale e responsabilità: spunti ricostruttivi*, in *Tecnologie e diritto*, 2021, 51 ss.; C. Leanza, *Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio*, in *Responsabilità civile e previdenza*, 2021, 1011 ss.; G. Finocchiaro, *Intelligenza artificiale e responsabilità*, in *Contratto e impresa*, 2020, 713 ss.; M. Martone, *Algoritmi e diritto: appunti in tema di responsabilità civile*, in *Tecnologie e diritto*, 2020, 128 ss.; U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della commissione europea*, in *Rivista di diritto civile*, 2020, 1246 ss.; G. D'Alfonso, *I nuovi scenari dannosi correlati all'impiego delle tecnologie digitali emergenti. L'intervento del legislatore europeo di modernizzazione della disciplina sulla responsabilità del produttore*, in B. Grasso (a cura di), *Scritti in memoria di Ubaldo La Porta*, Napoli, ESI, 2023, 217 ss.. E da ultimo, vedi A. Bertolini, *Intelligenza artificiale e responsabilità civile*, Bologna, Il Mulino, 2025.

[79] Il 28 settembre 2022 la Commissione UE aveva presentato una proposta di Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (Cfr. E. Bellisario, *Il pacchetto europeo sulla responsabilità per danni da prodotti e da intelligenza artificiale. Prime riflessioni sulle Proposte della Commissione*, in *Danno e responsabilità*, 2023, 153 ss.; R. Gellert, A. Jansenn, *The impact of artificial intelligence on european tort law: taking stock of an ongoing process*, in A. Janssen, M. Lehmann, R. Schulze (eds)*The future of European Private Law*, Hart Nomos, 2023, 185 ss.). Considerato che le norme nazionali in materia di responsabilità, in particolare per colpa, non sono adatte a gestire le azioni di responsabilità per danni causati da prodotti e servizi basati sull'IA, tale proposta – che si inseriva nel quadro più ampio della regolamentazione dell'intelligenza artificiale nell'UE, accanto ad altre normative quali, *in primis*, il Regolamento UE n. 2024/1689 sull'intelligenza artificiale (cd. IA Act), nonché la revisione delle norme (settoriali e orizzontali) in materia di sicurezza dei prodotti – si prefiggeva l'obiettivo di promuovere la diffusione di un'IA affidabile, affinché fosse possibile sfruttarne appieno i vantaggi per il mercato interno, e si proponeva di conseguirlo garantendo a coloro che hanno subito danni causati dall'IA una protezione equivalente a quella di cui beneficiano quanti subiscono danni causati da altri prodotti. La Proposta si applicava alle azioni civili di responsabilità extracontrattuale promosse successivamente alla data di rece-

del Parlamento europeo e del Consiglio sulla responsabilità per danno

pimento della direttiva da parte di: – soggetti direttamente danneggiati dall'IA; – soggetti subentrati/surrogati nei diritti del danneggiato dall'IA (es. eredi; compagnia assicurativa); – soggetti che agiscono per conto di uno o più danneggiati (azioni rappresentative), al fine di ottenere il risarcimento del danno causato dall'*output* di un sistema di IA o dalla mancata produzione di un *output* (che avrebbe dovuto essere prodotto da tale sistema) nell'ambito di regimi di responsabilità per colpa. L'obiettivo principale della direttiva era, dunque, quello di introdurre semplificazioni dell'onere della prova per qualunque soggetto instaurasse un'azione per danni causati da sistemi di IA in uno Stato membro, al fine di superare le principali criticità riscontrate in materia di responsabilità civile, ossia: – antieconomicità: le norme nazionali in materia di responsabilità civile risultano spesso di difficile applicazione alla materia dell'IA (in particolare, in relazione all'identificazione del soggetto responsabile); – incertezza: le norme nazionali possono, inoltre, essere interpretate diversamente in base all'apprezzamento del giudice nazionale; – frammentazione: aspetto derivante da adeguamenti specifici all'IA da parte delle norme nazionali in materia di responsabilità civile. Nell'ottica di semplificare l'onere probatorio, la proposta introduceva il diritto per il danneggiato/attore di ottenere in sede giudiziale elementi di prova sul sistema di IA c.d. «ad alto rischio», mediante un ordine giudiziale di divulgazione di tali elementi: tale provvedimento costituisce, infatti, un oggettivo mezzo efficace per l'identificazione delle persone responsabili, e delle relative prove, al netto, tuttavia, di eventuali limiti intrinseci, quali, *in primis*, la protezione dei segreti commerciali e delle informazioni riservate. A tal riguardo, la direttiva mirava, altresì, a fornire una base efficace per le domande di risarcimento in relazione alla colpa consistente nella non conformità a un obbligo di diligenza a norma del diritto dell'unione o nazionale: sul punto, era stata, dunque, prevista, all'art. 4 paragrafo 1) della direttiva, una presunzione relativa in relazione, appunto, al nesso di causalità tra la non conformità e l'*output* prodotto dal sistema di IA o la mancata produzione di un *output* da parte del medesimo sistema di IA che ha cagionato un danno. Risultava, infine, degno di attenzione il suggerimento, inserito nella relazione complementare alla direttiva, circa l'introduzione di un cd. regime misto, che combinasse elementi di responsabilità basata sulla colpa e di responsabilità oggettiva: nello specifico, la prima sarebbe rimasta applicabile in generale, mentre la seconda sarebbe stata riservata ai casi di danni causati da sistemi di IA ad alto impatto o cd. *general-purpose* (es. sanità). La Commissione europea ha motivato il ritiro della proposta di direttiva sulla responsabilità civile per l'intelligenza artificiale con l'obiettivo di evitare un eccesso di regolamentazione che incidesse negativamente sulla competitività delle imprese europee. L'adozione di criteri più stringenti per l'imputazione della responsabilità in caso di danni derivanti dall'impiego di sistemi autonomi avrebbe comportato un incremento degli oneri re-

da prodotti difettosi [80]. Quest'ultima mira a modernizzare l'attuale regime e si applicherebbe alle richieste di risarcimento presentate da privati contro il produttore per danni causati da prodotti difettosi, ampliando però il concetto di prodotto, includendo il «*software*».

Ciò, tenuto conto anche del fatto che, tra i principali rischi connessi all'utilizzo di modelli di analisi stocastica con tecniche di *machine learning*, vi sono quelli relativi a potenziali opacità nella fase di sviluppo dell'algoritmo o errori e distorsioni di diversa natura (cosiddetti *bias*), che possono verificarsi nell'elaborazione o nell'utilizzo di tali modelli ovvero correlati alla qualità e/o al volume dei dati di volta in volta utilizzati e che, se non correttamente identificati e mitigati, possono produrre conseguenze pregiudizievoli o risultati discriminatori per gli interessati [81].

---

golatori, con ripercussioni sullo sviluppo tecnologico e sull'attrattività del mercato europeo per gli investitori. (cfr. F. Niola, *Responsabilità civile per l'AI: gli effetti del ritiro della proposta di direttiva*, in *Cybersecurity360.it,* pubblicato in data 28 febbraio 2025).

[80] Cfr. la Risoluzione legislativa del Parlamento europeo del 12 marzo 2024 sulla proposta di direttiva del Parlamento europeo e del Consiglio sulla responsabilità per danno da prodotti difettosi (COM(2022)0495-C9-0322/2022-2022/0302(COD)), 2024, 1 ss.

[81] Un recente caso verificatosi negli Stari Uniti, richiamato anche dal Garante nel Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale (consultabile al link *https://www.garanteprivacy.it/web/guest/ho me/docweb/-/docweb-display/docweb/9938038*), rende evidenti i rischi di discriminazione che possono derivare da una selezione impropria, incompleta e non accurata dei dati utilizzati dai sistemi di IA (*Https://pubmed.ncbi.nlm.nih.gov/31649194/ Dissecting racial bias in an algorithm used to manage the health of populations*). Nell'uso di un sistema di IA utilizzato per stimare il rischio sanitario di oltre 200 milioni di americani è stato possibile osservare che lo stesso tendeva ad assegnare un livello di rischio inferiore ai pazienti afroamericani a parità di condizioni di salute, con la conseguenza di negare loro l'accesso a cure adeguate. La causa di tale alterazione era da attribuire alla metrica utilizzata per stimare il rischio, che era basata sulla spesa sanitaria media individuale, che risulta essere molto più bassa nella popolazione afro-americana. Tale esperienza rende evidente come sia indispensabile nell'addestramento e nell'utilizzo dell'algoritmo considerare la qualità dei dati, che è spesso fortemente condizionata anche dalle caratteristiche socio-economiche della popolazione di riferimento e come gli effetti discriminatori che possono derivare dall'uso di un sistema di IA possano avere significativi risvolti etici (cfr. punto 9 del predetto decalogo). In tal senso

Nella definizione del quadro di riferimento relativo all'impiego di tecniche di IA in sanità, non potrà poi essere dimenticato il tema dell'obbligatorietà o meno di avvalersi di tali servizi da parte del professionista sanitario quando il sistema sanitario nazionale o regionale glieli fornisca. Sotto questo profilo, si pone come centrale il tema della responsabilità professionale del professionista sanitario che fondi o meno le sue scelte terapeutiche sulla base dell'elaborazione dei dati offerta da un sistema di IA sviluppato e proposto da piattaforme nazionali o regionali sanitarie. Nell'attività diagnostica e terapeutica, un sistema di «assistenza cognitiva automatizzata» non dovrebbe essere immaginato come «sistema decisionale autonomo», bensì esclusivamente come uno strumento che può accelerare e facilitare il processo di analisi delle informazioni sanitarie da utilizzare solo a richiesta del medico che deciderà di avvalersene nell'ambito del principio di trasparenza che deve caratterizzare la relazione tra medico e paziente. Considerata la natura dei dati che sistemi di IA in sanità andrebbero a trattare e la vulnerabilità degli interessati (pazienti), i titolari del trattamento dovrebbero informare i soggetti i cui dati sanitari sono elaborati attraverso tecniche di IA se il trattamento sia effettuato nella fase di apprendimento dell'algoritmo (sperimentazione e validazione) ovvero nella successiva fase di applicazione dello stesso, se sussistono eventuali obblighi e responsabilità dei professionisti sanitari cui si rivolge nell'utilizzare servizi sanitari basati sull'IA e quali siano i vantaggi, in termini diagnostici e terapeutici, derivanti dall'utilizzo di tali nuove tecnologie [82]. L'approccio *privacy by design* dovrebbe essere la regola nelle ini-

---

anche il Considerando 47 del Regolamento sull'IA che, nel settore sanitario, in cui la posta in gioco per la vita e la salute è particolarmente elevata, indica come opportuno che i sistemi diagnostici e i sistemi di sostegno delle decisioni dell'uomo, sempre più sofisticati, siano affidabili e accurati (cfr. anche Considerando 67). Al riguardo, si evidenzia inoltre che l'art.10 del Regolamento sull'IA pone regole per la *governance* dei dati di addestramento di modelli di IA che pongono l'accento sui parametri di qualità dei dati e sui rischi di discriminazione dei diritti fondamentali.

[82] In tal senso, anche il Regolamento europeo sull'IA, nel Considerando 20, evidenzia come, al fine di ottenere i massimi benefici dai sistemi di IA, proteggendo nel contempo i diritti fondamentali, la salute e la sicurezza e di consentire il controllo

ziative dei singoli titolari e la strada da percorrere – anche da un punto di vista normativo – qualora si intenda utilizzare tali strumenti, in conformità al Regolamento sull'IA, per finalità domestiche di governo sanitario con un coinvolgimento dell'Autorità Garante al pari della comunità scientifica e professionale e delle categorie degli assistiti [83].

A tal fine, è necessario che, nella descrizione dei trattamenti, siano puntualmente indicate le logiche algoritmiche utilizzate al fine di generare i dati e i servizi attraverso i suddetti sistemi di IA, le metriche utilizzate per addestrare il modello e valutare la qualità del modello di analisi adottato, le verifiche svolte per rilevare a presenza di eventuali *bias*, le misure correttive eventualmente adottate, le misure idonee a verificare, anche a posteriori, le operazioni eseguite da ciascun oggetto autorizzato, i rischi insiti nelle analisi deterministiche e stocastiche. Nei sistemi di intelligenza artificiale in sanità, insomma, la protezione dei dati deve essere necessariamente considerata la cornice entro la quale viene garantita l'effettività dei diritti fondamentali in gioco.

Ma l'assenza di una disciplina specifica sulla responsabilità civile per l'intelligenza artificiale mantiene incertezze nel sistema giuridico per la sua disomogeneità a livello europeo, dovuta alla presenza di re-

---

democratico, l'alfabetizzazione in materia di IA dovrebbe dotare i fornitori, i *deployer* e le persone interessate delle nozioni necessarie per prendere decisioni formate in merito ai sistemi di IA.

[83] Il Garante, nel predetto decalogo per la realizzazione di servizi sanitari attraverso sistemi di IA, ha ricordato infatti che in base al principio della «protezione dei dati fin dalla progettazione» (art. 25, par. 1, del Regolamento), nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario, devono essere adottare misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati (art. 5 del Regolamento) e integrare nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati. Tali misure, volte ad assicurare l'effettiva applicazione dei principi in materia di protezione dei dati personali devono assicurare – per impostazione predefinita – la proporzionalità del trattamento rispetto all'interesse pubblico perseguito, ponendosi l'obiettivo di ottenere un reale effetto di tutela. Un approccio *privacy by design* impone anche l'analisi dei ruoli del trattamento connessi alla realizzazione di sistemi di IA in ambito sanitario, che deve corrispondere alle attività che il soggetto svolge in concreto alla luce dei compiti istituzionalmente demandati allo stesso, in conformità al quadro giuridico di settore (cfr. anche punto 3 del predetto decalogo).

golamentazioni domestiche non sovrapponibili. Inoltre, le vittime di danni causati da decisioni algoritmiche incontreranno ostacoli probatori significativi, visto che la vicinanza alle fonti di prova appartiene alla parte danneggiante. *De jure condendo*, non può che auspicarsi, pertanto, un nuovo modello di responsabilità oggettiva, che, eventualmente, ripartisca i costi sui soggetti che sono parte dell'operazione economica in modo collettivo, eventualmente prospettando la costituzione di un fondo ovvero la formulazione di meccanismi di assicurazione in capo ai soggetti che potrebbero essere chiamati a risarcire il danno [84]. La persistenza di tale vuoto normativo potrebbe, peraltro, determinare un ampliamento del ruolo della Corte di Giustizia dell'Unione europea nell'interpretazione dei principi di responsabilità in relazione all'intelligenza artificiale, generando un quadro nel quale le condizioni di responsabilità dipenderanno da un processo evolutivo non sempre lineare e caratterizzato da decisioni suscettibili di variare in base ai casi concreti esaminati.

---

[84] Cfr., in tal senso, anche G. FINOCCHIARO, *Intelligenza artificiale. Quali regole?*, Bologna, Il Mulino, 2024, 67 ss. I problemi maggiori sono strettamente collegati all'IA generativa di fronte alla quale soltanto un sistema di sicurezza sociale che «non cerca un responsabile ma considera il danno subíto e non quello causato» (così A. PROCIDA MIRABELLI DI LAURO, *La riparazione dei danni alla persona*, Napoli, ESI, 1993, 47) potrebbe consentire il diritto alla riparazione senza affaticarsi ad individuare il soggetto obbligato a risarcire. Si segnala, peraltro, che, sul fronte domestico, la nuova legge italiana sull'intelligenza artificiale n. 132/2025 ha previsto, all'art. 24, commi 3 e 5, una delega al Governo ad adottare, entro dodici mesi dalla data di entrata in vigore di tale legge, un decreto legislativo per adeguare e specificare la disciplina dei casi di realizzazione e di impieghi illeciti di sistemi di intelligenza artificiale. In particolare, nei casi di responsabilità civile, dovranno essere previsti strumenti di tutela del danneggiato, anche attraverso una specifica regolamentazione dei criteri di ripartizione dell'onere della prova, tenuto conto della classificazione dei sistemi di intelligenza artificiale e dei relativi obblighi come individuati dal regolamento (UE) 2024/1689. Appare chiaro, quindi, come il legislatore italiano abbia condivisibilmente previsto che, in caso di danni causati dall'utilizzo dell'intelligenza artificiale, l'onere probatorio, a prescindere dalla natura contrattuale o extracontrattuale della responsabilità, debba essere a carico del soggetto danneggiante.

Capitolo II

DIFFICOLTÀ INTERPRETATIVE E APPLICATIVE NELL'USO SECONDARIO DEI DATI SANITARI TRA GDPR, CODICE *PRIVACY* ED ELABORAZIONE DELLE CORTI E DELLE AUTORITÀ GARANTI

Sommario: 1. L'ulteriore utilizzo dei dati sanitari nella disciplina del GDPR, del Codice *Privacy* e delle regole deontologiche. – 2. Plurime difficoltà interpretative inibenti l'uso secondario dei dati. Il consenso ampio, il consenso a più livelli e la controversia sulle modalità di anonimizzazione – 3. Il trattamento ulteriore da parte del titolare o di terzi dei dati personali secondo gli art. 110 e 110 *bis* del Codice *privacy*

1. *L'ulteriore utilizzo dei dati sanitari nella disciplina del GDPR, del Codice Privacy e delle regole deontologiche*

Dato atto del contesto normativo in ordine alla regolamentazione del fascicolo sanitario elettronico e dell'Ecosistema dei dati sanitari, pare opportuno, a questo punto, analizzare la disciplina ad oggi vigente in merito all'utilizzo ulteriore dei dati sanitari (*secondary use*), desumibile dal GDPR e dal Codice Privacy, per constatarne la complessità e la scarsa chiarezza, dovuta anche alla molteplicità di fonti che la regolano. Ciò pure per comprendere i motivi della pressione generalizzata verso una regolamentazione unitaria a livello europeo quale quella ormai prossima all'esordio, in forza del Regolamento EHDS n. 327/2025.

Occorre, innanzitutto, partendo dal dato normativo eurounitario, tenere presente che, stando all'ultimo comma dell'articolo 6, GDPR,

al di fuori della legittimazione fornita dal consenso dell'interessato o dalla presenza di una norma del diritto europeo o interno che costituisca misura necessaria e proporzionata per la salvaguardia degli obiettivi di cui all'art. 23, comma 1, GDPR [1], un trattamento dei dati può riguardare finalità altre solo se compatibili rispetto a quelle originarie [2].

L'art. 5, par.1 lett. b, del Regolamento UE 2016/679, aggiunge che il trattamento secondario a fini di archiviazione nel pubblico interesse,

---

[1] Si tratta dei seguenti obiettivi: a) la sicurezza nazionale; b) la difesa; c) la sicurezza pubblica; d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale; f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari; g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate.

[2] Il Considerando n. 50 GDPR specifica che per il trattamento per finalità ulteriori ma compatibili non è necessaria una base giuridica diversa da quella originaria e che il trattamento ulteriore fondato sul consenso o sul perseguimento di obiettivi di interesse pubblico generale dovrebbe essere consentito, a prescindere dalla compatibilità dei fini. Il profilo si intreccia anche alla possibilità del titolare di mutare l'originaria base giuridica a fondamento del trattamento, argomento che il WP29 ha analizzato con riguardo al consenso nelle *Guidelines on consent under Regulation* 2016/679, adottate il 10 aprile 2018. Il documento si concentra in particolare sul passaggio dal consenso ad altre condizioni del trattamento ed appare dominato dalla preoccupazione di evitare che, sorti problemi sulla validità del consenso, il titolare possa proseguire il trattamento invocando un'altra base legittimante, in particolare facendo valere, con effetto retroattivo, il motivo legittimo, tanto da affermare che «*under the GDPR, it is not possible to swap between one lawful basis and another*». Nelle citate *Guidelines* 2/2019, l'EDPB precisa inoltre che, quando il trattamento è basato sul consenso, posto che l'interessato ha fatto affidamento sul rilascio dei suoi dati ai fini dell'esecuzione di un contratto, il trattamento ulteriore è consentito solo se la residua base giuridica è individuata all'inizio del trattamento ed esplicitata nell'informativa. Di conseguenza, «*it is generally unfair to swap to a new legal basis when the original basis ceases to exist*».

di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali, conformemente all'articolo 89, paragrafo 1 [3]. Si tratta di una presunzione di non incompatibilità, che, stando alla lettera della norma, non è assoluta, ma subordinata alla necessità di raccogliere i dati in forma anonima o di anonimizzarli subito dopo; se ciò non fosse possibile, i dati personali dovrebbero almeno essere pseudonimizzati. In realtà, però, già il Considerando 50 del

[3] Si rinviene una peculiare presunzione di conformità del reimpiego dei dati sanitari a fini di ricerca scientifica, nella misura in cui questa è operata in connessione «con attività di tutela della salute svolte da esercenti professioni sanitarie od organismi sanitari, ovvero con attività comparabili in termini di significativa ricaduta personalizzata sull'interessato» vedi Garante privacy, *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica*, pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101, 19 dicembre 2018. Cfr. altresì, Id., *Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati*, § 5, sulle disposizioni in materia di dati trattati per scopi di ricerca scientifica; Cfr., a riguardo, G. Garofalo, *Trattamento e protezione dei dati personali: spunti rimediali in àmbito sanitario*, in *Diritto di famiglia e delle persone*, 2021, 1392 ss. Con riguardo agli scopi statistici e scientifici, è opportuno riferirsi ai considerando 159 e 162 del Regolamento, secondo cui: «il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato fino ad includere lo sviluppo tecnologico e la dimostrazione, la ricerca fondamentale, la ricerca applicata, la ricerca finanziata da privati [...] e gli studi svolti nell'interesse pubblico nel settore della sanità pubblica». Secondo il Garante europeo, «tale nozione non può essere estesa oltre il suo significato comune per cui si debba intendere un progetto di ricerca istituito conformemente alle pertinenti norme metodologiche e deontologiche in materia e in linea con le buone pratiche di settore» (EDPB, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, 4 maggio 2020, [EDPB rev 01],33). Nella definizione di ricerca scientifica rientra anche la ricerca basata sui registri. Dalla combinazione delle informazioni provenienti dai registri, i ricercatori possono ottenere nuove conoscenze di grande utilità per la collettività, ad esempio, relativamente a patologie diffuse. Attraverso questo tipo di ricerca, i risultati ottenuti possono acquistare maggiore rilevanza, dal momento che si basano su una popolazione più ampia. Rientra dunque nella nozione di ricerca scientifica ogni attività diretta a generare nuova conoscenza e ad avanzare lo stato dell'arte in un determinato settore scientifico, sia che si tratti di ricerca di base, sia che si tratti di ricerca applicata e sia essa pubblica o privata e dunque anche quando abbia finalità commerciali.

GDPR pone qualche dubbio sull'automatica non incompatibilità dell'uso secondario, laddove così si esprime: «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. La base giuridica fornita dal diritto dell'Unione o degli Stati membri per il trattamento dei dati personali può anche costituire una base giuridica per l'ulteriore trattamento. Per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento dovrebbe, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tener conto tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto». Inoltre, l'EDPS, nella sua opinione preliminare sulla protezione dei dati e ricerca scientifica, propende per un'interpretazione restrittiva, suggerendo di non assimilare le condizioni di legittimità del trattamento con la determinazione della finalità, ma di effettuare, anche in caso di riuso dei dati per scopi di ricerca, il *test* di compatibilità di cui all'art. 6, par. 4[4]. Tale *test* non è di immediata eseguibilità, ma richiede un'attenta analisi. Sul punto, è atteso da tempo un chiarimento da parte dell'EDPB nelle future linee guida sul trattamento dei dati personali

[4] Cfr. EDPS, *Preliminary opinion on data protection and scientific research*, del 6/1/2020, 23 in *https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en*:"*We would therefore argue that, in order to ensure respect for the rights of the data subject, the compatibility test under Article 6(4) should still be considered prior to the reuse of data for the purposes of scientific research, particularly where the data was originally collected for very different purposes or outside the area of scientific research. Indeed, according to one analysis from a medical research perspective, applying this test should be straightforward*".

per finalità di ricerca scientifica [5]. Ordinariamente, poi, il titolare del trattamento è tenuto ad informare l'interessato del trattamento secondario, ai sensi dell'art. 14, par. 4 del GDPR, e questo determina che, laddove il trattamento originario si fondi sul consenso, l'interessato potrà comunque decidere di intervenire sulla circolazione, interrompendola (con la revoca o l'opposizione) [6] o conformandone la prosecuzione. L'art. 14, par. 5, lett. b) GDPR esenta però il titolare del trattamento dall'obbligo di fornire l'informativa *privacy* di cui ai par. da 1 a 4 dell'art. 14 GDPR, nella misura in cui ciò risulti impossibile o implichi uno sforzo sproporzionato [7]. L'esercizio del diritto di revoca produrrebbe effetti *ex nunc*, non incidendo sulla liceità del trattamento compiuto fino al momento del suo esercizio, e determinerebbe la cancellazione dei dati, ai sensi dell'art. 17, par. 1, lett. b), anche nei confronti dei terzi aventi causa del titolare del trattamento (art. 19).

---

[5] Come annunciato rispettivamente in EDPB, *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, e in EDPB, *Guidelines 3/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*.

[6] Cfr. a riguardo C. Rapisarda, *Ricerca scientifica e circolazione dei dati personali. verso il definitivo superamento del paradigma privatistico?*, in *Europa e diritto privato,* 2021, 301 ss.

[7] Come messo in luce dal Garante, resta in siffatti casi il dovere del titolare di adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche attraverso la pubblicazione, ad esempio, sui siti *internet* dei centri coinvolti (cfr. Garante per la protezione dei dati personali, provvedimento n. 285 del 6 luglio 2023, *doc. web 9919999*). Il Garante ha più volte rimarcato la descritta necessità della piena liceità del trattamento iniziale, per sorreggere la legittimità del trattamento ulteriore volto al perseguimento di finalità diverse, ma compatibili con quelle originarie, in particolare nei provvedimenti relativi al controllo a distanza dell'attività lavorativa, in relazione a quanto previsto dall'art. 4, ult. cpv., L. 20 maggio 1970, n. 300, ossia alla possibilità di trattare i dati raccolti dagli strumenti che consentono il controllo a distanza per successive finalità connesse al rapporto di lavoro (cfr. GPDP, 28 ottobre 2021, *doc. web n. 9722661;* GPDP, 13 maggio 2021 *doc. web n. 9669974*; GPDP, 24 maggio 2017, *doc. web n. 6495708*; in altro contesto, si veda GPDP, 10 novembre 2022, doc. web n. 9835095). Cfr. D. Sborlini, *Proporzionalità dei trattamenti di dati personali svolti mediante dispositivi di geolocalizzazione in ambito lavorativo*, in *Diritto di internet*, 2023, 1, 163 ss.

Il legislatore europeo, peraltro, ha lasciato agli Stati membri la possibilità di restringere ulteriormente il diritto di opposizione, nonché l'esercizio degli altri strumenti di controllo riconosciuti all'interessato (accesso, rettifica, limitazione), laddove gli stessi rischino di rendere impossibile o pregiudichino gravemente il conseguimento delle finalità specifiche di ricerca e tali deroghe siano necessarie, una volta prestate le dovute garanzie, al conseguimento di detti scopi (art. 89, par. 2, GDPR), quali la predisposizione di apposite misure tecniche e organizzative, per la tutela dei diritti e della libertà dell'interessato [8].

2. *Plurime difficoltà interpretative inibenti l'uso secondario dei dati. Il consenso ampio, il consenso a più livelli e la controversia sulle modalità di anonimizzazione*

Se questa è la cornice normativa di applicazione unionale, si deve precisare che, in base a quanto definito dall'art. 5 commi 2 e 3 delle «Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica» [9], il cui rispetto «costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali» (*ex* art. 2-*quater*, comma 4, del D. Lgs. 196/2003, Codice *privacy*) [10], il trattamento

---

[8] Cfr. Parere 3/2019, del Comitato europeo per la protezione dei dati, relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati, del 23 gennaio 2019; "*A preliminary Opinion on data protection and scientific research*" del Garante europeo, del 6 gennaio 2020; "*Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research", del 2 febbraio 2021 del Comitato europeo per la protezione dei dati, provv.* del Garante del 1° novembre 2021, (*docweb* 9731827).

[9] Cfr. Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101, 19 dicembre 2018 (*docweb 9069677*), in *www.garanteprivacy.it*

[10] Il Garante ha chiarito che «il trattamento di dati personali per scopi di ricerca scientifica deve essere effettuato nel rispetto del Regolamento, del Codice, delle pre-

ulteriore di dati sanitari da parte dei soggetti privati che partecipano al Sistema statistico nazionale ai sensi della legge 28 aprile 1998, n. 125, richiede comunque il consenso dell'interessato. L'ordinamento italiano, quindi, si è avvalso del potere conferito agli Stati membri dal par. 4 dell'art. 9 del GDPR, secondo cui «gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute», e richiede il consenso quale «ulteriore condizione di liceità» se ad operare sia un soggetto privato, per intuibili motivi di protezione dell'interessato [11].

---

scrizioni relative al trattamento dei dati genetici (se necessario) e delle prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica, allegati 4 e 5 al provvedimento del 5 giugno 2019 (*doc. web 9124510*), nonché delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, allegato A5 al Codice, che costituiscono condizione essenziale di liceità e correttezza dei trattamenti» (Garante *privacy*, provv. n. 118 del 7 aprile 2022, doc. web n. 9772545). Si ricorda che, in attuazione di quanto previsto dall'art. 9, par. 4 GDPR, il legislatore ha disposto all'art. 2-*septies* codice *privacy* che il trattamento di dati genetici, biometrici e relativi alla salute debba avvenire in conformità alle misure di garanzia adottate dal Garante e, in particolare, limitatamente ai dati genetici, quale ulteriore misura di protezione dei diritti dell'interessato, sulla base del consenso e di altre cautele specifiche.

[11] Durante il periodo pandemico, la Regione Friuli ha sviluppato un progetto di stratificazione statistica di pazienti fragili, correlato alle complicanze in caso di infezione da Covid-19: il progetto prevedeva il coinvolgimento dei medici di medicina generale, chiamati a validare attraverso il portale informatico regionale una lista di utenti/assistiti in relazione alle loro condizioni di complessità e comorbilità. Attraverso questo sistema si realizzava, accedendo alle banche dati delle ASL e lavorando i dati attraverso un *software* di classificazione, un profilo di rischio dei pazienti prodromico alla successiva presa in carico dei medesimi. Tali operazioni di trattamento rientrano nell'ambito della c.d. «medicina di iniziativa» rivolta, nel caso di specie, al solo contesto emergenziale (in tal senso, vedi provvedimento Garante Privacy del 15 dicembre 2022 (*docweb* 9844989). Per «medicina di iniziativa» si intende un modello assistenziale orientato alla «promozione attiva» della salute dell'individuo, specie se affetto da malattie croniche o disabilità, e alla responsabilizzazione delle persone nel proprio percorso di cura. Per il Garante, questo tipo di trattamenti è da considerare ulteriore e autonomo rispetto a quello strettamente necessario alle ordinarie attività

Il consenso, quale base giuridica, però, non sembra garantire sufficientemente la libertà di scelta dell'interessato, considerata la nota asimmetria informativa tra il paziente e il promotore della ricerca clinica. Vi è di più. Il considerando 33 del GDPR sembra non negare o non vietare possibili forme di utilizzo di un (pur discutibile) consenso ampio, affermando che: «in molti casi non è possibile individuare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica, laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati do-

---

di cura e prevenzione (art. 9, par. 2 lett. h) del GDPR), e quindi effettuabile solo sulla base dello specifico consenso informato dell'interessato (art. 9, par. 2 lett. a) GDPR (Cfr., *ex multis*, parere sul disegno di legge della Provincia autonoma di Trento che reca specifiche disposizioni in materia di medicina di iniziativa, dell'8 maggio 2020, *doc. web n. 9344635*). Secondo il Garante medesimo, il legislatore non ha incluso la medicina di iniziativa tra le finalità perseguibili attraverso il FSE e la prestazione del consenso dell'interessato al trattamento dei dati presenti nel FSE per finalità di cura non legittimerebbe i soggetti che vi accedono ad elaborare le informazioni ivi presenti per delineare specifici profili di rischio sanitario dell'interessato. Il Garante, quindi, ha sanzionato tre aziende sanitarie locali, in qualità di titolari del trattamento, che doveva considerarsi privo di base giuridica. Il Tribunale di Pordenone in data 13 ottobre 2023 e il Tribunale di Udine in data 21 settembre 2023 hanno però annullato il suddetto provvedimento (in *Garanteprivacy.it doc. web n. 9844989*). Pure il Tribunale di Trieste risulta aver disposto la sospensione dell'efficacia del provvedimento, a seguito di apposita impugnazione. (cfr. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9845312). Nell'occasione, i Giudici di merito hanno ritenuto che il trattamento effettuato avesse invece finalità di prevenzione, finalità espressamente elencata dall'art. 12 d.l. n. 179/2012, convertito con modificazioni in legge 17 dicembre 2012, n. 221 e d.p.c.m 29 settembre 2015, n. 178 e oggi D.M. 7 settembre 2023, e da considerarsi del tutto «compatibile con la finalità primaria di diagnosi e cura. Si evidenziava poi come tale trattamento potesse comunque trovare la sua base giuridica nell'art. 9 lett. i) GDPR, relativo ai motivi di interesse pubblico e, nello specifico, nei diversi provvedimenti legislativi emanati durante l'epoca Covid che legittimavano gli enti pubblici ad utilizzare i dati sanitari per gestire al meglio l'emergenza (O.C.D.P.C. n. 630 del 3 febbraio 2020; il DL 18/2020, il D.L. 34/2020).

vrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista»[12]. Ma le attuali «norme deontologiche riconosciute per la ricerca scientifica» in Italia puntualizzano che se il consenso viene utilizzato come base giuridica, esso dovrà essere dato «per una o più specifiche finalità» e soddisfare anche le condizioni di cui all'articolo 7, tra cui: – il fatto che il responsabile del trattamento deve essere in grado di dimostrare il consenso, richiedendosi una vera e propria struttura di governo dei trattamenti; la richiesta di consenso per la protezione dei dati deve essere presentata in un modo che sia «chiaramente distinguibile» dal consenso richiesto per altre questioni ed «in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro»; l'interessato deve avere il diritto di revocare il proprio consenso in qualsiasi momento; inoltre, alcuni diritti degli interessati si applicano solo se il consenso o gli interessi legittimi sono utilizzati come base giuridica.

---

[12] Com'è noto, i Considerando non sono enunciati di carattere normativo suscettibili di essere applicati (cfr. ad es. Corte UE, 13 settembre 2018, Česká pojišťovna a.s., C-287/17, in *www.curia.europa.eu*, punto 33), ma forniscono un supporto interpretativo all'applicazione, in senso tecnico, delle disposizioni normative. Per il Comitato europeo per la protezione dei dati, il Considerando in esame ammette un «approccio flessibile» al grado di specificazione del consenso nel contesto della ricerca scientifica (Cfr. EDPB, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, cit., 33 ss., e, in precedenza, Gruppo di lavoro ex Art. 29, Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, 10 aprile 2018, 31 ss.). Pertanto, se, in linea di principio, il trattamento da effettuarsi nell'esecuzione di un progetto di ricerca può essere legittimato da tale base giuridica solo ove la finalità sia descritta in modo ben definito, in via eccezionale, viene ammessa la possibilità di descrivere la finalità «a un livello più generale», laddove, nel contesto di un certo progetto, non risulti possibile specificare in modo pieno lo scopo nella fase iniziale dell'attività. Rileva efficacemente che il consenso ampio rende mobili i confini di liceità del trattamento e i limiti della situazione giuridica soggettiva attiva facente capo al titolare, D. Sborlini, *Il broad consent come mezzo per la valorizzazione dei dati personali nell'ambito della ricerca scientifica e il suo rilievo negli spazi di condivisione dei dati*, in *Contratto e impresa*, 2024, 223 ss.

A causa delle preoccupazioni che il consenso ampio non abbia i crismi di un reale consenso informato [13], il consenso a più livelli, che fornisce ai partecipanti una gamma di preferenze di consenso ed il consenso dinamico, che utilizza la tecnologia dell'informazione per facilitare il consenso ai progetti, modificare e aggiornare le loro preferenze di consenso, sono emerse come potenziali nuove forme di consenso per la ricerca ad alta intensità di dati [14].

Secondo l'EDPB, infatti, «quando non è possibile specificare appieno le finalità della ricerca, il titolare del trattamento deve cercare altri modi per garantire il rispetto dell'essenza dei requisiti del consenso, ad esempio permettendo agli interessati di acconsentire a una fina-

---

[13] L'espressione «consenso ampio» è mutuabile da documenti ufficiali quali ad es. EDPS, *A Preliminary Opinion on data protection and scientific research*, cit., 19; EDPB, EDPB, *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, cit., 7 ss. Si riferiscono al *broad consent* anche le indicazioni relative al Considerando n. 33, Reg. cit. fornite dalla Conferenza delle autorità di protezione dei dati indipendenti della Germania (DSK, «Datenschutzkonferenz», Beschluss der 97. *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO*, 3 April 2019), nonché le disposizioni della normativa austriaca che disciplinano il consenso contemplato dal medesimo Considerando (cfr. art. 2(d)(3) *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Forschungsorganisationsgesetz*). In argomento, vedi ancora D. SBORLINI, *Il broad consent come mezzo per la valorizzazione dei dati personali nell'ambito della ricerca scientifica e il suo rilievo negli spazi di condivisione dei dati*, in *Contratto e Impresa*, 2024, 223 ss.

[14] Sempre più spesso ci sono esempi di integrazione del consenso dinamico e del consenso elettronico nella ricerca (Cfr. R. BIASIOTTO, P. PRAMSTALLER, D. MASCALZONI, *The dynamic consent of the Cooperative Health Research in South Tyrol (CHRIS) study: broad aim within specific oversight and communication*, in *BioLaw Journal,* 2021, 277 ss.; H.J.A. TEARE, M. PRICTOR, J. KAYE, *Reflections on dynamic consent in biomedical research: the story so far*, in *European Journal of Human Genetics,* 2021, 649–56). Le critiche al consenso dinamico hanno sollevato preoccupazioni riguardo il fatto che il medesimo potrebbe causare alti tassi di abbandono, e il sistema sarebbe difficile da gestire, in particolare per coloro che non sono alfabetizzati digitalmente. Il consenso dinamico, peraltro, richiede investimenti nella creazione del sistema, sia in termini di infrastruttura che di personale.

lità di ricerca in termini più generali e a fasi specifiche di un progetto di ricerca che si sa già sin dall'inizio avranno luogo. Durante l'avanzare della ricerca, sarà quindi possibile ottenere il consenso per le fasi successive del progetto prima dell'inizio della fase corrispondente». L'EDPB precisa che la mancanza di specificazione della finalità può essere compensata dalla fornitura periodica, da parte del titolare del trattamento, di informazioni sullo sviluppo della finalità durante l'avanzamento del progetto di ricerca, in maniera tale che, nel tempo, il consenso sia il più specifico possibile. In tal modo l'interessato ha quanto meno una conoscenza di base dello stato di avanzamento, che gli consente di valutare se esercitare o meno, ad esempio, il diritto di revoca del consenso [15]. Anche la messa a disposizione di un piano

[15] Questa soluzione, che peraltro è stata fatta propria dal legislatore finlandese (cfr. art. 14, paragrafo 1, dell'attuale legge sui dati personali della Finlandia - Henkilötietolaki, 523/1999), come specificato dal Comitato europeo per la protezione dei dati personali, si baserebbe sulla « messa a disposizione di un piano di ricerca esaustivo al quale gli interessati [potrebbero] fare riferimento prima di esprimere il loro consenso [...] [contribuendo] a compensare una mancanza di specificazione delle finalità », comunicando agli interessati gli sviluppi del piano medesimo man mano che si concretizzano. Secondo una simile impostazione risulta a fasi progressive non l'ottenimento del consenso, ma esclusivamente l'obbligo informativo gravante sul Titolare, il quale deve pertanto informare l'interessato di tutti gli sviluppi del progetto di ricerca a cui quest'ultimo ha aderito, consentendogli così di scegliere liberamente se continuare a consentire il trattamento dei propri dati personali anche per le nuove attività di ricerca o se, al contrario, revocare il proprio consenso. È evidente come questa soluzione sia volta alla massimizzazione delle attività di ricerca: il consenso è infatti ottenuto in una fase in cui ancora non sono stati definiti tutti i criteri della ricerca, ma è comunque già stato realizzato un piano di ricerca esaustivo da presentare agli interessati. Nel momento in cui la ricerca viene sviluppata e integrata, il titolare deve semplicemente informare gli interessati senza premurarsi di ottenere un nuovo e ulteriore consenso specifico. Questo è un consenso definibile come informativo incrementale: non si ha infatti una progressione di consensi specifici, ma un incremento della consapevolezza degli interessati, che sono pertanto liberi di revocare il consenso (in tal senso, vedi M. Liotta, *Il favor per la ricerca scientifica e la sua effettiva applicazione nella normativa europea, nazionale e da parte dell'autorità garante*, in *Diritto dell'informazione e dell'informatica*, 2024, 363 ss.) La giurisprudenza di legitti-

di ricerca esaustivo al quale gli interessati possano fare riferimento prima di esprimere il loro consenso potrebbe contribuire a compensare una mancanza di specificazione delle finalità [16]. Il piano di ricerca dovrebbe specificare nella maniera più chiara possibile i quesiti che la ricerca si pone e i metodi di lavoro previsti [17]. L'acquisizione di una manifestazione di volontà dell'interessato rimane in ogni caso un'operazione complessa. Invero, quando l'attività di ricerca si svolge a distanza di molto tempo dal momento dell'originario conferimento dei dati, è frequente l'insorgere di difficoltà di natura tecnica, organizzativa o etica che rendono complesso o impossibile acquisire il consenso degli interessati, come nel caso in cui, ad esempio, i dati necessari alla ricerca siano relativi a persone decedute, non contattabili o versanti in uno stato clinico di particolare gravità. In questi casi, previsti dalla normativa primaria, l'implementazione delle soluzioni è resa assai complessa

---

mità ha però evidenziato che «in tema di trattamento dei dati personali, il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento a un trattamento chiaramente individuato» (Cass. 25 maggio 2021, n. 14381, in *Diritto dell'informazione e dell'informatica,* 2021, 1001 ss.). Sulla specificità del consenso, si veda Corte UE, 11 novembre 2020, Orange Romania, C-61/19, in *www.curia.europa.eu*.

[16] Lo scopo di tali trattamenti deve essere individuato in modo specifico all'interno del progetto di ricerca e in nessun caso risulta ammissibile un trattamento per generici e non meglio determinati «scopi di ricerca» (cfr. Article 29, *Data Protection Working Party, Opinion 03/2013 on purpose limitation*, cit., 15-16; EDPB, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, cit., 33 ss. Così, anche in base al consolidato orientamento del Garante, rispetto al quale cfr., ad es., GPDP, 6 luglio 2023, doc. web n. 9919999; GPDP, 27 aprile 2023, doc. web n. 9898815).

[17] Cfr. par. 158, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, versione 1.1 adottate il 4 maggio 2020, p 34. 11 Cfr. par. 160 e 161, cit., 34 e 35. Su questi temi, vedi anche EDPB, EDPB *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, che riprende l'orientamento dell'EDPS in relazione al concetto di *broad consent* contenuto nel considerando n. 33, specificando che "*It will also be necessary to take into account any provisions in MS law as allowed for in Article 9(4) GDPR containing further conditions pertaining to processing of health data, since those provisions in MS law could also impact (enable, facilitate or impede) the usability of 'broad consent' in that MS*" (par. 30, 9).

dalla normativa secondaria. Il consenso, pertanto, pur rappresentando il presupposto di liceità del trattamento certamente più noto e – talvolta impropriamente – anche quello più invocato, non sempre costituisce una soluzione sempre praticabile.

Alle difficoltà sinora esaminate, deve aggiungersi il fatto che, come già ricordato, la conduzione di studi transfrontalieri risente inevitabilmente delle differenti discipline giuridiche sulla protezione dei dati personali in questo specifico settore, dovute alla circostanza che, per effetto dell'art. 9, 4° comma del GDPR, i legislatori nazionali hanno la facoltà di introdurre ulteriori condizioni e limitazioni al trattamento dei dati relativi alla salute, biometrici e genetici [18]. Vi sono, infatti, Stati membri la cui disciplina appare più elastica, ed altri in cui sussistono norme più restrittive. Intimamente connessa alla discrezionalità riservata agli Stati membri appena accennata è anche la problematica relativa all'anonimizzazione dei dati [19].

---

[18] Se l'Italia, come visto, ha adottato un approccio restrittivo all'attuazione del GDPR per la ricerca e richiede il consenso come base giuridica per il trattamento dei dati genetici a fini di ricerca, in altri paesi, il consenso può non essere obbligatorio come base giuridica del trattamento dei dati, ma richiesto nell'ambito delle norme etiche nazionali. Cfr. *Assessment of the EU Member States' rules on health data in the light of GDPR. 2023,* consultabile in *https://health.ec.europa.eu/publications/assessment-eu-member-states-rules-health-data-light*-gdpr_en

[19] Tra le tecniche di anonimizzazione elencate dal Gruppo di lavoro «Articolo 29», figurano: i) le cd. tecniche di randomizzazione, secondo cui si altera la veridicità dei dati, rendendoli incerti e impedendo la correlazione tra gli stessi e l'interessato, tramite l'aggiunta di rumore statistico, permutazione o privacy differenziale; ii) le cd. tecniche di generalizzazione, consistenti nel generalizzare o diluire gli attributi degli interessati, tramite un'aggregazione (cosiddetto «k-anonimato») oppure un L-L-diversità/T-vicinanza (cfr. Gruppo di lavoro «Articolo 29», Parere 5/2014 sulle tecniche di anonimizzazione, cit., par. 3.1 e ss.). Nello specifico, il parere 05/2014 dell'EPBD precisa che, sebbene nessuna tecnica di per sé consenta un'anonimizzazione efficace, l'applicazione congiunta di più misure può ridurre il rischio in termini di: (i) «*single out*», con cui si intende la possibilità di isolare un interessato all'interno di un gruppo; (ii) «*linkability*» ovvero la possibilità di collegare un dato anonimizzato a dati personali di un interessato all'interno di un gruppo; (iii) «*inference*», ossia inferire nuovi dati personali di un interessato tramite l'elaborazione di dati anonimizzati. Tale

Come è noto, gli ostacoli sopra illustrati sarebbero facilmente superabili se le attività di ricerca potessero essere condotte su dati anonimi, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. La normativa in materia di protezione dei dati personali, infatti, non si applica a tali tipi di dati. Tuttavia, oggi non esistono criteri di valutazione della natura personale o anonima dei dati condivisi da tutti, bensì essi mutano da ordinamento a ordinamento e non è rinvenibile una tendenza comune. Anche in giurisprudenza i pareri sul concetto stesso di dato anonimo e pseudonimizzato sembrano discordi. Sul punto, giova richiamare una recente pronuncia del Tribunale dell'Unione europea che, sebbene con riferimento al Regolamento (UE) 2018/1725 sulla tutela delle persone fisiche in relazione al trattamento

---

verifica sulla riduzione del rischio, specifica l'EPBD, deve svolgersi caso per caso. Sulla stessa scorta si pongono anche le c.d. Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, all. 4 del d.lgs. 196/2003 («Codice Privacy»), novellato dal d.lgs. 101/2018, le quali forniscono indicazioni tecniche utili a valutare quando ricorra l'identificabilità dell'interessato e quali siano i criteri da osservare per la valutazione del rischio di identificazione. L'art. 4, co. 1, lett. a) di tali regole prevede che, in ambito statistico, «un interessato si ritiene identificabile quando, con l'impiego di mezzi ragionevoli, è possibile stabilire un'associazione significativamente probabile tra la combinazione delle modalità delle variabili relative ad una unità statistica e i dati che la identificano». Ancora, l'art. 4, co. 1, lett. b) elenca una serie di «mezzi ragionevolmente utilizzabili per identificare un interessato» tra cui: le risorse economiche e di tempo; dotazioni *hardware* e *software* alla base della re-identificazione, «tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al *software* di controllo adottati»; disponibilità congiunta di archivi contenenti informazioni di differente tipologia (nominative e non); «conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati». Si tratta, a ben vedere, di elementi di natura fattuale che dovrebbero essere oggetto di valutazione, anche sotto i profili della ragionevolezza, in sede di accertamento ispettivo, con il rischio, altrimenti, di precludere o restringere eccessivamente le possibilità di utilizzo dei dati e, pertanto, di conduzione degli studi clinici, come avvenuto nel caso Thin su cui *infra*.

dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, ha affermato un importante principio per l'interpretazione del concetto di dato anonimo e di dato pseudonimizzato, vale a dire che, al fine di stabilire la natura personale o meno di un'informazione, occorre in primo luogo verificare che quella informazione sia effettivamente «concernente» una persona fisica, tenendo conto del suo contenuto, della sua finalità e del suo effetto. In secondo luogo, si è aggiunto che, in caso di comunicazione di dati pseudonimizzati, non è sufficiente la mera esistenza di informazioni aggiuntive, tali da consentire la reidentificazione, presso terzi soggetti, bensì occorre accertare se il destinatario di tali dati pseudonimizzati disponga di «mezzi legali e realizzabili in pratica che gli consentano di accedere alle informazioni aggiuntive»[20]. Da

[20] Così Tribunale UE, 8a sezione ampliata, T 557/20, Comitato di risoluzione unico c. Garante europeo della protezione dei dati, 26 aprile 2023, ECLI:EU:T:2023:219. Tale approccio pare aderire a quanto precisato nelle linee guida dell'EPBD e delle autorità garanti nazionali per la protezione dei dati, che hanno delineato alcuni approdi interpretativi in materia di anonimizzazione dei dati (Sul punto, si vedano le linee guida in materia di pseudonimizzazione *dell'Agencia Espanola Protecciòn Datos* ("AEPD"), *Introduction to the hash function as a personal data pseudonymisation technique*, 2019, disponibili all'indirizzo *online https://www.aepd.es/documento/estudio-hash-anonimidad-en.pdf* e quelle, in materia di anonimizzazione, redatte *dall'Information Commissioner's Office, Privacy-enhancing technologies* (PETs), 2023 (disponibili all'indirizzo *https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf*). Per l'orientamento della nostra Authority, vedi però il Provvedimento del 1° giugno 2023 sul caso «Thin» (GPDP *doc.web* n.9913795), nel quale il Garante privacy ha negato la natura anonima dei dati raccolti dalla società Thin s.r.l. nell'ambito del cd. «*Health Improvement Network*», un progetto internazionale di raccolta e analisi di dati clinici fondato su di un *software* gestionale, in uso ai medici di medicina generale aderenti. Tali medici, in qualità di titolari del trattamento, raccoglievano e gestivano i dati dei pazienti, senza alcun intervento da parte di Thin. A seguito dell'anonimizzazione dei dati, questi erano, poi, trasferiti a Thin per la conduzione del proprio progetto. Il provvedimento del Garante mette in luce che la società Thin aveva adottato molteplici misure tecniche e organizzative volte a garantire l'anonimizzazione dei dati, quali processi di randomizzazione e generalizzazione dei dati, oltre al coinvolgimento di terze parti certificate, per ridurre il

ultimo, la Corte di Giustizia europea, con sentenza in data 4 settembre

---

rischio di re-identificazione dei pazienti. Secondo Thin, inoltre, non solo il progetto oggetto di contestazione era già stato condotto in altri Stati membri, senza alcuna contestazione da parte delle Autorità Garanti competenti, bensì le metodologie dalla stessa implementate risultavano assimilabili a quelle adottate in programmi afferenti alle principali Istituzioni pubbliche sanitarie (AIFA, Ministero della Salute, ecc.). Ciononostante, a giudizio del Garante, Thin, in qualità di autonomo titolare del trattamento, avrebbe raccolto dati personali — anche particolari — in violazione del principio di correttezza del trattamento (v. infra) di cui agli artt. 5, par. 1 lett. a) e 9, par. 2 GDPR, nonché in violazione dell'art. 13 sull'obbligo di informazione preventiva agli interessati. A giudizio del Garante, la società sanzionata avrebbe fondato il proprio progetto «sull'erroneo presupposto della natura anonima dei dati trattati», posta l'insufficienza delle misure di anonimizzazione del dato dalla stessa adottate. Il provvedimento del Garante sembrerebbe restringere la categoria dei dati anonimi a quei soli casi in cui la re-identificazione sia impossibile, in termini assoluti. Tale interpretazione non pare condivisibile sia sul piano pratico, considerata la celerità dello sviluppo tecnologico e la disponibilità di *database* sempre più vasti che, agendo sinergicamente, ampliano i margini di re-identificazione di un interessato, sia sul piano normativo, posto che il *test* di verifica sulla natura anonima o pseudonima dei dati oggetto di trattamento dovrebbe fondarsi, secondo il GDPR, sulla «ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica», nonché sulla verifica che i dati personali siano stati resi «sufficientemente anonimi». Il provvedimento è stato criticato da parte della dottrina (Vedi S. STEFANELLI, *Thin, perché il Garante sbaglia e blocca la ricerca in Sanità*, in *www.agendadigitale.eu* del 2 agosto 2023), che ha posto in luce come le motivazioni sul processo di anonimizzazione non tengano conto dei principi di cui alla sopracitata sentenza Tribunale UE 26 aprile 2023 T-557/2020, per cui la medesima anonimizzazione dovrebbe essere valutata in base a prove concrete, da svolgersi tanto da parte dei soggetti che la sostengono, quanto da parte delle Autorità di protezione dei dati nel corso delle istruttorie, e le suddette motivazioni sarebbero in controtendenza rispetto agli orientamenti delle altre Autorità Garanti europee. Va poi rimarcato che pure il CNIL, Autorità di controllo francese, ha adottato una posizione rigorosa in materia di anonimizzazione dei dati, al pari del Garante *Privacy* italiano (Cfr. provvedimento CNIL del 5.9.2024 nei confronti della società Cegedim Santé in *https://www.cnil.fr/en/health-data-cegedim-sante-fined-eu800000*). Esso, infatti, ha sottolineato l'importanza della corretta gestione dei dati sanitari pseudonimizzati, sanzionando una Società per non aver adottato misure sufficienti a garantire l'anonimizzazione dei dati sanitari trattati tramite un *software*, utilizzato da migliaia di medici per la gestione delle loro agende, delle cartelle cliniche e delle prescrizioni. Più in particolare, la Società aveva creato un osservato-

2025 (C-413/23P), ha precisato che l'esistenza di informazioni aggiuntive che consentono di identificare la persona interessata non implica, di per sé, che dati pseudonimizzati debbano essere considerati, in ogni caso e per qualsiasi persona, come dati personali ai fini dell'applicazione del Regolamento 2018/1725. Se chi intende trattare i dati ha la possibilità di re-identificare gli interessati, dovrà trattare i dati come personali; se questi non ha la possibilità materiale o legale di re-identificazione oppure il rischio che ciò avvenga può essere considerato insignificante (anche in ragione del fatto che comporterebbe uno sforzo sproporzionato in termini di tempo, costi e manodopera), i dati potranno essere considerati anonimi.

3. *Il trattamento ulteriore da parte del titolare o di terzi dei dati personali secondo gli art. 110 e 110 bis del Codice privacy*

Il Legislatore italiano, sulla base della più volte citata ampia delega prevista dall'art. 9, par. 4 GDPR, ha introdotto, con la riforma del Codice *privacy* del 2018, misure più restrittive rispetto a quanto previsto sia dalla previgente normativa nazionale, che dal GDPR stesso; si tratta dell'art. 110 del Codice *privacy*, rubricato «Ricerca medica, biomedica ed epidemiologica». Nello specifico, l'art. 110 stabilisce che i trattamenti dei dati sulla salute, per scopi primari e secondari, nell'ambito delle sperimentazioni cliniche, sono ammessi solo previa acquisizione del consenso dell'interessato [21]. Si tratta di una disposizione che, a dif-

---

rio sanitario, attraverso il quale i medici potevano condividere i dati estratti dalle cartelle cliniche dei pazienti per fini statistici e di studio, in cambio di sconti sull'uso del *software*. Sebbene la Società sostenesse che i dati fossero stati anonimizzati, l'indagine ha dimostrato che questi erano in realtà solo pseudonimizzati, poiché era ancora possibile risalire all'identità dei pazienti. Infatti, il processo di pseudonimizzazione aveva rimosso gli identificatori diretti, come nome e codice fiscale, ma ogni paziente rimaneva associato ad un identificatore univoco collegato al proprio medico di riferimento, che permetteva di tracciare la storia clinica del paziente nel tempo all'interno dello stesso studio o clinica, mantenendo quindi la possibilità di reidentificazione

[21] La Corte di Giustizia dell'Unione europea (CGUE, 21 dicembre 2023, ZQ,

ferenza di quella di cui all'art. 110-*bis*, si riferisce all'utilizzo ulteriore di

causa C-667/21, ECLI:EU:C:2023:1022, par. 67), ha precisato che: «uno Stato membro che intenda avvalersi della facoltà concessa all'articolo 9, paragrafo 4, di detto regolamento dovrebbe, conformemente al principio di proporzionalità, garantire che le conseguenze pratiche, segnatamente di ordine organizzativo, economico e sanitario, derivanti dagli ulteriori obblighi di cui tale Stato intende imporre il rispetto, non siano eccessive nei confronti dei titolari di un tale trattamento, i quali non dispongono necessariamente di dimensioni o di risorse tecniche e umane sufficienti per soddisfare tali obblighi». Orbene, gli articoli 110 e 110-*bis* del Codice Privacy, come si vedrà, parrebbero non del tutto aderenti al principio di proporzionalità, causando una restrizione eccessiva allo svolgimento di trattamenti di dati personali nell'ambito delle sperimentazioni cliniche, soprattutto da parte di operatori economici di piccole-medie dimensioni, non in grado di adempiere ai gravosi oneri procedurali imposti da tali norme. In tal senso, vedi anche M. GUIDI, *L'interazione tra la normativa dell'UE in materia di protezione dei dati personali e il Regolamento UE 536/2014 sulle sperimentazioni cliniche*, in *Diritto dell'informazione e dell'informatica*, 2024, 157. Tali norme, peraltro, si inseriscono in un quadro normativo di matrice europea che risulta, al contrario, caratterizzato da un evidente *favor* per la ricerca scientifica. In effetti nel GDPR sono numerose le disposizioni di favore per la ricerca scientifica e in particolare per quella medica. Basti pensare alle previsioni dettate dalle lettere a) ed e) dell'art. 5, che consentono il riutilizzo (*secondary use*) a fini di ricerca scientifica e la connessa conservazione di dati inizialmente raccolti per finalità diverse (ad esempio di cura), in deroga ai principi di limitazione della finalità e di limitazione della conservazione; si veda l'art. 14, par. 5, lettera b), che consente di derogare all'obbligo di informativa per la raccolta di dati finalizzati alla ricerca scientifica (purché siano presenti tutta una serie di requisiti fissati dalla stessa norma); l'art. 89, par. 2, che consente di derogare, nel rispetto delle garanzie poste dal par. 1 della stessa norma, a una serie di diritti dell'interessato (accesso, rettifica, limitazione, opposizione), qualora tali diritti rischino di rendere impossibile o pregiudicare gravemente il perseguimento delle finalità di ricerca scientifica e tali deroghe siano necessarie (Cfr. R. DUCATO, *Commento all'art. 89*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, Lefebvre Giuffrè, 2021, 970 ss.). Nel «Parere 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati» adottato dal CEPD il 23 gennaio 2019, l'EDPB, peraltro, sottolinea che il consenso non può ritenersi pienamente libero in situazioni di squilibrio (anche solo emotivo) tra le parti, come avviene appunto in ambito medico quando l'espressione del consenso è ridotta spesso a una pura formalità. In tali ipotesi, pertanto, secondo EDPB (vedi anche le «Linee guida 5/2020 sul consenso ai sensi del Regolamento

dati sanitari da parte del titolare che ne ha acquisito la disponibilità per motivi di cura. La necessità del consenso come condizione di liceità del trattamento conosce solo due eccezioni. La prima deroga trova applicazione quando la ricerca viene svolta in base a disposizioni normative o regolamentari, quali i programmi di ricerca biomedica o sanitaria di cui all'art. 12-*bis* del d.lgs. 30 dicembre 1992, n. 502, oppure quelli previsti dal diritto dell'Unione europea, ai sensi dell'art. 9, par. 2, lett. j) GDPR [22]. In tal caso, il trattamento dovrà essere antici-

(UE) 2016/679» adottate il 4 maggio 2020), il consenso non può costituire la base legittimante il trattamento dei dati (ma semmai rappresenta una garanzia aggiuntiva) e la tutela dell'interessato deve essere perseguita predisponendo un rigoroso quadro di misure di garanzia appropriate e specifiche, nel rispetto dei principi di proporzionalità del trattamento e di minimizzazione e pseudonimizzazione dei dati. Garanzie che, a livello interno, si rinvengono nelle «Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica» (adottate dal Garante con provv. 5 giugno 2019, n. 146, doc. web n.9124510), nonché nelle «Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica» (approvate dal Garante con provv., 19 dicembre 2018, n. 515, doc. web n. 9069637). La ricerca medica costituisce, peraltro, una *species* del *genus* della ricerca scientifica. Pertanto, se le norme di favore per la ricerca scientifica dettate dal Regolamento e sopra ricordate si applicano a tutte le ipotesi di ricerca scientifica, le previsioni dell'art. 110 del Codice trovano invece applicazione esclusivamente alle ipotesi di ricerca medica, declinata anche come ricerca biomedica (ossia ricerca di carattere interdisciplinare che recepisce in ambito medico nozioni e apporti provenienti dalla biologia e dalle scienze naturali) e come ricerca epidemiologica (che si occupa di studiare l'insorgenza, la distribuzione e la frequenza delle malattie nella popolazione con particolare riferimento ai fattori che le determinano), espressamente considerate da detta norma, mentre esula dal campo di applicazione di tale norma il trattamento dei dati relativi alla salute effettuato per finalità di cura o per finalità in senso lato sanitarie (per le quali occorre pur sempre il consenso dell'interessato: cfr. Garante privacy, provv. 7 marzo 2019, n. 55, «Chiarimenti nell'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario», *doc. web n.9091942*).

[22] Un recente esempio di ricerca epidemiologica prevista da una norma di legge è rappresentato dal D.L. 10 maggio 2020, n.30 (recante Misure urgenti in materia di studi epidemiologici e statistiche sul SARS-COV-2), che, nell'ambito dell'emergenza da Covid-19, ha espressamente autorizzato il trattamento dei dati personali, anche genetici e relativi alla salute, per fini statistici e di studi scientifici svolti nell'interesse pubblico nel settore della sanità pubblica, nell'ambito di un'indagine di sieroprева-

pato dalla redazione di una valutazione di impatto ai sensi degli artt. 35 e 36 GDPR[23]. La seconda deroga rileva ogniqualvolta, a causa di particolari ragioni, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, e il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale. Inoltre, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del codice *privacy*[24].

La recente modifica dell'art. 110 del Codice Privacy, apportata dal Decreto Pnrr, ha eliminato il requisito obbligatorio dell'autorizzazione preventiva da richiedere al Garante *Privacy* (in caso di impossibilità di

---

lenza condotta congiuntamente dai competenti uffici del Ministero della salute e dall'Istituto nazionale di statistica (ISTAT), in qualità di titolari del trattamento e ognuno per i profili di propria competenza (art. 1), secondo le modalità individuate dallo stesso articolo.

[23] Il che significa che il titolare del trattamento deve preliminarmente: a) valutare la necessità e la proporzionalità dei trattamenti in relazione alle finalità, nonché i rischi per i diritti degli interessati, indicando le misure previste per affrontarli, e b) all'esito di tale valutazione, consultare l'autorità di controllo qualora il trattamento presenti rischi elevati.

[24] Tale comma è stato così modificato dall'art. 44, comma 1-*bis*, D.L. 2 marzo 2024, n. 19, convertito, con modificazioni, dalla L. 29 aprile 2024, n. 56. Il Garante *privacy*, alla luce dell'innovazione legislativa, ha stabilito che in tutti questi casi i titolari del trattamento – oltre ad acquisire, come già previsto, il parere favorevole del competente Comitato etico a livello territoriale sul progetto di ricerca – dovranno motivare e documentare le ragioni etiche o organizzative in base alle quali non hanno potuto acquisire il consenso dei pazienti, nonché effettuare e pubblicare la valutazione di impatto, dandone comunicazione al medesimo Garante (provvedimento del 9 maggio 2024, *doc. web* n. 10016146). Con lo stesso provvedimento, il Garante, alla luce della riforma normativa e considerato il rilevante impatto delle nuove tecnologie nelle modalità di realizzazione dell'attività di ricerca, ha promosso l'avvio della procedura per l'adozione delle nuove regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, promuovendo una consultazione pubblica.

raccogliere il consenso degli interessati) per effettuare studi osservazionali retrospettivi in ambito medico, biomedico ed epidemiologico, ove vengano utilizzati dati sanitari già disponibili presso i centri di sperimentazione (ad es. nelle cartelle cliniche o nei referti) e per i quali sarebbe difficile coinvolgere gli interessati, affinchè manifestino uno specifico nuovo consenso (ad esempio perché defunti o irraggiungibili o non contattabili per specifici motivi etici od organizzativi) [25].

[25] La normativa del 2018 aveva comportato un impatto insostenibile sulla disciplina dei progetti di ricerca medica, biomedica ed epidemiologica nell'impossibilità di ottenere consensi dagli interessati (in particolare, per gli studi osservazionali retrospettivi), non potendo i ricercatori basarsi su autorizzazioni generali del Garante e dovendo anzi ricorrere a consultazioni-autorizzazioni *ad hoc*, ai sensi dell'articolo 36 del Regolamento. Tra il 2018 e il 2024, il Garante ha comunque espresso spesso parere favorevole alle richieste di consultazione preventiva sottoposte, confermando la correttezza del binomio alternativo consenso-consultazione come base giuridica, rispettivamente, per gli studi dove il consenso potesse essere raccolto (gli studi prospettici) e dove invece fosse impossibile farlo (gli studi retrospettivi). Si veda, in tal senso, l'autorizzazione concessa dal Garante all'Azienda Ospedaliera Universitaria Integrata di Verona relativamente allo studio dei pazienti affetti da patologie neoplastiche, infettive, degenerative e traumatiche del distretto toracico (database "torax") (Parere ai sensi dell'art. 110 del Codice e dell'art. 36 del Regolamento, 30 giugno 2022, *doc.web n. 9791886*). In tal caso, l'Autorità Garante aveva consentito di fondare la raccolta – e il successivo trattamento di dati sulla salute per scopi di ricerca medica – sul consenso «a fasi progressive», prevedendo un primo consenso espresso al momento della decisione di partecipare allo studio ed un consenso successivo (o, in caso di impossibilità, una consultazione del Garante) alla definizione dei progetti e protocolli successivi, approvati dai Comitati etici. In tale occasione, poiché nello studio erano coinvolti anche pazienti già deceduti o comunque non più contattabili, il Garante aveva confermato che «con riferimento ai pazienti non contattabili è la consultazione preventiva in esame, unitamente al parere favorevole del Comitato etico territorialmente competente, a costituire il presupposto giuridico equipollente al consenso, per la raccolta e la conservazione dei dati nel *database*». Ancora, si legga il provvedimento autorizzativo nei confronti dell'Azienda Ospedaliera Universitaria Careggi (Parere ai sensi dell'art. 110 del Codice e dell'art. 36 del Regolamento, 18 luglio 2023, *docweb n. 9920977*). Tra gli altri vedansi, poi, a titolo esemplificativo, i seguenti pareri positivi rilasciati dal Garante per la protezione dei dati personali: parere ai sensi dell'art. 110 del Codice e dell'art. 36 del Regolamento, 30 giugno 2022,

L'autorizzazione preventiva del Garante, ex art. 36 GDPR, è stata sostituita dal rispetto delle garanzie eventualmente indicate dal Garante nelle Regole deontologiche sul trattamento di dati per fini di ricerca o, in mancanza, in ossequio agli obblighi di natura *privacy* richiesti ai sensi del principio di *accountability*.

L'art. 110-*bis* del Codice in materia di protezione dei dati attribuisce, invece, al Garante la facoltà di autorizzare il trattamento ulteriore (quindi per scopo diverso da quello per il quale il dato era stato primariamente raccolto) di dati personali, compresi quelli ex art. 9 GDPR, a scopo di ricerca scientifica o statistica, da parte di soggetti terzi che svolgano principalmente tali attività se, a causa di particolari ragioni, informare gli interessati ai fini della manifestazione del consenso risulta impossibile o implica uno sforzo sproporzionato o, ancora, rischia di rendere irrealizzabile o pregiudicare gravemente il conseguimento delle finalità di ricerca»[26], sempre a condizione che siano

---

doc. web n. 9791886; provvedimento del 10 dicembre 2020, *doc. web* n.9520597; provvedimento del 29 ottobre 2020, *doc. web* n. 9517401; parere in ordine al trattamento dei dati personali, anche inerenti a particolari categorie di dati, per finalità di ricerca medica, biomedica e epidemiologica, riferiti alla coorte di pazienti arruolati nello studio «Matterhorn», 20 giugno 2019, *doc. web* n. 9123447. Nonostante l'efficiente attività autorizzativa del Garante, è indubbio che il legislatore italiano avesse di fatto complicato e limitato l'operatività di ricercatori e medici, richiedendo procedimenti gravosi (con i relativi tempi e burocrazie) per ricerche che, prima, potevano essere svolte sulla base delle autorizzazioni generali.

[26] Il trattamento deve essere posto in essere da un terzo, quindi da un soggetto diverso dal Titolare, che ha determinato il trattamento in precedenza. In tal senso, la nozione di terzo, non essendo specificata dall'articolo, né in generale dal Codice *privacy*, deve essere desunta dall'articolo 4 del GDPR, per cui è tale «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento (primario), il Responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare (primario) o del Responsabile». I soggetti terzi che svolgono «principalmente» attività di ricerca scientifica (Università, centri di ricerca, fondazioni, ecc., ma viene lasciato al Garante, il compito di definire il concetto di attività principale svolta nell'ambito della ricerca scientifica e statistica) potranno richiedere l'accesso ai dati raccolti e conservati da altro titolare del trattamento per utilizzarli ai fini di una ricerca, quan-

preventivamente adottate misure appropriate di salvaguardia, come forme preventive di minimizzazione e di anonimizzazione dei dati come indicate nel provvedimento autorizzatorio del Garante ovvero successivamente in caso di verifica, in cui sono stabilite le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del riutilizzo dei dati, anche sotto il profilo della loro sicurezza [27]. Al Garante è attribuita anche la possibilità di emana-

---

do, a causa di particolari ragioni, riuscire ad informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di ricerca (analogamente, vedi anche S. Melchionna, *Commento all'art. 110-bis*, in R. Sciaudone, *Commentario al codice della privacy,* Pisa, Pacini, 2023, 340 ss.)

[27] Con l'autorizzazione del Garante privacy in tema di ricerca scientifica, n. 9/2016 del 15 dicembre 2016, «Autorizzazione generale al trattamento dei dati personali effettuato per scopi di ricerca scientifica», rimasta in vigore fino al 15 maggio 2018 e poi trasfusa, ai sensi dell'art.21, D.lgs. 101/2018, nelle già citate «Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica» del 5 giugno 2019, sono state autorizzate in via generale le Università, gli altri enti o istituti di ricerca e società scientifiche, nonché i ricercatori e gli esercenti le professioni sanitarie (nei limiti del codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici) al trattamento dei dati idonei a rivelare lo stato di salute, anche in assenza del consenso degli interessati, per scopi di ricerca scientifica in campo medico, biomedico o epidemiologico, a condizione che: i) il trattamento sia necessario per la conduzione di studi non aventi significativa ricaduta personalizzata sull'interessato; ii) la ricerca sia effettuata sulla base di un progetto oggetto di motivato parere favorevole del competente comitato etico territoriale; iii) i dati siano trattati in forma anonima o comunque riducendo al minimo l'utilizzazione di dati identificativi; iv) i dati siano strettamente pertinenti ai sopra indicati scopi di ricerca (fermo restando che i dati genetici sono oggetto di diversa disciplina); v) sia impossibile informare gli interessati per motivi etici (ossia riconducibili alla circostanza che l'interessato ignora la propria condizione e la sua conoscenza potrebbe arrecargli un danno materiale o psicologico) o per motivi organizzativi (riconducibili al numero di interessati coinvolti nella ricerca); vi) i dati siano trattati nel rispetto del codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici nonché con modalità tali da rendere non identificabili gli interessati mediante tecniche di cifratura. In tal modo, la disciplina dei dati relativi alla salute da utilizzarsi a fini di ricerca scientifica ha trovato

re provvedimenti generali rivolti a determinate categorie di titolari e di trattamenti [28].

Resta escluso dalla nozione di riutilizzo e, pertanto, dall'applicazione dell'art. 110-*bis*, il trattamento dei dati raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca (ma i soggetti menzionati, a rigore, sarebbero nient'altro che titolari del trattamento, e non terzi) [29]. Il motivo di tale eccezione risiede nel fatto che tali enti perseguono finalità di ricerca, prevalentemente clinica e traslazionale, nel campo biomedico e in quello dell'organizzazione e gestione dei servizi sanitari ed effettuano prestazioni di ricovero e cura di alta specialità (art.1 d.lgs. 16/10/2003, n. 288), avendo la missione istituzionale di effettuare ricerca nell'interesse della collettività con una diretta ricaduta sull'assistenza del malato, sull'organizzazione e sulla gestione dei servizi sanitari, effettuando prestazioni di ricovero e cura di alta specializzazione.

Assume, infine, un significativo rilievo nella materia *de qua* anche l'intervento effettuato dal D.L. n. 139/2021, in base al quale i dati relativi alla salute, privati di elementi identificativi diretti, possono essere trattati dal Ministero della salute, dall'Istituto superiore di sanità (ISS), dall'Agenzia nazionale per i servizi sanitari regionali (Agenas), dall'Agenzia italiana del farmaco (AIFA), dall'Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle

---

concreta implementazione, venendo indicati nel dettaglio limiti e modalità di trattamento volti a tutelare l'interessato anche in assenza del suo consenso.

[28] La scelta di rimettere la possibilità di riutilizzare dati sanitari all'autorizzazione espressa del Garante diviene però un ulteriore requisito, non previsto a livello europeo, e come tale suscettibile di essere considerato incompatibile con la normativa comunitaria.

[29] Tale previsione, secondo S. MELCHIONNA, *Commento all'art.* 110-*bis*, in R. SCIAUDONE, *Commentario al codice privacy*, Pisa, Pacini, 2023, 340 ss., appare in realtà tautologica, alla luce del fatto che l'articolo in commento presuppone un trattamento ulteriore da parte di terzi e non dello stesso titolare che li ha raccolti (cfr. Garante, Parere del 22 maggio 2018, cit.).

malattie e della povertà (Inmp) e dalle Regioni (relativamente ai propri assistiti), anche mediante l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Servizio sanitario nazionale, ivi incluso il Fascicolo Sanitario Elettronico (FSE). La norma mira evidentemente a superare gli ostacoli legislativi relativi alla comunicazione a terzi dei dati presenti nelle banche dati dei predetti enti e soprattutto alla condivisione delle informazioni presenti nei sistemi informativi del Ministero della salute. I limiti normativi espressamente previsti per tale interoperabilità sono stati individuati nel rispetto delle finalità istituzionali di ciascuno degli enti indicati e nella previsione secondo cui i predetti sistemi informativi perseguano finalità compatibili con quelle sottese al trattamento. Il medesimo D.L. n. 139/2021 ha poi apportato modifiche pure all'art. 7, D.L. n. 34/2020, prevedendo che il Ministero della salute, nell'ambito dei propri compiti istituzionali, possa trattare, ai sensi dell'art. 2-*sexies,* c.2, lett. v), Codice Privacy e nel rispetto del GDPR, i dati relativi alla salute degli assistiti, raccolti nei sistemi informativi del Servizio sanitario nazionale, per lo sviluppo di metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione, secondo le modalità previste nel richiamato decreto interconnessioni. Lo scopo di tale attività è quello di utilizzare le attuali basi informative per individuare gruppi di assistiti, aventi lo stesso rischio di morbilità, su cui programmare gli interventi sanitari e, quindi, prevedere il relativo impatto in termini di spesa sanitaria. In questo quadro, è indubbia la necessità di fornire senza ritardo agli interessati le informative ex artt. 13 e 14 GDPR, nonché di avvisarli al variare di elementi essenziali e significativi del trattamento, fra cui rientrano le modificazioni soggettive riguardanti il titolare. Su tale solco, si innesta l'esigenza di valorizzare le modalità attuative dei diritti dell'interessato, particolarmente la revoca del consenso (ove questo sia stato la base giuridica iniziale) ed il diritto di opposizione, al fine di evitare che l'interessato rimanga di fatto soggiogato da un trattamento che, quali che siano le ragioni, non condivide più.

Da ultimo, va menzionata la legge italiana sull'intelligenza artificiale n. 132/2025, che all'art. 8, stabilisce che, fermo restando l'obbligo di informativa in favore dell'interessato, senza ulteriore consenso dell'in-

teressato ove inizialmente previsto dalla legge, è sempre autorizzato l'uso secondario di dati pseudonimizzati anche sanitari, salvi i casi nei quali la conoscenza dell'identità degli interessati sia inevitabile o necessaria al fine della tutela della loro salute; ciò nel caso in cui l'uso secondario sia operato da soggetti pubblici e privati senza scopo di lucro, dagli Istituti di ricovero e cura a carattere scientifico (IRCCS), di cui al decreto legislativo 16 ottobre 2003, n.288, nonché da soggetti privati operanti nel settore sanitario nell'ambito di progetti di ricerca a cui partecipano soggetti pubblici e privati senza scopo di lucro o IRCCS. Tale uso secondario è consentito per la ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale per finalità di prevenzione, diagnosi e cura di malattie, sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicali, incluse protesi e interfacce fra il corpo e strumenti di sostegno alle condizioni del paziente, salute pubblica, incolumità della persona, salute e sicurezza sanitaria, nonché studio della fisiologia, della biomeccanica e della biologia umana anche in ambito non sanitario, in quanto necessari ai fini della realizzazione e dell'utilizzazione di banche di dati e modelli di base.

Capitolo III

NUOVI MODELLI DI INTERMEDIAZIONE PROPOSTI DAL DATA GOVERNANCE ACT PER UNA TUTELA SOSTANZIALE DEI DIRITTI DELL'INTERESSATO

Sommario: 1. Gli obiettivi e gli strumenti inseriti nel *Data governance act* per il reimpiego dei dati e il perseguimento di finalità sociali. – 2. L'ingresso della cooperativa di dati nel nostro sistema giuridico. – 3. L'incerta disciplina afferente le cooperative di dati dettata dal *Data Governance Act* – 4. L'esperienza delle cooperative di dati sanitari d'oltralpe e l'ipotetica sussunzione di tali modelli nel nostro sistema giuridico. – 5 L'ambito di applicazione soggettivo della disciplina concernente gli intermediari dei dati nel *Data governance act* e la sottile linea di confine tra concetto di «*no profit*» e «altruismo dei dati». I contratti di servizi tra soci e società cooperativa di dati sanitari e il relativo vantaggio mutualistico.

1. *Gli obiettivi e gli strumenti inseriti nel Data governance act per il reimpiego dei dati e il perseguimento di finalità sociali*

All'incerto contesto normativo descritto nei precedenti paragrafi, si è aggiunta di recente un'altra fondamentale regolamentazione di derivazione europea, spinta dall'esigenza di condividere, per fini di prevenzione e ricerca, una quantità maggiore di dati sanitari (oltreché di dati relativi ad altri settori strategici dell'economia quali la mobilità, l'industria manifatturiera, i servizi finanziari, l'energia, l'agricoltura e l'ambiente). Si tratta del cosiddetto *Data Governance Act*[1].

[1] Ci si riferisce al Reg. UE 2022/868, pubblicato il 3 giugno 2022 ed entrato in

Il DGA (così lo indicheremo per brevità), nella consapevolezza del valore economico dei dati, si propone di dare impulso alla costituzione di uno spazio unico europeo dei dati, attraverso la condivisione, cui possano accedere, a parità di condizioni, tutti gli operatori economici, comprese le piccole imprese, scardinando in tal modo l'oligopolio di quelle di maggiori dimensioni. Tale Regolamento intende favorire pure la destinazione altruistica dei dati, assecondando un'esigenza sociale emersa prepotentemente con l'esperienza pandemica, che ha posto in luce la necessità del reimpiego dei dati nell'interesse generale, per la promozione, ad esempio, della ricerca scientifica ed il supporto alle politiche sanitarie, nell'acquisita consapevolezza della funzione sociale che la protezione dei dati è chiamata a realizzare (Considerando 4, GDPR). Più in generale, il riutilizzo dei dati protetti detenuti da enti pubblici ed i servizi di intermediazione dei dati, punti focali di tale nuova normativa, sono immaginati dal legislatore europeo anche al servizio del perseguimento di finalità sociali, attraverso la previsione di norme di favore. Dunque, pure il DGA, come il GDPR, è figlio della dialettica tra tutela della persona e libera circolazione dei dati [2].

---

vigore in data 24 settembre 2023. Cfr., in argomento, per tutti, F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 199 ss. Si intende, con tale atto normativo, superare l'attuale sistema incentrato, essenzialmente, sul controllo dei dati (personali), anziché sulla loro condivisione, attraverso lo strumento del consenso informato, rivelatosi nella pratica fallimentare, considerato che il medesimo si traduce, il più delle volte, in una foglia di fico «atta a mascherare una realtà fortemente asimmetrica e in cui l'idea dell'autodeterminazione dell'interessato si è rivelata poco più che un'etichetta priva di riscontri operazionali» (Cfr. G. RESTA, *La regolazione digitale nell'Unione Europea - Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, 2022, 971 ss., il quale parla di «burocratizzazione del consenso sia nei rapporti con i soggetti privati, sia in quelli con i soggetti pubblici»; vedi anche S. RODOTÀ, *Elaboratori elettronici e controllo sociale,* Bologna, Il Mulino, 1973, 47 ss., nonché 133 ss.).

[2] È emersa dunque, grazie anche alle riflessioni dei civilisti (Cfr. S. RODOTÀ, *Conclusioni,* in. V. CUFFARO, V. RICCIUTO, V. ZENO ZENCOVICH *Trattamento dei dati* e *tutela della persona,* Milano, Giuffrè, 1998, 308 e RICCIUTO (a cura di), *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali,* in *Rivista di diritto civile,*

Benché la parola d'ordine sia diventata "*data sharing",* ad indicare l'esigenza di riutilizzo delle informazioni e della loro condivisione, in vista della creazione di un mercato unico europeo, basato sullo scambio massivo dei dati, personali e di altra natura, le ragioni dell'economia non sbiadiscono la tutela della persona. Va, infatti, chiarito che le diverse forme di uso di dati regolate dal DGA contemplano in via preferenziale dati non personali e/o anonimizzati e/o, conformemente al principio della *privacy by design,* pseudonimizzati. Inoltre, il legislatore europeo ha chiaramente stabilito la prevalenza del GDPR sul DGA, in caso di conflitto, e ribadito la centralità del rispetto dei diritti fondamentali.

Il risultato che si intende conseguire è di creare fiducia tra gli interessati, considerati come soggetti da tutelare, e le imprese, per quanto riguarda l'accesso ai dati, la loro condivisione e il loro controllo, l'utilizzo e il riutilizzo [3].

Il *Data Governance Act* non dà indicazioni diverse dal GDPR in riferimento alle basi giuridiche per il riutilizzo dei dati (art. 3 cpv. 3 DGA) [4], ma, dal punto di vista definitorio, si individuano rilevanti di-

---

2020, 642 ss.; Id., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno,* in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo,* Torino, Giappichelli, 2019, 23 e ss., e alla giurisprudenza dell'Autorità antitrust (AGCM) e amministrativa, la dimensione economico/negoziale alla base del fenomeno del trattamento dei dati personali, che, oltre che espressione della persona, costituiscono utilità economiche, suscettibili di essere "scambiate."

[3] Per «riutilizzo», ai sensi dell'art. 2 di tale regolamento, si intende: l'utilizzo di dati in possesso di enti pubblici da parte di persone fisiche o giuridiche a fini commerciali o non commerciali diversi dallo scopo iniziale, nell'ambito dei compiti di servizio pubblico per i quali i dati sono stati prodotti, fatta eccezione per lo scambio di dati tra enti pubblici esclusivamente in adempimento dei loro compiti di servizio pubblico.

[4] Con precipuo riferimento al riutilizzo dei dati, infatti, il considerando 7, anche alla luce delle osservazioni formulate dall'EDPB e dal GEPD nel Parere congiunto n. 3/2021 riguardo alla proposta di Regolamento, in maniera inequivoca afferma che «il trattamento dei dati personali dovrebbe in generale essere basato su una o più delle basi giuridiche per il trattamento dei dati personali previste agli articoli 6 e 9 del regolamento (UE) 2016/679» (Cfr. "*Joint Opinion 3/2021 on the Proposal*

screpanze rispetto alla normativa di cui al GDPR, che segnalano la diversa prospettiva e, in parte, i diversi obiettivi ricercati da questa ultimo atto normativo. Il «titolare dei dati» (*data holder*), per tale Regolamento, è, infatti, «una persona giuridica, compresi gli enti pubblici e le organizzazioni internazionali, o una persona fisica che non è l'interessato rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli» (art. 2, par. 1, n. 8, DGA) [5]. L'«utente dei dati» (*data user*), invece, è «una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che ha diritto, anche a norma del regolamento (UE) 2016/679, in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali» (art. 2, par. 1, n. 9, *Data Governance act*) [6]. Certamente, il titolare dei dati appartiene ad una

for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)", disponibile in *https://edpb.europa.eu/system/files/2021-09/edpb-edps_joint_opinion_dgaitO.pdf*

[5] Il GDPR, invece, fa riferimento al «titolare del trattamento» come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali» (art. 4, par. 1, n. 7). Secondo A. MORACE PINELLI, *Dalla Data Protection alla Data Governance: il regolamento (UE) 2022/868. Commentario al Data Governance Act*, Pisa, Pacini, 2024, 1 ss., come già sottolineato dal Comitato e dal Garante europeo nel loro parere congiunto del 2021 (Parere congiunto EDPB-GEPD n. 03/2021 sulla proposta di Regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati, v.1.1.), sarebbe stato appropriato disciplinare se e a quali condizioni un determinato trattamento di dati personali possa essere effettuato o meno, chiarendo il ruolo del titolare dei dati alla luce della normativa vigente in materia di protezione dei dati personali.

[6] Fa notare come il mutamento del lessico di tale Regolamento sia indice di un cambio di paradigma nell'approccio del legislatore, perché tende ad oggettivare i dati personali in funzione del loro impiego economico, con il serio rischio di una progressiva perdita di tutela per gli attributi della persona e, con essa, per i diritti della personalità, F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act* in *Contratto e impresa/Europa*, 2021, 199 ss. In argomento, vedi pure D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, 46 ss.

categoria diversa rispetto al titolare del trattamento di cui al GDPR, sia per la tipologia di dati (personali e non personali) con cui è posto in relazione, sia per l'oggetto stesso su cui si focalizza la nozione, costituito dal diritto di concedere l'accesso ai dati a terzi o di condividere i dati con questi ultimi. Diversamente, il titolare del trattamento definito dal GDPR è il soggetto che, in relazione ai soli dati personali, definisce finalità e mezzi del trattamento, quest'ultimo comprendente qualsiasi operazione su dati personali e non riguardante solo l'accesso di terzi o la loro comunicazione, come avviene nel DGA.

A rientrare nell'ambito di applicazione oggettivo di tale Regolamento, in particolare, sono le categorie di dati detenuti da enti pubblici e tutelati per ragioni anche di protezione dei dati personali [7]. Pertanto, i dati che saranno gestiti nell'ambito dell'Ecosistema dei Dati Sanitari, come quelli attualmente presenti nel Fascicolo sanitario elettronico, possono rientrare nella sfera di applicazione di questa normativa.

Il *Data Governance Act* non introduce però un obbligo generalizzato di riutilizzo dei dati [8]. Ogni soggetto pubblico è libero di decidere se consentire o negare l'accesso per il riutilizzo [9]. Il modello del riutilizzo

---

[7] Oltre che per fini di riservatezza commerciale, riservatezza statistica, protezione dei diritti di proprietà intellettuale di terzi.

[8] II DGA estende quindi la disponibilità dei dati detenuti dagli enti pubblici anche a quelli che sono oggetto di diritti in capo a terzi, ossia ai dati protetti per motivi di *privacy*, riservatezza commerciale o diritti di proprietà intellettuale di terzi, ampliando in sostanza, secondo la dottrina (Cfr. sempre F. Bravo, Il *principio di solidarietà tra data protection e data governance,* in *Diritto dell'informazione e dell'informatica*, 2023, 481 ss.), la nozione di «dato pubblico» ossia di «dato conoscibile da chiunque» di cui all'art. 2, comma 1, lett. d), d.lgs. n. 36/2006. In questa ottica, il DGA disciplina, quindi, in maniera peraltro anche piuttosto dettagliata, se si considera la complessiva impostazione di normativa generale e di principio, il riutilizzo di detti dati, circondandolo di una serie di regole e cautele e facendo gravare sulle Amministrazioni, che detengono i dati e ne consentono il riuso, compiti e responsabilità legate alla correttezza ed alla sicurezza di tale riutilizzo.

[9] Gli enti pubblici devono essere in grado di predisporre tecniche per l'anonimizzazione dei dati o, qualora la fornitura di dati anonimizzati o modificati non rispondesse alle esigenze del riutilizzatore, altre tecniche per proteggere i diritti degli

risponde alla *ratio* secondo cui i dati generati o raccolti da enti pubblici o altre entità a carico dei bilanci pubblici debbano apportare benefici alla società, sviluppando così la linea politica dell'Unione sugli *Open Data «*Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019», relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

Il riutilizzo dei dati personali, però, ai sensi dell'art.5, comma 3, DGA è possibile solo qualora l'ente pubblico che concede l'accesso garantisca, tra le altre cose, che i dati siano stati previamente anonimizzati, ossia privati della loro natura di informazione riguardante una persona fisica identificata o identificabile. In generale, come chiarito dal considerando 15: «Le condizioni cui è subordinato il riutilizzo dei dati dovrebbero essere concepite in modo da assicurare garanzie efficaci per quanto concerne la protezione dei dati personali». Gli enti pubblici che, a norma del diritto nazionale, hanno facoltà di concedere o negare l'accesso per il riutilizzo di una o più delle categorie di dati devono rendere pubbliche tali condizioni per consentire il riutilizzo dei dati, nonché la procedura di richiesta del riutilizzo attraverso lo sportello unico [10].

---

interessati (ad esempio, *privacy* differenziale, generalizzazione, soppressione e casualizzazione, utilizzo di dati sintetici o metodi analoghi, nonché altri metodi all'avanguardia di tutela della vita privata (cfr. Considerando n.7). La condizione tecnico-giuridica per la trasmissione di dati non anonimizzati è costituita da una valutazione d'impatto in materia di protezione dei dati e la consultazione dell'autorità di controllo, ai sensi degli articoli 35 e 36 del GDPR. In tal caso, occorre altresì fornire un ambiente di trattamento sicuro fornito o controllato dall'ente pubblico. Si tratta quindi di un'attività procedimentalizzata, tale da comportare un apparato tecnico in capo alle pubbliche amministrazioni e le necessarie garanzie dovute alle interlocuzioni con le autorità di garanzia.

[10] Sul sito della Commissione europea sono riportati i seguenti esempi: la *Finnish social and health data permit authority Findata (https://findata.fi/en/),* che elabora le richieste e concede l'accesso ai dati per il loro riutilizzo (esempi di fonti di dati a disposizione di Findata sono: l'istituto di previdenza sociale, il registro delle pensioni e il registro della popolazione); la società francese DAMAE Medical *(https://damae-medical.com),* che consente l'accesso a immagini a risoluzione cellulare delle microstrutture interne della pelle fino al derma, in modo immediato e non invasivo, con nuovi

Nel Regolamento viene inoltre cristallizzato un modello già registrato nella prassi, basato sul ruolo dell'intermediario di dati che, nel fornire il servizio di *data sharing*, agisce come una sorta di *broker* "*sui generis*" tra «titolare dei dati» e «utente dei dati»[11].

Secondo la definizione proposta nell'art. 2, n. 11, DGA, si intende per servizio di intermediazione dei dati un «servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeter-

---

dati di formazione resi disponibili attraverso il *French Health Data Hub*. (https://www.health-data-hub.fr/). L'obiettivo di quest'ultimo progetto è quello di migliorare la capacità di identificare i potenziali segni di cancro della pelle e di delimitare meglio l'area di intervento chirurgico. (Fonte URL:*https://digital-strategy.ec.europa.eu/policies/data-governance-act-explained)*.

[11] I servizi di intermediazione previsti dal DGA risultano già ampiamente affermati nella prassi negoziale e hanno assunto svariate nomenclature. Si pensi ai *Personal information management systems* (PIMS), che mirano a dare agli interessati un maggiore controllo sui loro dati personali; ai *Data exchanges*, che operano come piattaforme di dati *online* in cui è possibile pubblicizzare e accedere agli insiemi di dati, a scopo commerciale o *no-profit*; le *Industrial data platforms*, che forniscono un'infrastruttura condivisa per facilitare la condivisione sicura di dati e analisi tra aziende (per una completa panoramica, vedi A F. Ferraris, *European data strategy e intermediario di dati: nuove prospettive per il mercato della condivisione*, in *Il Quotidiano Giuridico*, 2022). Si pensi ai *Data trusts*, che usualmente forniscono una gestione fiduciaria dei dati per conto degli interessati, spesso per finalità non lucrative, ma di ricerca scientifica o sanitaria. Sebbene possano offrire servizi equivalenti a quelli dei PIMS (Personal Information Management Systems), ci si può chiedere se tali *trust* di dati rientrino nell'ambito di applicazione dell'articolo 2, paragrafo 11 DGA, dato che, a differenza dei PIMS, i fiduciari dei dati non consentono agli interessati di esercitare direttamente i loro diritti, ma raggiungono obiettivi equivalenti agendo per loro conto. Poiché, appunto, *i trust* di dati offrono servizi fiduciari di gestione dei dati per conto dei loro utenti, ci si può chiedere pure se stabiliscano relazioni commerciali tra i titolari/soggetti dei dati e gli utenti dei dati nel senso previsto dal DGA. Cfr., in argomento, S. Delacroix, N. Lawrence, *Bottom-up data trusts: disturbing the 'one size fits all' approach to data governance. International Data Privacy Law*, 2019; 236–52; R. Milne, A. Sorbie, M. Dixon-Woods, *What can data trusts for health research learn from participatory governance in biobanks?* In *Journal of Medical Ethics*, 2022; 48:323–8; N. Lawrence, J. Montgomery, S. Oh, *Enabling data sharing for social benefit through data trusts at the Global Partnership on AI, GPAI*, in *OECD AI Policy Observatory*, 2021,18.

minato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali». L'art. 10, comma 1, contempla tre tipologie di servizi di intermediazione tra loro molto diversi. La prima è relativa a servizi di intermediazione tra «titolari dei dati» e «potenziali utenti» di essi, i quali «possono includere scambi di dati bilaterali o multilaterali o la creazione di piattaforme o banche dati che consentono lo scambio o l'utilizzo congiunto dei dati». La seconda tipologia è quella consistente nei servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, permettendo in particolare l'esercizio dei diritti degli interessati di cui al regolamento (Ue) 2016/679. La terza tipologia è costituita dai servizi di cooperative dei dati, di cui si tratterà diffusamente nel prossimo paragrafo.

Le nuove norme intendono rimediare alla constatata debolezza dell'interessato nell'esercizio del suo diritto al controllo, che necessita di essere supportato (o anche sostituito in questa attività) da soggetti che perseguono finalità non egoistiche. Si presume, infatti, che gli intermediari aumentino la fiducia nella condivisione dei dati ed eliminino le asimmetrie esistenti di potere e di informazione, interponendosi in modo neutrale tra i titolari dei dati e gli utenti [12]. Emerge, di fronte

[12] Tali intermediari potranno aiutare l'interessato nella gestione dei diritti riconosciuti dal GDPR, dal diritto di accesso, alla rettifica, alla cancellazione, alla limitazione del trattamento e alla portabilità dei dati. Per un'analisi delle questioni giuridiche concernenti tale tipo di intermediazione, cfr. F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act* in *Contratto e impresa/Europa*, 2021, 199 ss.; F. BRAVO, *Il commercio elettronico dei dati personali*, in T. PASQUINO, A. RIZZO, M. TESCARO (a cura di), *Questioni attuali in tema di commercio elettronico*, Napoli, ESI, 2020, 83-130. Vengono però imposti obblighi rigorosi agli intermediari che si occupano di facilitare la condivisione e lo scambio dei dati. Innanzitutto, vige il principio di neutralità, che trova la sua applicazione nell'esclusività dello scopo per cui il trattamento viene posto in essere. Il fornitore, intermediario dei dati, non può quindi

al *data subject,* la prospettiva dell'esercizio delegabile dei diritti e la configurazione di un rapporto gestorio e fiduciario tra intermediari e interessati, che si ponga al centro di nuovi rapporti contrattuali, che fuoriescono dall'originaria relazione dell'interessato con il titolare del trattamento. Si può ipotizzare un doppio livello di supporto all'interessato. Il grado più "*soft*" è rappresentato dall'attività di consulenza e di assistenza; il grado più elevato spinge fino alle soglie della rappresentanza sostitutiva, con gli intermediari che trattano e negoziano termini e condizioni per conto dei propri membri. Ma il reticolo normativo del GDPR e del DGA limita e confina tale ultima prospettiva, nel considerando n. 31, secondo cui: «in tale contesto è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi» [13].

---

utilizzare i dati oggetto del servizio di condivisione – siano essi dati personali o non personali – per scopi diversi dalla loro messa a disposizione agli «utenti dei dati». Cfr. Considerando 33 del *Data governance act*, che aggiunge che i fornitori di servizi di intermediazione dei dati dovrebbero essere in grado di mettere a disposizione dei titolari dei dati, degli interessati o degli utenti dei dati strumenti propri o di terzi, al fine di agevolare lo scambio di dati, ad esempio strumenti per la conversione o la cura di dati, solamente su richiesta esplicita o con l'esplicita approvazione dell'interessato o del titolare dei dati. I fornitori di servizi di intermediazione dei dati che agiscano da intermediari tra i singoli individui, quali gli interessati, e le persone giuridiche, quali gli utenti dei dati, dovrebbero inoltre avere l'obbligo fiduciario nei confronti dei singoli individui di garantire che agiscono nel migliore interesse degli interessati. Nell'intento di rafforzare ulteriormente la trasparenza e l'affidabilità del servizio, il fornitore di servizi di intermediazione dei dati che offre servizi agli interessati, agisce nell'interesse superiore di questi ultimi nel facilitare l'esercizio dei loro diritti, in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera concisa, trasparente, intelligibile e facilmente accessibile sugli utilizzi previsti dei dati da parte degli utenti dei dati e sui termini e le condizioni *standard* cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso.

[13] Il ruolo degli intermediari andrà vagliato in concreto. Se i servizi di intermediazione sono stati concepiti per dare impulso alla *data driven economy*, favorendo il rilascio dei dati attraverso una più pregnante garanzia dei diritti degli interessati al trattamento, di cui non è seriamente consentita la tutela individuale, «essi potrebbero invece finire per esaltare la redditività dei dati personali, incoraggiandone l'utilizzo

L'ultimo modello innovativo definito dal legislatore europeo del *Data governance act* è relativo all'«altruismo dei dati», inteso dall'art. 2 come «la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale» [14].

---

per fini commerciali» (Cfr. D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 46 ss. Cfr. pure I. SPEZIALE, *L'ingresso dei dati personali nella prospettiva causale dello scambio: i modelli contrattuali di circolazione*, in *Contratto e impresa*, 2021, 602 ss., la quale segnala il rischio che «dietro la promessa di maggiori tutele, oltre che di guadagni per l'utente... si celi una mercificazione pressoché totale e definitiva della persona e delle sue informazioni», concependo l'individuo «(solo) come il proprietario di una ricchezza da commercializzare»).

[14] Il *Data Governance Act* detta i requisiti che devono essere posseduti dalle organizzazioni dedicate all'altruismo dei dati, che dovranno operare mediante una struttura giuridicamente indipendente, separatamente dalle altre attività che l'ente abbia intrapreso. Viene istituita la possibilità per le organizzazioni che praticano l'altruismo dei dati di registrarsi in qualità di «organizzazioni per l'altruismo dei dati riconosciute nell'UE», purché soddisfino una serie di requisiti, al fine di accrescere la fiducia nelle loro attività. Tali organizzazioni saranno soggette ad una serie di obblighi di trasparenza. Sarà inoltre sviluppato un modulo europeo comune di consenso all'altruismo dei dati per ridurre i costi della raccolta dei consensi e facilitare la portabilità dei dati. L'art. 15 sottrae alla disciplina procedurale e sostanziale dei servizi di intermediazione le «organizzazioni per l'altruismo dei dati riconosciute», nonché le «altre entità senza scopo di lucro nella misura in cui le loro attività consistano nel cercare di raccogliere, per obiettivi di interesse generale, dati messi a disposizione da persone fisiche o giuridiche sulla base dell'altruismo dei dati». L'intento è quello di ritagliare un complesso di regole di favore per enti collettivi che, operando senza scopi di lucro, si propongano di stimolare la raccolta di dati personali e non perso-

Lo schema negoziale in questo caso prevede che l'oggetto delle prestazioni (i dati) sia fornito su base volontaria (tramite il consenso, da parte degli interessati, o l'autorizzazione per i dati non personali), laddove l'onerosità (e l'eventuale corrispettività) è esclusa, ma l'eventuale compenso rappresenti formalmente un rimborso per le spese di messa a disposizione dei dati.

Passando in rassegna la disciplina del DGA, ci si imbatte in una molteplicità dei rapporti disegnati dal legislatore europeo, che vanno dalla messa in servizio e gestione di infrastrutture e piattaforme (anche per *data spaces* comuni), ai servizi di elaborazione di dati, alla conservazione temporanea e custodia di dati, all'esercizio su delega di diritti, alla consulenza, a varie attività di controllo sull'operato di terzi (presenti anche nelle attività di riuso e dovute in caso di processazione di dati in ambienti sicuri). Tali rapporti sono riconducibili a specifici tipi contrattuali, suscettibili di convergere in contratti a causa complessa o collegati, quali contratti di somministrazione, appalti di servizi, contratti di mandato od opera professionale, contratti di deposito. E di tali tipologie contrattuali occorrerà valutare la relativa disciplina, a cavallo tra le normative di derivazione comunitaria e quelle interne agli stati membri, e controllata la meritevolezza degli interessi sottesi a tali operazioni.

---

nali e la loro destinazione a finalità di interesse generale. Si consideri che l'altruismo dei dati è stato finora discusso nella letteratura di lingua tedesca con il termine di donazione di dati (Cfr. R. Schildbach, *Access to public data and data altruism under the draft Data Governance Act*, in ZD 2022, 148 ss.; von Hagen P., Völzmann L., *Datenaltruismus aus datenschutzrechtlicher Perspektive*, in MMR 2022, 176 (176); A. Hartl, A. Ludin, *Recht der Datenzugänge*, in MMR, 2021, 534 ss.) L'esempio pratico più importante di donazione di dati è probabilmente l'app *Corona Data Donation* del *Robert Koch Institute*, che ha come obiettivo quello di comprendere meglio la diffusione del COVID-19, attraverso i dati creati dai cosiddetti dispositivi indossabili (braccialetti *fitness*, *smartwatch*, smartphone, ecc.). (In argomento vedi K. Schreiber, P. Pommerening, P. Schoel, *Das neue Recht der Daten-Governance*, 2023 § 4, Rn. 3.) L'idea, sia alla base dell'altruismo dei dati che della donazione dei dati, è quella di promuovere la messa a disposizione volontaria e gratuita dei dati a beneficio del pubblico in generale.

2. *L'ingresso della cooperativa di dati nel nostro sistema giuridico.*

Tra le tipologie di intermediari descritti dal *Data Governance Act*, come anticipato, spicca la figura nuova, almeno per la nostra esperienza giuridica, della cooperativa di dati, che, in prima approssimazione, può definirsi come uno strumento atto a rafforzare l'influenza effettiva di un gruppo di persone sui propri dati personali nei confronti di terzi e, allo stesso tempo, ad assoggettare tale risorsa a regole comuni di utilizzo, in vista di un obiettivo collettivo [15].

La società cooperativa, come noto, è un modello d'impresa nato in funzione della realizzazione dei bisogni dei suoi promotori e partecipanti e del miglioramento delle loro condizioni sociali ed economiche. [16] Le dinamiche mutualistiche tipiche del modello cooperativo mirano, infatti, a consentire a categorie svantaggiate di soggetti – quali consumatori, utenti, lavoratori, risparmiatori - di accedere a beni, servizi od occasioni di lavoro a condizioni più convenienti rispetto a quelle offerte dal mercato. La cooperazione, quindi, si è storicamente

---

[15] Il numero di cooperative di dati istituite a livello europeo è stato finora esiguo. Resta quindi da vedere se e in che misura le cooperative di dati si svilupperanno sul mercato. Cfr. in tal senso, pure A. PASCHKE, D. RÜCKER, *Data governance act, Kommentar*, München, C.H. Beck, 2024, sub art. 10, 180.

[16] Si tratta di un modello le cui origini vengono tradizionalmente rinvenute nell'Inghilterra della metà del diciannovesimo secolo dello scorso millennio e ricondotte all'iniziativa dei cosiddetti «probi pionieri di Rochdale», che costituirono la *Rochdale Pioneers Equitable Society*. Sulle origini e sull'evoluzione della disciplina delle società cooperative, si vedano, tra i tanti contributi, G. BONFANTE, *La legislazione cooperativa. Evoluzione e problemi*, Milano, Giuffrè, 1984, 9 ss.; A. BASSI, *Delle imprese cooperative e delle mutue assicuratrici (artt. 2511-2548)*, in *Il codice civile comm.*, diretto da Schlesinger, Milano, Giuffrè, 1988, 1 ss.; V. BUONOCORE, *Diritto della cooperazione*, Bologna, Il Mulino, 1997, 35 ss.. Sulla storia del movimento cooperativo in Italia, cfr. M. FORNASARI, V. ZAMAGNI, *Il movimento cooperativo in Italia. Un profilo storico-economico (1854-1992)*, Firenze, Vallecchi, 1997; R. ZANGHERI, G. GALASSO, V. CASTRONOVO, *Storia del movimento cooperativo in Italia. La Lega Nazionale delle Cooperative e Mutue (1886-1986)*, Torino, Einaudi, 1987; S. ZAMAGNI, V. ZAMAGNI, *La cooperazione*, Bologna, Il Mulino, 2008.

proposta e affermata come una forma organizzativa dell'attività d'impresa capace di dare impulso, attraverso metodologie produttive incentrate sulla gestione di servizio ai soci, e non ispirate da logiche speculative, all'elevazione economica e sociale delle categorie interessate; promuove e favorisce, inoltre, processi di crescita complessiva delle collettività destinatarie della sua azione. Proprio tale attitudine dell'impresa cooperativa ha condotto al riconoscimento, nell'art. 45 della Costituzione italiana, della «funzione sociale della cooperazione a carattere di mutualità e senza fini di speculazione privata» [17]. Storicamente, le cooperative sono state create per affrontare i cambiamenti sociali strutturali attraverso innovazioni economiche dirompenti. Peraltro, assecondando e metabolizzando i processi evolutivi che, negli anni, hanno attraversato la società, il fenomeno cooperativo ha vissuto sensibili mutamenti, indotti dall'esigenza di affrontare, nei diversi settori in cui esso ha trovato esplicazione, sfide nuove e sempre più impegnative e di acquisire competitività, rispetto all'impresa per così dire lucrativa, nel quadro di mercati sempre più dinamici e sensibili alle emergenti istanze economiche e sociali e sempre più improntati alle logiche della globalizzazione [18].

---

[17] Per una compiuta ricostruzione del dibattito sulla dimensione costituzionale del fenomeno cooperativo, cfr. A. Nigro, *Art. 45*, in G. Branca (a cura di) *Commentario della costituzione italiana,* III, Bologna-Roma, Zanichelli, 1980, 4 ss.; G. De Ferra, *Principi costituzionali in materia di cooperazione a carattere di mutualità*, in *Rivista delle società*, 1964, 776, R. Romboli, *Problemi costituzionali della cooperazione*, in *Rivista trimestrale di diritto pubblico*, 1977, 105; F. Galgano, *La cooperazione nel sistema costituzionale*, in *Nuovo diritto agrario*, 1977, 412; S. M. Cesqui, *La funzione sociale della cooperazione nel progetto costituzionale*, in *Rivista delle società*, 1995, 1153.

[18] Cfr., in tal senso, G. Capo, *Le cooperative di comunità*, in *Giurisprudenza commerciale,* 2021, 616. In argomento, vedi da ultimo anche G. Bonfante, *La società cooperativa*, in *Società*, 2023, 102 ss. D'altra parte, la proiezione dell'attività economica verso fini d'interesse generale costituisce una vocazione la cui compatibilità con i modelli organizzativi tradizionali dell'impresa, se pure non mutualistica, rappresenta un dato oggi acquisito anche in ottica normativa, se solo si considera — aldilà della disciplina speciale in tema di cooperative sociali — la regolamentazione dell'impresa sociale (d.lgs. 3 luglio 2017, n. 112), che, come è noto, tale qualifica riconosce a «tutti gli enti

Il fenomeno cooperativo, caratterizzato da un polimorfismo strutturale, fermi restando i principi generali enunciati a livello europeo, presenti nel Reg. CE n. 1453/2003 del 22 luglio 2003 sulla società cooperativa europea (SCE), trasfusi anche nel codice civile, è stato regolamentato nel nostro ordinamento, a livello extracodicistico, da norme speciali di settore la cui casistica è estremamente ampia. Si pensi alle cooperative di abitazione (cfr. r.d. 28 aprile 1938, n. 1165), le cooperative sociali (cfr. L. n. 381/91), le cooperative di credito (cfr. artt. 28 ss., D. Lgs. n. 385/93) le cooperative di garanzia o confidi (cfr. art. 13, D. L. n. 269/2003) i consorzi agrari (cfr. L. 28 ottobre 1999, n. 410).

Nonostante un'evidente inclinazione del legislatore europeo verso una torrenziale e quasi sfrenata normazione sulla *governance* dei dati, nulla è stato invece ancora concepito sulle cooperative di dati, e neppure a tale istituto si è dedicato alcun legislatore domestico nell'ambito dell'Unione. Non si può però negare che tale tipo di cooperativa, sia per la funzione sociale che dovrebbe ricoprire per riequilibrare la posizione di sottomissione o dipendenza che ha il cittadino nei confronti dei grandi operatori che bramano di ottenere dati personali, che per le peculiarità che la medesima ricopre rispetto agli altri tipi di coo-

---

privati, inclusi quelli costituiti nelle forme di cui al libro V del codice civile, che [...] esercitano in via stabile e principale un'attività d'impresa di interesse generale, senza scopo di lucro e per finalità civiche, solidaristiche e di utilità sociale, adottando modalità di gestione responsabili e trasparenti e favorendo il più ampio coinvolgimento dei lavoratori, degli utenti e di altri soggetti interessati alle loro attività» (art. 1, co. 1). Cfr., in argomento, A. FICI, *Tipo e status nella nuova disciplina dell'impresa sociale*, in *Contratto e impresa*, 2023, 112 ss. Non si può che concordare con chi (C. CAMARDI, *Enti collettivi e formazioni sociali, dal Libro I al Libro V attraverso il Terzo settore*, in *Contratto e impresa*, 2023, 470 ss.) ha rilevato come la situazione odierna esibisca uno scenario che sembra aver sostituito il paradigma dell'autonomia relativa (e della pacifica coesistenza) dei singoli sottosistemi giuridico-sociali con quello dell'ibrido, cioè con un paradigma che destruttura il precedente tentativo di bilanciamento istituito tra ciascuna funzione e le corrispondenti figure organizzative di riferimento. Ciò – indipendentemente dall'intenzione del legislatore – viene non solo semanticamente rappresentato dalle espressioni identificative delle discipline dei nuovi enti: «terzo settore», «impresa sociale», «società *benefit*».

perativa esistenti nel nostro ordinamento, necessiterebbe di una disciplina *ad hoc* che ne regoli le intrinseche sue tipicità.

Allo stato, quindi, l'attività delle cooperative di dati non potrà che rimanere all'interno dei vincoli, come si è accennato, non poi così limitanti, della normativa attualmente in vigore.

3. *L'incerta disciplina afferente le cooperative di dati dettata dal Data Governance Act*

Pur in assenza di una vera legislazione *ad hoc*, ma solo sulla base delle poche e non certo esaustive disposizioni presenti nel *Data governance act,* è possibile tentare di ricostruire la funzione della cooperativa di dati, che si sostanzia nel consentire agli interessati/titolari di dati personali di avere un maggiore controllo sulle proprie informazioni, di esercitare i propri diritti, di compiere scelte informate sul trattamento dei dati personali e di orientarne l'uso in base alle loro motivazioni e preferenze. Il tutto, previa raccolta o recupero collaborativo dei dati dei propri membri, ad esempio nella propria infrastruttura *cloud*, aiutando a ridurli e gestirli in un formato utile a livello di interoperabilità. Si veda infatti l'art. 12, par. 1, lett. *e)* del *Data governance act*, nel quale si stabilisce che i servizi di intermediazione, incluso quello di cooperative di dati, «possono comprendere l'offerta di strumenti e servizi supplementari specifici ai titolari dei dati o agli interessati allo scopo specifico di facilitare lo scambio dei dati, come la conservazione temporanea, la cura, la conversione, l'anonimizzazione e la pseudonimizzazione, fermo restando che tali strumenti e servizi sono utilizzati solo su richiesta o approvazione esplicita del titolare dei dati o dell'interessato e gli strumenti di terzi offerti in tale contesto non utilizzano i dati per altri scopi».

Le cooperative di dati mirano, quindi, a creare alternative più eque, sostenibili e socialmente responsabili rispetto alle piattaforme digitali tradizionali [19]. Sembra pertanto affacciarsi con questo nuovo strumen-

[19] Cfr., per la dottrina italiana sulle cooperative di dati, F. Bravo (a cura di), *EU*

to l'archetipo di quello che è stato definito il «*neomutualismo digitale*», come modello di crescita dell'economia, delle imprese, delle persone e della comunità, con l'obiettivo di agevolare una redistribuzione equa del valore aggiunto prodotto e l'affermarsi di un'economia del riuso sostenibile e dalla circolarità comunitaria [20].

Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo, Torino, 2024; F. BRAVO, *Cooperative di dati*, in *Contratto e impresa*, 2023, 757 ss.; L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, 800 ss. Per approfondimenti di dottrina straniera di taglio perlopiù economico sulle cooperative di dati, cfr. K. MILLER, 2021 *Radical proposal: data cooperatives could give us more power over our data*, consultabile in *https://hai.stanford.edu/news/radical-proposal-data-cooperatives-could-give-us-more-power-over-our-data*; J. KNAPP, J. KOBLER, F. RICHTER, *Data cooperatives– collective action as an opportunity for the european data economy and a european data private Law* in *InTeR* 1/23; M. MICHELI, E. FARELL, B. CARBALLA-SMICHOWSKI, M. POSADA-SÁNCHEZ, S. SIGNORELLI, M. VESPE, *Mapping the landscape of data intermediaries: Emerging models for more inclusive data governance*, 2023 [Report], Publications Office of the European Union, in *https://data.europa.eu/doi/10.2760/8943*; R. GADONI CANAAN, *Data cooperatives in Brazil: applicability and property rights*, in *Revista de Direito e as Novas Tecnologias*, n.11, 2021; I. NAEEM, A. NURUL, M. VASKA, S. GOOPY, R. RASHID, A. KASSAN, F. AGHAJAFARI, I. FERRER, A. KAZI, I. SADI, M. O'BIERNE, C. LEDUC, T.C. TURIN, *Community-based health data cooperatives towards improving the immigrant community health: a scoping review to inform policy and practice*, 2020, in *https://ijpds.org/article/view/1158/3214*; P. KENKEL, *Economic justification for a cooperative*, 2020, in *https://cooperatives.extension.org/economic-justification-for-a-cooperative/*; T. HARDJONO, T. PENTLAND, *Data Cooperatives: towards a foundation for decentralized personal data management* in *arXiv.org*; F. GILLE, E. VAYENA. 2021, *How private individuals maintain privacy and govern their own health data cooperative: MIDATA in Switzerland*, in *Governing privacy in knowledge Commons*, Cambridge, Cambridge University Press, 2021; 53-69; A. BLASIMME, E. VAYENA, E. HAFEN, *Democratizing health research through data cooperatives*, in *Philosophy and technology*, 2018, 31(3): 473 ss., in *https://doi.org/10.1007/s13347-018-0320-8*; M. DAWANDE, S. MEHTA, L. MU, *Robin Hood to the rescue:sustainable revenue-allocation schemes for data cooperatives*, in *Production and operation management*, 2022, vol. 32, 8; A.S. TANWAR, N. EVANGELATOS, G. VENNE, L. OGILVIE, K. SATYAMOORTHY, A. BRAND, *Global Open Health Data Cooperatives Cloud in an Era of COVID-19 and Planetary Health*, in *OMICS: A Journal of Integrative Biology, 2021*, in *https://doi.org/10.1089/omi.2020.01*.

[20] Lo evoca F. BRAVO, *Cooperative di dati*, cit., 764 ss., il quale a sua volta fa esplicito riferimento agli scritti di P. VENTURI, F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e welfare*, Milano, Egea, 2022.

In linea di principio, le cooperative promuovono un approccio comunitario alla condivisione dei dati, inteso come un modello decentralizzato in cui l'intera comunità partecipa al processo decisionale, ad esempio quando i dati sono gestiti come beni comuni. Viene, quindi, sostenuta la *governance* dal basso verso l'alto, con l'obiettivo di ridurre le asimmetrie di potere e i monopoli per la raccolta e l'utilizzo dei dati [21]. La comunità di una cooperativa di dati dovrebbe essere in grado di decidere su diverse questioni, quali: le regole, le norme e i principi per l'uso dei dati; la raccolta dei dati; le finalità di utilizzo dei dati; le modalità di accesso ai dati, ecc. Attraverso tale strumento, gli interessati possono mantenere un maggiore controllo sui propri dati rispetto a quanto accade nella maggior parte degli altri regimi di *governance* ed eventualmente ricevere un'equa quota dei benefici prodotti dall'uso dei dati. [22]. Il prerequisito che viene in gioco è quindi una competenza giuridica ed etica della cooperativa di dati, che consenta la valutazione dei fatti e la successiva consulenza ai soci, anche attraverso organi di revisione interni o esterni e comitati etici. In questo contesto, il servizio di supporto può includere anche meccanismi di risoluzione dei conflitti dei soci nell'ambito di una procedura regolamentata [23].

La cooperativa di dati è stata definita in maniera pervero ambigua dall'art. 2 n. 16, *Data governance act*, come «(...) una *struttura organizzativa* costituita da *interessati*, *imprese individuali o* da *PMI*, che sono *membri di tale struttura*». La lettera della norma non esplicita in maniera chiara la

---

[21] Cfr. K. Miller, *Radical proposal: data cooperatives could give us more power over our data*, Stanford HAI, 2021, consultabile in *https://hai.stanford.edu/news/radical-proposal-data-cooperatives-could-give-us-more-power-over-our-data*. Sulla distinzione tra fiduciari di dati e cooperative di dati, si veda L. Specht-Riemenschneider, A. Blankertz, P. Sierek, R. Schneider, J. Knapp, T. Henne, *Die Datentreuhand*, in *MMR-Beil.* 2021, 25.

[22] Cfr., in tal senso, S. Borkin, *Platform co-operatives – solving the capital conundrum*, 2019, consultabile in *https://platform.coop/blog/nesta-foundation-proposes-gbp-1-million-investment-fund-for-platform-co-ops/*.

[23] Cfr., in argomento, L. Specht, M. Hennemann, *Data governance act*, Baden-Baden, C.H. Beck, 2023, 103 ss.; vedi pure, a riguardo, A. Paschke, D. Rücker, *Data governance act. Kommentar,* cit., 179 ss.

forma societaria, ma essa sembra potersi concretizzare anche in una «struttura organizzativa» «costituita» nella forma del gruppo cooperativo (con una cooperativa in posizione di *holding*), nella declinazione delle sue tipologie, quali il gruppo–consorzio, la cooperativa *holding*, il gruppo cooperativo paritetico [24]. Né può aiutare a livello ermeneutico il Reg. CE n. 1453/2003 del 22 luglio 2003 sulla società cooperativa europea (SCE), che però, lo si ricorda, esprime una sostanziale identità con la normativa italiana [25].

---

[24] In questo caso, potrebbe richiamarsi il concetto di mutualità mediata, che ha avuto il suo battesimo legislativo con il regolamento (CE) n.1435/2003 sulla società cooperativa europea, il quale precisa che i soci possono essere anche persone giuridiche, a condizione che i membri di queste ultime siano utilizzatori dei servizi della cooperativa. Peraltro, già negli anni Sessanta, in una fase di uscita dalla marginalità economica della cooperativa, specie nel settore del consumo, abbondavano le prese di posizione della giurisprudenza sulla conciliabilità dello scopo mutualistico con lo scopo di lucro prendendo così forma una maggiore disponibilità in ordine alla partecipazione alla cooperativa di società ordinarie (Cfr. Cass., 13 dicembre 1967, n. 2943, in *Diritto fallimentare*, 1968, II, 564, Cass., 24 febbraio 1968, n. 632, in *Giustizia civile,* 1968, I, 1475). Non si può negare che in molti casi le stessi leggi speciali e la prassi consentano altresì la partecipazione di enti o società, anche di capitali, in una logica di strumentalità rispetto all'attività della cooperativa. La piena legittimità di una siffatta fattispecie resta incontrovertibilmente confermata dal 1°comma dell'art. 2527 c.c., che, vietando l'accesso alla cooperativa ai soggetti che esercitano in proprio un'attività imprenditoriale in concorrenza con quella della cooperativa, legittima il fatto che possano far parte della compagine sociale imprenditori con diversi campi di attività. Con la L. n. 127 del 1971, poi, il consorzio fra cooperative ha avuto un suo adeguato riconoscimento a livello generale e nel 1983 con la c.d. Visentinibis ha avuto diritto di cittadinanza la c.d. *holding* cooperativa controllante una o più società capitalistiche. Il legislatore ha introdotto poi il gruppo paritetico cooperativo con la riforma del 2003, e sono nate altre forme di collaborazione quali i c.d. contratti di rete. Su queste tipologie di cooperative, vedi F. VELLA, R. GENCO, P. MORARA, *Diritto delle società cooperative*, Bologna, Il Mulino, 2018, 235 ss. Suggerisce l'ipotesi che possano essere coinvolte associazioni temporanee di imprese (ATI) o dei raggruppamenti temporanei di impresa (RTI) o, ancora, delle «reti di imprese», che svolgano «servizi di intermediazione di dati» mediante logiche di «cooperazione» a beneficio dei propri membri, F. BRAVO, *Cooperative di dati*, cit., 760 ss.

[25] Cfr., riguardo alla legge sulla società cooperativa europea, *ex multis*, R. DABOR-

Gli obiettivi individuati dalla definizione di servizi di cooperativa di dati di cui all'art. 2 n. 16 del *Data governance act* sono menzionati in via alternativa. Si richiede che la predetta «struttura organizzativa» agisca con il fine principale di: aiutare i propri membri nel far valere le facoltà che l'ordinamento giuridico riconosce loro, favorendo l'acquisizione delle informazioni per l'esercizio dei diritti sui propri dati, in particolare qualora si tratti di dati personali; facilitare un confronto interno tra i propri membri, basato sullo «scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati», per rappresentare «al meglio gli interessi dei propri membri in relazione ai loro dati»; « (...) negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri (...)», ossia concordare con soggetti terzi, che utilizzeranno i dati, quali siano le condizioni giuridiche ed economiche volte a regolare i rapporti aventi ad oggetto l'uso di dati, personali e non personali, dei propri membri, persone fisiche o giuridiche. L'attività di negoziazione, aggiunge la definizione del servizio in questione, va svolta in un momento antecedente rispetto all'autorizzazione o al consenso al trattamento dei dati da parte dei «membri» della «struttura organizzativa» fornitrice del servizio.

Il *considerando* n. 31 precisa che «Le cooperative di dati mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del *gruppo*, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un *gruppo* in merito alle modalità di utilizzo dei dati, laddove tali dati riguardino più interessati all'interno di tale *gruppo*. In tale contesto, è importante riconoscere che i diritti a norma del Reg.

MIDA, *La cooperativa europea finalmente in porto*, in *Rivista della cooperazione*, 2003, 123; A. Ceccherini, *La società cooperativa europea (Regolamento CE, n. 1435/03 del Consiglio),* in *Le nuove leggi civili commentate*, 2003, 1295; E. Marra, *La società cooperativa europea*, in *Notariato*, 2005, 108; P. Marano, *La società cooperativa europea e le politiche comunitarie per reti e gruppi di imprese*, in *Rivista della cooperazione*, 2006, 9.

(UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi»[26].

[26] In sede di commento al testo della Proposta di Regolamento sulla governance dei dati, l'EDPB e l'EDPS hanno reso il Parere congiunto n. 3/2021, vers. 1.1 del 9 giugno 2021, ove sono state sollevate alcune critiche al servizio di cooperative di dati, ad iniziare dal concetto poco chiaro di tale servizio, in particolare con riferimento alla sua natura (Edpb-Edps, Parere congiunto sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati) n. 3/2021, par. 3.4.2, 35, consultabile in *https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_it*). Veniva denunciata altresì l'assenza di chiarezza, in realtà, anche nella stessa definizione di tali intermediari di dati e della disciplina applicabile, con riguardo soprattutto agli obblighi a loro carico, con conseguenti rischi di incertezza giuridica nella fornitura di tali servizi. Si tratta di problemi non risolti neanche nel testo definitivo del Regolamento. In tale parere, l'EDPB e l'EDPS affermano poi «che la posizione dei singoli individui nel compiere scelte informate e la soluzione di potenziali controversie sulle modalità di utilizzo dei dati non siano da considerarsi condizioni negoziabili, ma piuttosto obblighi dei titolari del trattamento a norma del regolamento (UE) 2016/679. Ancora, l'EDPB e l'EDPS hanno rinvenuto una contraddizione tra il Considerando n. 24 della Proposta di regolamento sulla governance dei dati (ora Considerando 31), in cui si trovava affermato espressamente che «i diritti a norma del regolamento (UE) 016/679 possono essere esercitati soltanto a titolo individuale e non possono essere conferiti o delegati a una cooperativa di dati» e il potere di negoziazione di cui godrebbe la cooperativa medesima su termini e condizioni da ottenere a beneficio dei soci persone fisiche, prima che questi forniscano il consenso al trattamento dei propri dati personali. Nella prospettiva dell'EDPB e dell'EDPS, «i "termini e le condizioni" per il trattamento di dati personali di fatto sono quelli contenuti nel GDPR e pertanto non possono essere modificati, né sostituiti, in virtù di un contratto o di un altro tipo di accordo privato». Cfr. però F. BRAVO, *Cooperative di dati*, cit., 787 ss., che evidenzia efficacemente che «i termini e le condizioni a cui fa riferimento la nuova disciplina europea sulla *data governance* – rimessi alla negoziazione delle *data cooperatives* – sono ben altra cosa rispetto alle condizioni di liceità del trattamento individuate nel GDPR quale base giuridica del trattamento. Una volta che sia stato rimosso il vincolo giuridico che impedisce lo svolgimento delle attività di trattamento a protezione dei diritti e delle libertà dell'interessato e sia operante il presupposto giuridico che consente al titolare di svolgere attività di trattamento sui dati personali – qual è, *in primis*, il consenso dell'interessato, che è atto autorizzatorio unilaterale volto a rimuovere il vincolo giuri-

Come visto, la definizione basata sui compiti suggerita dal *Data governance act* comprende le cooperative che aiutano i membri a compiere scelte informate prima di acconsentire all'uso dei dati e a negoziare termini e condizioni con gli utenti dei dati prima di dare il consenso individuale. La cooperativa di dati, insomma, dovrebbe avere la capacità di fornire agli individui e alle comunità le risorse e le conoscenze per valutare i termini del consenso. I membri della cooperativa, dopo essersi giovati della consulenza dalla struttura, saranno più propensi ad accettare condizioni favorevoli e, dopo il consenso, potranno avvalersi delle competenze della cooperativa per valutare il trattamento dei dati da parte di terzi. Le cooperative di dati dovrebbero avere anche la possibilità di avviare unilateralmente negoziati contrattuali con le organizzazioni di utenti dei dati nell'interesse dei loro membri e di adoperarsi per ottenere condizioni contrattuali che meglio si adattino ai loro interessi.

Le cooperative di dati dovrebbero poi valutare le conseguenze sociali prodotte dall'implementazione di sistemi di IA da parte di terzi o aiutare a distribuire i dati in *pool* per fornire valore ai propri membri eseguendo algoritmi in modo autonomo.[27] In taluni casi, la coopera-

---

dico che l'ordinamento europeo ha previsto al fine di rimettere all'interessato le decisioni in ordine al bilanciamento degli interessati in gioco nella fattispecie di trattamento, nella prospettiva dell'autodeterminazione informativa –, l'utilizzo del dato personale (e non il «dato personale» in sé) può essere oggetto di negoziazione e di contrattualizzazione, attraverso un accordo che si raggiunge mediante un consenso di natura contrattuale (non autorizzatorio), vertente sulle condizioni economiche e contrattuali (*terms and conditions*) stabilite tra le parti (Per tale ricostruzione cfr., F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Bologna, Zanichelli, 2019, 140 ss.; F. Bravo, *Lo "scambio di dati personali" nella fornitura di servizi digitali ed il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, 34 ss., con considerazioni rese anche a commento di due importanti *leading case* della S.C., e, segnatamente, Cass. n. 1748 del 29 gennaio 2016, caso Segafredo Zanetti, e Cass. n. 17278 del 2 luglio 2018, caso AdSpray, entrambe in *Dejure*, in cui la Cassazione apre ad una manifestazione congiunta delle due componenti, autorizzatoria e contrattuale, che rimangono tuttavia ontologicamente distinte, in quanto una incidente sul regime giuridico dei diritti della personalità, l'altra sul regime giuridico del diritto dei contratti.

[27] Cfr. F. Bravo, *Cooperative di dati*, cit., 785 ss., secondo cui si viene a realizzare

tiva potrà intervenire in proprio, quale soggetto autonomo e distinto dai propri soci; in altri casi, potrebbe intervenire come soggetto che agisce in nome e per conto dei soci; in altri casi ancora come facilitatore o mediatore per la formazione di accordi o, più in generale, di atti giuridici (anche unilaterali, come il consenso in materia di protezione dei dati personali) che verranno posti in essere direttamente dal socio o dal socio per il tramite della cooperativa, mediante il meccanismo della delega.

Ovviamente, l'apporto del socio-interessato alla formazione della volontà della cooperativa non può tradursi nell'automatico trasferimento alla cooperativa del potere di autodeterminazione facente capo all'interessato medesimo [28]. È ribadito il principio di irrinunciabilità dei diritti dell'interessato, incluso il diritto di revoca del consenso al trattamento dei dati personali, che non può ritenersi abdicato neanche

---

una «governance» duale, in base alla quale le scelte strategiche ed operative delineate a livello di cooperativa di dati (tramite la «governance collettiva») non precludono l'esercizio della «governance individuale», quantomeno qualora si tratti di dati personali facenti capo a singoli membri qualificabili come interessati al trattamento ai sensi del Reg. UE 679/2016.

[28] Come ricorda F. BRAVO, *Cooperative di dati*, cit., 789 ss., il principio è stato già espresso dalla S.C. (Cass. 1 giugno 2022 n. 17911, commentata da S. THOBANI, *Consenso al trattamento e delibere assembleari*, in *Giurisprudenza italiana*, 2022, 12, 2599 ss.), in un caso di trattamento illecito posto in essere da una cooperativa nei confronti di un socio lavoratore, in una fattispecie in cui veniva contestato il difetto del consenso al trattamento da parte di quest'ultimo, senza che potesse supplire, in tal senso, la volontà formatasi in seno all'adozione della delibera assembleare di funzionamento della cooperativa (la fattispecie riguardava la pubblicazione in bacheca di dati relativi a contestazioni disciplinari e le valutazioni effettuate dalla cooperativa sull'attività svolta dai soci lavoratori, mediante uso di "faccine" accostate alle foto di questi ultimi, nell'ambito di un "concorso" interno). La Cassazione, nella citata sentenza, ha infatti chiarito che è priva di rilievo la circostanza che «il trattamento sarebbe stato comunque, nella specie, giustificato dal consenso espresso in seno al rapporto associativo venutosi a costituire liberamente tra i soci e la cooperativa (e tra i soci stessi). La circostanza che il rapporto abbia natura associativa (o anche organizzativa) sì che alla gestione e alla formazione della volontà dell'ente contribuiscano gli stessi soci nelle forme assembleari previste, non comporta affatto che ogni trattamento di dati divenga per ciò solo consentito dai singoli secondo le forme stabilite in assemblea».

qualora l'esercizio dei diritti fosse delegato alla cooperativa di dati. Ciò spinge a ritenere che i diritti sui dati non possano essere mai oggetto di trasferimento e, al contempo, sono da escludere operazioni volte a configurare l'apporto dei soci, che forniscono dati alle cooperative, come una sorta di conferimento reale. I dati personali hanno tutt'altra natura e, al più, ciò che può essere conferito riguarderà il diritto all'utilizzo dei dati, sempre revocabile ad opera dell'interessato, ma non i dati in sé, su cui gli interessati continuano a mantenere inalterato il controllo [29]. Sembra ragionevole ritenere, però, che, mentre il divieto della rinunzia, quale tipico atto abdicativo, implichi l'impossibilità del conferimento in società (atto con efficacia reale), esso non precluda la stipula di un contratto di mandato (con rappresentanza), in quanto atto con mera efficacia obbligatoria. In questo modo, la cooperativa opererebbe per la tutela esterna dei diritti degli interessati in qualità di rappresentante dei suoi membri [30]. Che il consenso al trattamento dei dati personali non sia atto personalissimo, ma manifestabile anche tramite un rappresentante, emerge, peraltro, con evidenza nell'art. 8 GDPR, relativo al consenso dei minori, ove si trova stabilito che, nei casi in cui questi non possano esercitarlo personalmente, potrà essere esercitato, in loro rappresentanza, da chi esercita la responsabilità genitoriale [31].

---

[29] Lo sottolinea F. Bravo, *Cooperative di dati*, cit., 757 ss.

[30] Così G. Resta, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, 2022, 971-995, e F. Bravo, *Cooperative di dati*, cit., 793 ss.

[31] Del resto, nessuna norma prevede espressamente il contrario. Anche in tempi più recenti, viene più volte confermata la conformità all'ordinamento giuridico della delega per l'esercizio dei diritti dell'interessato. Così, ad esempio, il Garante ha precisato che «la disciplina in materia di protezione dei dati personali prevede –in ambito sanitario – che le informazioni sullo stato di salute devono essere comunicate all'interessato e possono essere comunicate a terzi solo sulla base di un idoneo presupposto giuridico o su indicazione dell'interessato stesso previa delega scritta di quest'ultimo» (GPDP, provv. 29 aprile 2021, n. 174, *doc. web* n. 9676143). L'art. 80, par. 1, del GDPR prevede, poi, espressamente che l'interessato abbia «il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo

Le cooperative di dati, come visto, rientrano nell'ambito di applicazione del terzo capitolo del *Data governance act*, in quanto servizi di intermediazione di dati (art. 10 lett. c). Si differenziano, però, in maniera significativa rispetto ai servizi di intermediazione di dati di cui all'art. 10, lett. *a)* e *b)*[32].

---

di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli artt. 77, 78 e 79 nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82».

[32] La disciplina sulla fornitura del servizio di cooperativa di dati, come per gli altri servizi di intermediazione dei dati, è delineata all'art. 12 del *Data Governance Act*, contenente le «condizioni» applicabili alla fornitura del servizio. La prima "condizione" riguarda sia l'esclusività dello scopo relativo all'utilizzo dei dati per i quali il fornitore si appresta ad erogare il servizio, sia il criterio di separazione, sotto il profilo soggettivo, tra fornitore e utilizzatore dei dati intermediati. Segnatamente, l'art. 10, par. 1, lett. a), *Data governance act*, precisa che «il fornitore di servizi di intermediazione dei dati [e dunque anche il fornitore del servizio di cooperativa di dati] non utilizza i dati per i quali fornisce servizi di intermediazione dei dati per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati e fornisce servizi di intermediazione dei dati attraverso una persona giuridica distinta» Secondo F. BRAVO, *Cooperative di dati*, cit., 757 ss., «la norma, per come è formulata, si presta a facili elusioni, in quanto si può ben prevedere un aggiramento, nell'ambito di gruppi societari o di collegamenti tra imprese, in cui una di esse esercita il ruolo di intermediario, un'altra quello di utilizzatore dei dati». Il medesimo Autore suggerisce che da un lato si potrebbe intervenire a livello interpretativo, applicando in maniera non rigida la "condizione" concernente l'obbligo di separazione soggettiva tra (fornitore del servizio di) cooperativa di dati e utilizzatore di dati, volta a sterilizzarne l'applicazione in considerazione della natura mutualistica della cooperativa, al fine di far salve le norme tipiche della società cooperativa, che devono essere coordinate a livello di sistema con quelle frettolosamente inserite, sul punto, nel *Data Governance Act*. La natura stessa della cooperativa potrebbe consentire, cioè, un'interpretazione volta a valorizzare la funzione della cooperativa di dati anche in ragione di un utilizzo dei dati medesimi a favore di quest'ultima e, dunque, anche a beneficio dei soci che la vanno a costituire. Dall'altro lato, propone di intervenire in via normativa – in sede europea o in sede nazionale, a livello di coordinamento della disciplina domestica con quella unionale –, chiarendo in maniera più dettagliata le peculiarità della disciplina della *data governance* con riguardo al caso specifico delle cooperative di

Se i *broker* di dati hanno lo scopo di ridurre i costi di transazione attraverso la loro funzione di *match-making* e di supporto nell'esecuzione tecnica e legale delle transazioni di dati, le cooperative di dati perseguono primariamente l'obiettivo di rafforzare la formazione e l'applicazione degli interessi dei loro membri e quindi aumentare il loro controllo dei dati. Queste ultime si distinguono pure per la struttura di gestione, considerando che sono composte da soci, che partecipano in una certa misura al processo decisionale e organizzativo dell'ente.

Va pure considerato il fatto che l'articolo 2 del *Data governance act* definisce il servizio di intermediazione dei dati come qualsiasi servizio il cui scopo è quello di stabilire relazioni commerciali per lo scambio di dati tra un numero indeterminato di interessati e di titolari, da un lato, e gli utenti dei dati, dall'altro. Tale definizione non pare calzante rispetto alla condizione dei soci di cooperativa, che sono soggetti «interessati» determinati o determinabili *a priori* (a meno che non si considerino come «indeterminati» i titolari di *account*, che non abbiano la condizione di socio, di cui si tratterà nel prossimo paragrafo).

Inoltre, per le stesse peculiarità strutturali della cooperativa di dati, salvo quelle che abbiano società o imprese come membri, non dovrebbero essere previsti conflitti di interesse tra chi fornisce servizi di intermediazione dei dati e l'utente dei dati, contrariamente a quanto può avvenire per gli altri intermediari di dati. Ci si chiede, quindi, per quale motivo, il legislatore abbia deciso di includere le cooperative di dati nell'ambito di applicazione del *Data governance act*[33]. Peraltro, tali differenze di struttura e funzioni tra intermediari non può che riverberarsi sull'eventuale natura della responsabilità civilistica degli uni e degli altri, in caso di illegittimo trattamento dei dati personali degli interessati, rispondendo gli intermediari di cui alla lettera a) e b) di cui

---

dati, facendo salva l'utilizzabilità dei dati da parte di quest'ultima, nello spirito mutualistico che la contraddistingue e la contrappone al modello più tipicamente capitalistico.

[33] Si pone questo interrogativo pure L. von Ditfurth, *Datenmärkte, Datenintermediäre Und Der Data Governance Act: Eine Analyse Der Europäischen Regulierung Von B2b-datenvermittlungsdiensten*, Berlin, De Gruyter, 2023, 265 ss.

all'art. 10, DGA, come soggetti autonomi, sulla base di una responsabilità precontrattuale o contrattuale a seconda dell'inquadramento del rapporto preesistente, in linea con la discussa posizione degli intermediari finanziari, e le cooperative di dati, invece, sulla base del rapporto societario, salvo per quanto si preciserà nel prosieguo, in ordine all'esistenza di contratti di servizi conclusi tra socio e cooperativa [34].

La fiducia che l'interessato deve riporre nell'intermediario è uno degli obiettivi del *Data governance act*, e, nel caso delle cooperative, dovrebbe essere accentuata o quantomeno preservata, oltre che dalla presenza dei controlli propri della normativa a tutela della *privacy*, anche da quelli previsti dalle norme sulle cooperative *tout court*. Al controllo dei dati da parte dell'individuo, con il sistema ormai consolidato del consenso dell'interessato, è stato affiancato un meccanismo incentrato: sulla notifica preventiva all'autorità competente in tema di intermediazione dei dati, accompagnata dall'istituzione del registro pubbli-

---

[34] Viene suggerita l'istituzione di un quadro normativo che chiarisca le questioni di responsabilità degli intermediari di cui al *Data Governance act* nel documento dell'associazione federale dell'organizzazione dei consumatori intitolato *Verbraucherzentrale Bundesverband, 'Neue Datenintermediäre'* (VZBV, 15 September 2020), consultabile in: *https://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15_vzbv-positionspapier_datenintermediaere.pdf*. In senso dubitativo a riguardo, ritenendo che sia sufficiente un maggiore controllo da parte delle istituzioni di vigilanza, e che il mercato sia così immaturo che le norme esistenti lascerebbero un margine di manovra e incentivi sufficienti per sviluppare tali servizi di intermediazione, J. KÜHLING, F. SACKMANN, H. SCHNEIDER, *Datenschutzrechtliche Dimension Datentreuhänder: Kurzexpertise' (Bundesministerium für Arbeit und Soziales*, 2020), 20, in https://nbn-resolving.org/urn:nbn:de:0168-ssoar-70086-9. In argomento, vedi pure H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, in *GRUR International*, 72, 5, May 2023, 458–470, consultabile in https://doi.org/10.1093/grurint/ikad014. Sulla disciplina degli intermediari finanziari, vedi V. TROIANO, R. MOTRONI (a cura di) *La Mifid II. Rapporti con la clientela – regole di governance - mercati*, Milano, Wolters Kluwer, 2016. Per una rassegna giurisprudenziale sull'argomento, vedi G. FAPPIANO, *Gli obblighi informativi degli intermediari finanziari al vaglio della giurisprudenza*, in *Contratti*, 2019, 4, 424 ss.. Ci si consenta, inoltre, un rinvio in argomento a S. FAILLACE, *La controversa categoria delle obbligazioni ex lege*, Milano, Wolters Kluwer, 2023, 161 ss.

co degli intermediari di dati tenuto dalla Commissione europea; sulla previsione di una serie articolata di condizioni di fornitura del servizio; sul monitoraggio delle conformità ad esse da parte della medesima autorità. È stato poi introdotto un sistema di esercizio rafforzato dei diritti dell'interessato, tramite l'azione esercitata dall'intermediario dei dati per conto dell'interessato, che si prospetta di maggior efficacia quando l'intermediario è una cooperativa di dati. Ma, come appena accennato, non ci si può dimenticare che la società cooperativa è sottoposta già ad una serie di ulteriori controlli esterni sulla gestione di natura amministrativa, che si aggiungono a quello dei sindaci, delle società di revisione e dello stesso tribunale *ex* art. 2409 c.c., controlli che mirano anche a preservare il rispetto delle finalità mutualistiche in ogni espressione cooperativa ed hanno indirettamente una funzione di tutela degli interessi dei soci e dei terzi [35].

[35] La fonte giuridica dei controlli sulle cooperative citati nel testo si trova nel D.Lgs. 220/2002, parzialmente emendato dalla L. n. 99/2009 e dall'art. 23 del D.L. 18 ottobre 2012, n. 179, ove viene statuito come questa funzione sia affidata al Ministero dello sviluppo economico, salvo per le banche popolari (Banca d'Italia), le cooperative di assicurazione (ISVAP), i consorzi agrari, le cooperative edilizie a contributo erariale, le cooperative con sede nelle regioni a statuto speciale per le quali la vigilanza spetta a soggetti diversi. L'altro soggetto protagonista nell'attività di vigilanza nel nostro ordinamento è rappresentato dalle organizzazioni di rappresentanza. Sul tema, vedi S. Patanè, *La revisione cooperativa*, in E. Cusa (a cura di), *La cooperativa s.r.l. fra legge e autonomia statutaria*, Padova, Cedam, 2008, 489; C. Tedeschi, *I controlli*, in G. Marasà (a cura di), *Le cooperative prima e dopo la riforma societaria,* Padova, Cedam, 2004, 717, P. Morara, *Il sistema dei controlli*, in R. Genco (a cura di), *La riforma delle società cooperative*, Milano, Ipsoa, 2003, 211; M. Iengo, sub art.2545 *quaterdecies*, in G. Bonfante, D. Corapi, G. Marziale, R. Rordorf, V. Salafia (a cura di), *Codice delle società commentato*, Milano, Giuffrè, 2011, 1851; E. Cusa, *La vigilanza sulla gestione delle cooperative nella legge n. 142 del 2001*, in *Rivista della cooperazione*, 2002, 33.

4. *L'esperienza delle cooperative di dati sanitari d'oltralpe e l'ipotetica sussunzione di tali modelli nel nostro sistema giuridico.*

Tra le cooperative di dati, saranno oggetto di analisi in questa sede quelle attinenti il settore sanitario, le quali, oltre a fornire un modello di *governance* equo per gli ecosistemi dei dati di tale tipologia, possono aspirare a garantire il miglioramento della qualità dell'assistenza sanitaria ed i progressi nella diagnostica e nella terapia, attraverso la ricerca scientifica, correggendo così l'asimmetria di potere tra interessati o titolari del trattamento dei dati e utenti dei dati, in particolare quelli del settore privato [36]. A fronte di questi potenziali benefici individuali e collettivi, le cooperative di dati sanitari devono però affrontare una sfida irta di ostacoli: il non poter disporre di un chiaro flusso di entrate.

Infatti, i dati provenienti dalle cooperative possono generare benefici non economici per i membri della comunità che hanno interessi condivisi, e che sono dediti alla raccolta e alla gestione dei dati sanitari per far progredire la ricerca sulle malattie rare o il miglioramento della salute, obiettivi che non possono essere perseguiti individualmente. Però questo tipo di incentivo è solitamente specifico per una comunità ristretta di individui. Per raggiungere la sostenibilità finanziaria, le cooperative di dati dovrebbero condividere i dati a fronte di un corrispettivo economico di terze parti e utilizzare una parte del valore generato per sostenersi. Tuttavia, nel caso il progetto sia di nicchia e manchi di *input* continui da parte degli interessati, il reddito ottenuto rischia di essere molto limitato e non sufficiente a garantire la sostenibilità dell'ente [37].

---

[36] Cfr. J. WILBANKS, E. TOPOL, *Stop the privatization of health data*, in *Nature*, 2016, 535, 345 ss.

[37] Le cooperative di dati hanno un alto rischio di fallimento, in quanto affrontano problemi di sostenibilità a causa del fatto che il loro modello di *business* sottende iniziative altruistiche, volontarie e condotte da privati. Si pensi al caso della cooperativa europea, con sede a Berlino, denominata Polypoly, che si è brevemente affacciata in questo panorama, con il fine dichiarato di aiutare i suoi soci a rivendicare

Nelle cooperative di dati sanitari, come vedremo, gli individui caricano e condividono dati, allo scopo di sostenere la ricerca scientifica, mantenendo al contempo un controllo granulare sui propri dati personali (conservando la possibilità di limitare o revocare l'accesso). Pertanto, dopo il consenso alla raccolta, i dati non scompaiono in banche dati inaccessibili, ma è consentito agli utenti di modificare le autorizzazioni di accesso in qualsiasi momento e di conoscere per quale scopo vengono utilizzati i propri dati. Ciò è reso possibile da sistemi tecnici, che includono l'archiviazione *cloud*, l'infrastruttura informatica, la gestione del consenso, le applicazioni *front-end* e *back-end* per l'accesso, la manipolazione e l'analisi dei dati e le considerazioni sulla sicurezza.

L'organizzazione collettiva e la messa in comune delle risorse nelle cooperative avranno peraltro lo scopo di attribuire ai membri un potere di contrattazione collettiva attraverso il quale possono negoziare con centri di potere esterni, quali, ad esempio, le aziende farmaceutiche. A tal proposito, le cooperative di dati potrebbero concedere un beneficio anche economico nel fornire un *surplus* ai propri membri, utilizzando dati aggregati elaborati per ottenere un valore aggiunto. Tuttavia, le cooperative che cercano di mettere in comune ed elabo-

---

la sovranità sui propri dati. Ogni membro della cooperativa poteva scaricare un'applicazione che memorizzava i dati dell'utente sul dispositivo personale. Questa applicazione aveva pure la funzione di raccogliere e ordinare i dati presenti *online* dell'interessato. I soci della cooperativa potevano scegliere come rendere disponibili i propri dati, in forma di donazione o a pagamento e se inoltrarli o meno in *database* di terze parti. In caso di scambio di denaro, la cooperativa riceveva una piccola percentuale da distribuire poi a tutti i soci della cooperativa. Purtroppo, a quanto risulta, l'avventura di questa società è già volta al termine, essendo attualmente in liquidazione. Anche LunaDNA, cooperativa di dati con sede a San Diego, California, che, offrendo un compenso, intendeva sollecitare le persone a condividere i propri dati personali, ha in realtà avuto vita breve (risulta essere stata cancellata in data 31 gennaio 2024). Destino diverso pare avere, invece, Savvy Cooperative, con sede a New York, che propone uno schema diverso, offrendo un *database* per i propri membri e promettendo ai medesimi un corrispettivo economico variabile a seconda del contributo proposto durante l'anno ai progetti di ricerca considerati dalla cooperativa degni di essere sviluppati.

rare dati aggregati sembrano non rientrare nelle tre funzioni di cui al *Data governance act* (cfr. Considerando n. 28). Inoltre, la possibilità che l'interessato ottenga un corrispettivo economico per condividere i propri dati sanitari è stata ampiamente criticata da chi ritiene che in tal modo si amplifichino le disuguaglianze, con riduzione dell'altruismo, suggerendo, a contrasto, l'idea del dato sanitario come una proprietà collettiva [38].

Lo stato di fatto, anche precedente all'emanazione ed entrata in vigore del *Data governance act,* ci ha presentato tipologie di cooperative di dati che hanno funzioni e svolgono compiti diversi [39]. Alcune cooperative cercano di isolarsi dal mercato adottando uno *status* senza scopo di lucro: ciò consente all'ente di godere di determinate forme di sgravio fiscale e rende ammissibili in suo favore sovvenzioni, finanzia-

---

[38] Cfr, in tal senso, B. PRAINSACK, N. FORGÓ, *Why paying individual people for their data is a bad idea,* in *Nature Medicine*, 2022, 28, 1989 ss.

[39] Ad esempio, *Healthbank Cooperative*, fondata nel 2019 in Svizzera, fornisce una piattaforma per lo scambio di dati sanitari, che può provenire da qualsiasi fonte. Chiunque può diventare azionista della cooperativa, che è finanziata attraverso *Initial Coin Oferings* (ICO) e *Security Token Oferings* (STO). Le ICO sono un modo per raccogliere fondi in un ambiente non regolamentato, offrendo un *token* di criptovaluta che può poi essere detenuto o scambiato. Tali azioni di criptovalute sono supportate da beni tangibili come azioni o persino profitti della società, consentendo partecipazioni azionarie e dividendi. Gli utenti hanno il pieno controllo dei propri dati, potendo revocare la condivisione dei propri dati anonimizzati in qualsiasi momento e per qualsiasi motivo. Se autorizzati, i dati possono essere condivisi con qualsiasi *partner*, come medici, *team* di assistenza, parenti e chiunque altro disponga di una connessione *internet*. I ricercatori possono acquistare i dati dalla cooperativa, che in cambio compensa i suoi membri. Un prerequisito per tale *trading* è il consenso informato degli utenti partecipanti. Si veda poi la *Holland Health Data Cooperative* (HHDC), fondata nel 2017 da diverse istituzioni private e pubbliche con l'obiettivo di consentire ai cittadini di gestire la propria salute e fornire un'alternativa alle aziende IT nell'economia dei dati sanitari. Tale cooperativa ha lo scopo di utilizzare collettivamente i dati nell'interesse dei suoi membri, che hanno sempre il controllo sui loro dati e possono rilasciarli ai fini della ricerca sanitaria. I dati hanno lo scopo di migliorare la prevenzione, l'autogestione, i prodotti, i servizi e i trattamenti. I ricavi generati dalla vendita dei dati vengono reinvestiti nel settore sanitario.

menti governativi, ecc. Tuttavia, è probabile che questa forma di finanziamento sia, da sola, insufficiente per i costi considerevoli che comporta, ad esempio, lo sviluppo e l'utilizzo del *software* dedicato di cui necessita l'ente per i servizi per la gestione dei dati. Altre cooperative operano come entità commerciali, il che apre la possibilità di ricevere finanziamenti da una gamma più ampia di operatori del mercato, quali investitori esterni, come categoria di membri particolari all'interno della cooperativa che detengano una classe distinta di azioni o valutando l'emissione di obbligazioni cooperative, titoli di partecipazione e certificati senza diritto di voto. Il fatto che possano coesistere motivazioni economiche senza scopo di lucro, imprenditoriali e altre motivazioni economiche ibride conferma più in generale l'ambivalenza delle cooperative, cui non possono far eccezione le cooperative di dati.

Le cooperative di dati sanitari che, nel prosieguo, saranno oggetto di analisi si configurano come cooperative dichiaratamente senza scopo di lucro. All'esito di tale studio, valuteremo se, in quanto tali, siano o meno destinatarie della disciplina di cui agli articoli 10-14 del *Data Governance act* e segnatamente delle condizioni per la fornitura di servizi di intermediazione dei dati (art. 12).

La cooperativa di dati Midata, fondata nel 2015 da un gruppo di ricercatori dell'ETH Zurigo e dell'Università di Scienze Applicate di Berna, è un'istituzione senza scopo di lucro [40], con una motivazione altruistica che va oltre la stessa comunità dei suoi membri e tesa a creare beneficio per l'intera società, come proclamato dall'articolo 2 del suo statuto [41]. Tale cooperativa gestisce una piattaforma informatica definita «sicura» per l'archiviazione, la gestione e la condivi-

[40] In base alla legge delle obbligazioni svizzera, all'art. art. 828, «la società cooperativa è l'unione di un numero variabile di persone o di società commerciali, organizzata corporativamente, la quale si propone in modo principale l'incremento o la salvaguardia, mediante un'azione comune, di interessi economici dei suoi membri o persegue uno scopo di utilità pubblica».

[41] Lo statuto è consultabile al seguente indirizzo: https://midata.coop/docs/MIDATA_Statuten_20170905.pdf.

sione di dati personali di qualsiasi tipo, in particolare dati sanitari e relativi all'istruzione, e per fornire i relativi servizi. Da un lato, afferma di «promuovere l'autodeterminazione digitale della popolazione consentendo ai titolari di conti di utilizzare i propri dati personali secondo i propri desideri, in particolare per sostenere scopi di ricerca»; dall'altro «promuove gli interessi collettivi dei titolari dei conti, consentendo l'utilizzo dei loro dati personali come risorsa comune». Adotta un approccio di *governance* chiamato supervisione sistemica che si basa sui principi di adattabilità, flessibilità, monitoraggio, reattività, riflessività e inclusività, per affrontare le preoccupazioni relative alla *privacy*, contribuendo attivamente alla ricerca medica e agli studi clinici, garantendo ai propri membri un accesso selettivo ai propri dati personali [42].

Chiunque può aprire un conto sulla piattaforma Midata o diventare socio della cooperativa (conferendo un contributo), il che ha il potenziale per rafforzare tale ente, aumentando il volume di dati e quindi il valore per la ricerca, e facilita la democratizzazione dell'economia dei dati. Il titolare di un *account* deposita copia dei propri dati (che usual-

[42] In argomento, vedi F. GILLE, E. VAYENA, *How private individuals maintain privacy and govern their own health data cooperative – MIDATA in Switzerland,* in M. SANFILIPPO, K. STRANDBURG, B. FRISCHMANN, *Governing Privacy as Knowledge Commons*, Cambridge, Cambridge University Press, 2021; S. GIRISH, M. AVERY, *Data Cooperative: Enabling Meaningful Collective Negotiation of Data Rights for Communities,* 2022, consultabile in https://ssrn.com/abstract=4414473; A. BLASIMME, E. VAYENA, E. HAFEN, *Democratizing Health Research Through Data Cooperatives*, Philos. Technol., 2018, 31, 473 ss., consultabile in https://doi.org/10.1007/s13347-018-0320-8; J. RODON MÒDOL, *Citizens Cooperation in the Reuse of Their Personal Data: The Case of Data Cooperatives in Healthcare,* in K. RIEMER, S. SCHELLHAMMER, M. MEINERT, *Collaboration in the Digital Age: how technology enables individuals, teams and businesses*, in *Progress in IS,* Berlin, 2018, 159 ss., consultabile in https://doi.org/10.1007/978-3-319-94487-6_8; I. VAN ROESSEL, M. REUMANN, A. BRAND, *Potentials and Challenges of the Health Data Cooperative Model,* in *Public health genomics* 20, n. 6 (2018): 321–331, consultabile in https://doi.org/10.1159/000489994; *CNIL (Commission Nationale de l'Informatique et des Libertés) and Analysis of Big Data Projects in the Health Sector,* consultabile al link: https://link.springer.com/chapter/10.1007/978-3-030-32161-1_29.

mente sono stati raccolti e archiviati altrove), e poi sceglie di renderli accessibili ai ricercatori, sulla base di progetti di ricerca. Tale cooperativa, peraltro, rimborsa le strutture sanitarie che forniscono dati in formato *standard*, partendo dal presupposto che tali dati possano generare entrate da reinvestire nella cooperativa stessa. I dati memorizzati da Midata sui *server* situati in Svizzera sono crittografati e accessibili solo dal titolare dell'*account*, a meno che il medesimo non li rilasci per uno scopo specifico. Il titolare di *account* può richiedere la cancellazione dei propri dati in qualsiasi momento, ma può anche condividere i propri dati personali (o specifici sottogruppi dei propri dati personali) con altri titolari di conto, con la cooperativa o con terzi. L'accesso da parte della cooperativa e da parte di terzi ai dati personali di un titolare di *account* richiede ovviamente il consenso espresso e informato di quest'ultimo, sia che i dati personali siano in forma originale, sia che siano in forma criptata (collegata attraverso una chiave ad una persona determinata) o anonima. Il consenso, peraltro, è gestito elettronicamente direttamente tramite la cooperativa. I titolari del conto hanno il potere decisionale esclusivo su quali dati devono essere memorizzati all'interno della cooperativa e quali dati rilasciare in vista di un progetto di ricerca.

La cooperativa si serve di un revisore indipendente e gli utenti dei dati devono presentare una proposta per l'utilizzo dei dati dei soci che deve essere esaminata dal comitato etico. Questo organo valuta gli strumenti a garanzia della *privacy* offerti dall'utente dei dati-richiedente e poi relaziona all'assemblea generale. Se tale proposta viene valutata positivamente dal comitato etico, il titolare dell'*account* può acconsentire a rilasciare i propri dati per il progetto specifico. Infatti, i meccanismi di supervisione all'interno della cooperativa garantiscono una valutazione scientifica ed etica delle richieste di accesso ai dati in entrata, ma gli interessati mantengono il controllo sull'opportunità di concedere tale accesso. Inoltre, gli interessati possono diventare soci della cooperativa, ed in tal caso esercitano un controllo sulla medesima in occasione dell'assemblea generale, cui possono partecipare. I soci partecipano inoltre alla *governance* della piattaforma, direttamente o indirettamente (ad esempio, eleggendo i membri dei comitati di sor-

veglianza) ed esercitano un controllo collettivo sull'intero *set* di dati, decidono come reinvestire i ricavi ed elaborano politiche per attività o questioni specifiche.

La cooperativa non fornisce alcun servizio che consenta ai titolari di *account* di vendere l'accesso ai propri dati personali a fronte di un corrispettivo individuale. Si evita in tal modo la creazione di incentivi finanziari personali in grado di creare problemi di tipo etico. Se l'uso secondario dei propri dati personali è richiesto da parte di terzi, il titolare di *account* può però chiedere in cambio una remunerazione economica da devolversi alla cooperativa. Ciò fermo restando il fatto che la cooperativa non distribuisce dividendi e non garantisce ai propri membri e ai titolari di *account* alcun indennizzo. Per finanziarsi, inoltre, la cooperativa può svolgere attività di investimento finanziario, detenere partecipazioni in altre società in Svizzera e all'estero, acquistare, detenere e vendere beni immobili. L'utile di bilancio deve però essere utilizzato per il miglioramento dei servizi offerti con e tramite la piattaforma Midata da un punto di vista qualitativo-quantitativo, per assicurare la sostenibilità finanziaria e perseguire gli scopi di utilità pubblica che si prefigge la cooperativa. Ciò dovrebbe garantire al contempo elevati *standard* di sicurezza e tutela dei dati. Tale cooperativa può, inoltre, sostenere la costituzione di cooperative di pari utilità in Svizzera e all'estero e costituire insieme ad esse una federazione di cooperative.

Similare all'esperienza di Midata, è quella di Salus.coop, una cooperativa di dati, pure senza scopo di lucro, con sede in Barcellona, fondata nel 2017, che mira a facilitare la condivisione sicura dei dati sanitari, consentendo ai cittadini di controllare le proprie cartelle cliniche, e incentivando al contempo l'innovazione della ricerca sanitaria. È definita come una società cooperativa di consumatori e utenti, soggetta ai principi e alle disposizioni della Legge sulle cooperative della Catalogna [43]. Ai sensi dell'art. 115 della suddetta legge,

[43] La legge 12/2005 delle cooperative catalane si basa sui principi generali storici dell'Alleanza cooperativa internazionale (ICA) e, in particolare, afferma che la

«obiettivo primario delle cooperative di consumatori e utenti è la consegna di beni o la prestazione di servizi per il consumo diretto dei soci e delle loro famiglie, e lo sviluppo delle attività necessarie a promuovere l'informazione, la formazione e la difesa dei diritti dei consumatori e degli utenti»[44]. Ai sensi dell'art. 2 dello statuto della cooperativa Salus, lo scopo di tale ente è: *a)* operare attraverso una piattaforma informatica sicura per la conservazione, la gestione e lo scambio di dati personali di ogni genere, ed in particolare dati sanitari e scolastici per fornire i relativi servizi; *b)* mettere a disposizione delle persone fisiche la piattaforma informatica per l'utilizzo da parte dei titolari di *account* di dati personali; *c)* lo sviluppo delle attività necessarie per l'incremento dell'informazione, della formazione e della difesa dei diritti dei consumatori e degli utenti. La cooperativa può sviluppare il proprio oggetto sociale direttamente o indiretta-

---

cooperativa è un'associazione autonoma di persone unite volontariamente per soddisfare i propri bisogni e le proprie aspirazioni economiche, sociali e culturali comuni attraverso un'impresa di proprietà comune e controllata democraticamente.

[44] È noto che il modello di cooperazione di consumo sia tra quelli più diffusi anche in Italia e si articola in diversi settori dell'economia. Tra le manifestazioni più risalenti di tale tipologia di cooperativa può citarsi la cooperazione di abitazione, di credito o di assicurazione, ma stanno emergendo già da alcuni anni altre tipologie di cooperative tra consumatori, quali – a titolo di esempio – quelle per l'acquisto di energia. La normativa riferita al modello delle cooperative di consumo è quella presente nel codice civile, né vi è una nozione di cooperativa di consumo e/o del suo scopo mutualistico. Quest'ultimo è stato ricostruito dalla dottrina o da circolari dei Ministeri competenti: i soci consumatori conseguono il vantaggio mutualistico attraverso un risparmio di spesa nell'ambito di rapporti di scambio originati da autonomi contratti intercorsi tra i soci stessi e la cooperativa. Un riferimento alla cooperazione di consumo nel codice civile è previsto dall'articolo 2512 c.c, il quale afferma, tra l'altro, che sono società cooperative a mutualità prevalente quelle che «svolgono la loro attività prevalentemente in favore dei soci, consumatori o utenti di beni o servizi». L'art. 2513 c.c. precisa poi che le cooperative di consumo acquisiscono il requisito della prevalenza mutualistica qualora dimostrino di avere ricavi dalle vendite dei beni e dalle prestazioni di servizi verso i soci superiori al cinquanta per cento del totale dei ricavi delle vendite e delle prestazioni, ai sensi dell'art. 2425, co. 1, punto A 1, c.c.

mente, anche attraverso la partecipazione in altre società. Ai sensi dell'articolo 5 dello statuto, in maniera generica si stabilisce che può essere socio chiunque desideri ottenere beni e/o servizi per il proprio consumo e uso e quello delle proprie famiglie nelle migliori condizioni di qualità, opportunità, informazioni e prezzi. Ai sensi dell'art. 6 dello Statuto, per l'ammissione di una persona come membro, occorre sottoscrivere il contributo minimo obbligatorio al capitale sociale.

Salus.coop fornisce consulenza ai propri soci in ordine all'utilizzo dei propri dati ed effettua controlli di *due diligence* sugli utenti dei dati, crea un modello di *governance* collaborativa per la gestione dei dati sanitari, che consente ai membri di decidere quale ricerca sostenere. Le persone che intendono donare i propri dati sanitari possono essere informate e assistite dalla cooperativa, che fornisce loro le informazioni necessarie per decidere con consapevolezza. Le persone che ripongono fiducia nella cooperativa possono delegare le decisioni ad essa. Al socio viene chiesta una quota associativa in denaro. Una parte di questo contributo sarà collocata nel fondo cooperativo e il resto sarà fornito all'individuo sotto forma di SalusCoin nel suo portafoglio personale. SalusCoin è la moneta interna sviluppata dalla cooperativa, che dà valore ai dati e alla partecipazione dei soci della cooperativa. I membri della cooperativa non ricevono incentivi monetari personali, per questo motivo è stata proposta la creazione di tale moneta interna, che permette alla cooperativa di premiare il contributo di tutti i soggetti coinvolti nel rendere possibile il modello. Più dati corrispondono a più Saluscoin. I cittadini possono utilizzare SalusCoin per acquisire servizi da fornitori accreditati o per finanziare progetti di ricerca promossi dalla cooperativa.

È prevista poi la creazione di un fondo di proprietà della cooperativa atto a concedere finanziamenti a specifici progetti di ricerca. Salus.coop si propone di offrire condizioni migliori ai progetti di ricerca più in linea con i valori delle cooperative e addebitare un prezzo più alto per i progetti considerati meno pertinenti dai membri della cooperativa (ad esempio, ricerca su malattie rare vs. ricerca su chirurgia estetica). Pertanto, grazie a questo fondo, la cooperativa è in grado

di contribuire ai campi di ricerca ritenuti più importanti, non solo con i dati, ma anche con le risorse finanziarie.

Come è possibile notare, nello svolgersi della vita societaria di entrambe le cooperative di dati sanitari analizzate, i rapporti tra le parti sono vincolati da una serie di accordi contrattuali che delineano il comportamento etico, lo scambio di valori, gli standard tecnologici, i termini di utilizzo dei dati, ecc., che le parti devono accettare. Tali accordi richiedono la gestione degli interessi divergenti delle parti, affrontando questioni quali le licenze, la proprietà intellettuale e la protezione dei dati. Un ruolo importante della cooperativa è quello di garantire il rispetto di questi accordi. Il contenuto specifico di tali accordi proviene da una decisione collettiva dei membri del gruppo. Innanzitutto, viene in rilievo l'accordo sul trasferimento dei dati tra gli interessati e la cooperativa. L'accordo stabilisce il diritto dei primi di essere ricompensati con dati meglio strutturati rispetto ai dati iniziali forniti. In altre parole, i dati saranno restituiti dopo essere stati ordinati e trattati in forma anonima e sicura. Vi è poi un contratto tra le società fornitrici di servizi e la cooperativa, nonché tra le prime e utenti dei dati o i membri della cooperativa. Per poter concludere tali contratti, le aziende esterne devono ricevere l'accreditamento rilasciato dalla cooperativa. Vi è poi un accordo di sfruttamento, destinato agli utenti dei dati che effettuano richieste di accesso ai dati dei membri. Il nucleo di questo accordo regola l'utilizzo consentito dei dati, le condizioni in base alle quali i dati vengono messi a disposizione e gli obblighi a cui gli utenti dei dati devono attenersi. Copre anche i criteri che governano il flusso economico tra le parti. Stabilendo il tipo di utilizzo dei dati consentito, questo accordo è finalizzato all'obiettivo precipuo di accelerare la ricerca e generare benefici collettivi. L'accordo riguarda anche la titolarità della proprietà intellettuale, le condizioni di licenza e di pubblicazione per i servizi sviluppati utilizzando l'insieme di dati cooperativo. A tale riguardo, un obiettivo importante dell'accordo è la promozione di licenze che garantiscano il prezzo più basso possibile dei farmaci (ad esempio *royalty free*, non esclusivo), riservatezza limitata e condivisione aperta delle conoscenze (ad esempio *Creative Commons*, pubblicazioni ad accesso aperto).

5. *L'ambito di applicazione soggettivo della disciplina concernente gli intermediari dei dati nel Data governance act e la sottile linea di confine tra concetto di «no profit» e «altruismo dei dati». I contratti di servizi tra soci e società cooperativa di dati sanitari e il relativo vantaggio mutualistico*

Come già rilevato, le due cooperative di dati sanitari analizzate dichiarano di non avere scopo di lucro, e, in tal senso, per come sono attualmente strutturate, non sembrerebbero loro applicabili, a prima vista, gli art. 10 e ss. del *Data Governance Act*, ma la disciplina dedicata agli enti per l'altruismo dei dati di cui agli artt. 16 e ss. della medesima norma. Del resto, le organizzazioni per l'altruismo dei dati riconosciute nell'Unione e i servizi di intermediazione di dati, nell'ambito di tale regolamento europeo, sono soggetti che hanno punti di contatto fra loro e, in alcuni casi, i loro modelli sembrano sovrapporsi.

Occorre, quindi, un breve approfondimento a riguardo, visto che tali cooperative di dati si inseriscono in un dibattito già incandescente sul concetto di *no profit* nell'interpretazione vigente in sede unionale e nel nostro ordinamento [45]. Di recente la Corte di Giustizia dell'Unione Europea ha tracciato un chiaro confine tra organizzazioni lucrative e

[45] In generale, sull'argomento, vedi da ultima C. CAMARDI, *Enti collettivi e formazioni sociali, dal Libro I al Libro V attraverso il Terzo settore*, in *Contratto e impresa*, 2023, 470, ss., secondo cui vi è un affievolimento della dicotomia concettuale tra scopo lucrativo e non lucrativo, da tempo avvertito da autorevoli studiosi attraverso il riferimento sia al tramonto dello scopo lucrativo nelle società, con riferimento ad alcuni tipi sociali, sia – correlativamente – alla funzionalità della figura fondazione all'esercizio di un'impresa. Cfr., ad esempio, Cass. Civ., sez. I, 27 ottobre 2023, n. 29801, in *Fallimento*, 2023, 12, 1492, che ricorda che le imprese sociali disciplinate dal d.lgs. n. 112/2017, a differenza degli enti del terzo settore (di cui al parallelo d.lgs. n. 117 del 2017), possono assumere tanto la forma organizzativa societaria (del Libro V del c.c.), che quella *lato sensu* associativa o fondazionale (del Libro I c.c.). Le imprese sociali, conservando l'assenza di scopo di lucro e le finalità civiche solidaristiche o di utilità sociale e secondo criteri di gestione e partecipazione solidaristica, possono dunque rivestire veste giuridica di società, cooperative comuni, cooperative sociali o loro consorzi. La possibilità di limitate forme di remunerazione del capitale o le regole sui ristorni hanno poi attenuato il distanziamento in termini

organizzazioni non lucrative, confine che è certamente vincolante per chi è chiamato a interpretare il diritto dell'Unione europea (e pertanto anche il conseguente diritto italiano di attuazione) in materia di contratti pubblici, ma allo stesso tempo utilizzabile al fine di fissare il perimetro dell'economia sociale e distinguere le diverse forme di enti, anche con limitati scopi lucrativi. Secondo la Corte di Giustizia le «organizzazioni e associazioni senza scopo di lucro» (di cui all'art. 10, lett. *h)*, Dir. 2014/24/UE) sono quelle che «hanno l'obiettivo di svolgere funzioni sociali», «non hanno finalità commerciali» e «reinvestono eventuali utili al fine di raggiungere l'obiettivo della stessa organizzazione o associazione». Non sono, invece, sussumibili tra gli enti *no profit*, secondo tale sentenza, quelli il cui statuto consenta la distribuzione degli utili tra i soci, anche solo a titolo di ristorno [46]. Ebbene, negli statuti delle sopra analizzate cooperative di dati sanitari non sono contemplati ristorni. Inoltre, tali cooperative non forniscono alcun servizio che consenta ai titolari di *account* di cedere la possibilità di utilizzare i propri dati personali a fronte di un corrispettivo individuale. Tali cooperative, poi, non distribuiscono dividendi e non garantiscono ai propri membri e ai titolari di *account* alcun indennizzo. Dunque, anche secondo l'interpretazione della Corte di Giustizia europea, tali enti dovrebbero correttamente essere inseriti tra quelli che non perseguono un fine di lucro. Peraltro, i titolari di *account* o i soci di tale cooperativa possono dare un esplicito consenso informato per l'uso secondario dei propri dati personali da parte di terzi, in cambio di una remunerazione economica da devolversi alla cooperativa per il raggiungimento dei fini propri di essa. E ciò confligge con l'art. 2, punto 16, del

assoluti tra *non profit* e scopo di lucro (in argomento vedi pure Marasà, *Imprese sociali, altri enti del terzo settore, società* benefit, Torino, Giappichelli, 2019).

[46] Cfr. Corte Giustizia Unione Europea, Sez. VIII, 7 luglio 2022 n. 213/21, in *Società*, 2023, 21, con nota di E. Cusa, *La nozione unionale di organizzazione non lucrativa tra contratti pubblici, terzo settore e trasporti sanitari di urgenza*, che afferma che i ristorni sono da considerare una quota dell'utile di esercizio, quand'anche fossero regolati dalla cooperativa come costi derivanti da appositi negozi parziari (nel medesimo senso, anche Cons. Stato, 3 maggio 2022, n. 3460 e Cass. Civ., 30 agosto 2022, n. 25495, entrambe in *Dejure*).

Data governance Act, secondo cui le organizzazioni riconosciute per l'altruismo dei dati non dovrebbero «chiedere o ricevere una ricompensa che vada al di là del compenso relativo ai costi sostenuti quando mettono a disposizione i loro dati per obiettivi di interesse generale»[47]. Ci troviamo, quindi, di fronte a cooperative senza scopo di lucro che svolgono attività commerciale solo al fine di perseguire il proprio sostentamento, ma che non possono, per ciò solo, essere inserite tra gli enti per l'«altruismo dei dati» e rispettare la relativa disciplina.

Per giungere ad inquadrare la disciplina corretta cui possono essere assoggettate tali cooperative di dati sanitari, corre in soccorso quanto stabilito dall'art. 15 del *Data governance act*, il quale traccia le condizioni di applicabilità della normativa di cui agli artt. 10 e ss., nei seguenti termini: «Il presente capo non si applica alle organizzazioni per l'altruismo dei dati riconosciute o ad altre entità senza scopo di lucro nella misura in cui le loro attività consistono nel cercare di raccogliere, per obiettivi di interesse generale, dati messi a disposizione da persone fisiche o giuridiche sulla base dell'altruismo dei dati, a meno che tali organizzazioni e entità non puntino a stabilire relazioni commerciali tra un numero indeterminato di interessati e titolari dei dati, da un lato, e utenti dei dati, dall'altro». E tra le organizzazioni senza fini di lucro che puntano, per sostenersi, a stabilire relazioni commerciali tra un numero indeterminato di interessati (sempre che si possano considerare come interessati «indeterminati» i titolari di *account*, e financo i soci, in base al principio proprio delle cooperative della porta aperta), e titolari dei dati, da un lato, e utenti dei dati, dall'altro, paiono annoverarsi società cooperative quali Midata e Salu-

[47] È stato il *Data governance act* a definire per la prima volta giuridicamente il termine «altruismo dei dati». È interessante notare che tale Regolamento europeo non usa il termine «donazione» e il richiamo a tale istituto pare sia stato deliberatamente evitato dal legislatore, in quanto implica il trasferimento di proprietà, mentre il diritto fondamentale alla protezione dei dati personali non può essere ceduto. Il concetto di altruismo dei dati sottende un consenso volontario e proattivo degli interessati all'uso dei loro dati per obiettivi di interesse generale, come la ricerca scientifica o il miglioramento dei servizi pubblici. In argomento, si rimanda a F. BRAVO, *Il principio di solidarietà tra data protection e data governance*, in *Diritto dell'informazione e dell'informatica*, 2023, 481 ss.

s.coop, che quindi ben potrebbero essere prese a modello per la costituzione di future cooperative di dati ai sensi dell'art. 10 lett. c) del *Data governance act*. Tali cooperative, infatti, da statuto, prima che i propri membri diano il loro consenso al trattamento dei dati personali, aiutano i medesimi nell'esercizio dei loro diritti, consentendo loro di operare scelte informate ed eventualmente anche negoziando i termini e le condizioni per il trattamento dei dati (in linea con quanto stabilito all'art. 2, n. 15 del *Data Governance Act*). Dovranno, altresì, sottostare alle condizioni per la fornitura dei servizi di cui all'art. 12, oltre che ai controlli e monitoraggi da parte delle autorità competenti per il servizio di intermediazione dei dati disciplinati dagli articoli 13 e 14 del *Data Governance Act*.

Ma è legittimo porsi ancora una domanda. È possibile nell'ordinamento cooperativo italiano attuale escludere con apposita clausola statutaria, come sembrerebbe avvenire per le due cooperative di dati sopradescritte, la ripartizione dei ristorni, una delle forme attraverso cui il socio può partecipare ai vantaggi cooperativistici, vantaggi che possono avere contenuto diverso a seconda del tipo di cooperativa? Per un'impostazione dottrinale, in assenza di una norma del nostro ordinamento che riconosca esplicitamente o implicitamente un diritto al vantaggio mutualistico e che riconosca più in particolare un diritto al ristorno, tale tipo di clausola sarebbe legittima [48]. Ma l'interpretazione contraria ha solide basi normative nell'art. 2521, n. 8, c.c., il quale pretende che lo statuto indichi i criteri di ripartizione dei ristorni, e nell'art. 2545 *sexies* c.c., che precisa che il ristorno remunera il servizio mutualistico in ragione della qualità e quantità degli scambi mutualistici [49]. Si prefigura, quindi, un problema interpretativo rilevante per chi

---

[48] Cfr. E. Cusa, *I ristorni nelle società cooperative*, Milano, Lefebvre Giuffrè, 2000, 163. Ritiene che una clausola siffatta andrebbe nel senso del rafforzamento della struttura patrimoniale della società, senza che quest'ultima perda di per sé quel tasso di mutualità che può essere goduto dal socio all'atto stesso dello scambio, R. Genco, *La struttura finanziaria*, in R. Genco (a cura di) *La riforma delle società cooperative*, Milano, Ipsoa, 2003, 92. Sul punto, vedi Trib. Milano 10 dicembre 2014, con nota di R. Dabormida, *Mutualità e ristorni nei consorzi con attività esterna*, in *Società,* 2015, 670.

[49] Cfr., in tal senso, anche G. Bonfante, *sub* art. 2545 *sexies*, in G. Cottino, G.

volesse sussumere nel nostro ordinamento tale tipo di cooperative, che non prevedono ristorni a livello statutario. Peraltro, il nostro legislatore, anche con la riforma societaria di cui al d.gs. 17 gennaio 2003, n. 6, così come già il codice civile, evita di definire espressamente lo scopo mutualistico, alimentando il dibattito a riguardo, ancorché sussista una certa prevalenza a riconoscere tale scopo nei termini della c.d. gestione di servizio al socio [50]. Quindi, il vantaggio mutualistico per il socio deve esistere e nelle cooperative nelle quali il socio chiede, e poi retribuisce, la prestazione della società (come nella cooperativa di consumo), viene conseguito attraverso un risparmio di spesa, mentre in quelle in cui è la società che chiede, e poi retribuisce, la prestazione del socio, il vantaggio viene conseguito attraverso un aumento del corrispettivo per l'attività prestata o per le forniture effettuate [51].

BONFANTE, O. CAGNASSO, P. MONTALENTI, *Il nuovo diritto societario*, *Commentario*, Bologna, Zanichelli, 2004, 2626, che ritiene che il ristorno sia la misura dell'efficacia mutualistica della cooperativa. Nell'attuale contesto normativo, secondo una dottrina (così G. FALCONE, *Commento* sub *art. 2545*-sexies, in M. SANDULLI, V. SANTORO (a cura di), *Le riforma delle società. Società cooperative. Artt. 2511-2548 cod. civ.*, Torino, Giappichelli, 2003, 179-180), il ristorno sarebbe divenuto una vera e propria categoria normativa. Si tratterebbe di una prescrizione obbligatoria, anche se poi la legge lascia una notevole, ma non assoluta, autonomia statutaria di fissazione dei criteri di attribuzione del ristorno, i quali devono rispettare comunque la parità di trattamento di cui all'art. 2516 c.c. Ossia a parità di condizioni quantitative e qualitative non è permessa una discriminazione fra i soci nel trattamento dello scambio mutualistico. Viene fatto salvo il caso in cui la mancata attribuzione del ristorno sia giustificata dalla dimostrazione, nella relazione *ex* art. 2545 c.c., di aver già conferito la prestazione mutualistica al costo o comunque anticipatamente o per contingenti necessità di investire nel patrimonio sociale tutte le eccedenze mutualistiche.

[50] Sulla circostanza che il legislatore dell'ultima riforma societaria del 2003 abbia fatto una precisa scelta di campo a favore della mutualità come gestione di servizio al socio, vi è una sostanziale concordia di opinioni nella maggioranza degli studiosi. Si veda a riguardo A. BASSI, sub art. 2511 c.c., in G. PRESTI (a cura di), *Le società cooperative*, Milano, Egea, 2007, 3 ss.; F. CASALE, *Scambio e mutualità nella società cooperativa*, Milano, Lefebvre Giuffrè, 2005, 86; G. MARASÀ, *Problemi attuali della società cooperativa e soluzioni della riforma*, in G. MARASÀ, *La riforma di società, cooperative, associazioni e fondazioni*, Padova, Cedam, 2005, 156.

[51] In molti casi, il vantaggio cooperativistico viene realizzato anche praticando

Dunque, da dove deriva il vantaggio mutualistico per i soci della cooperativa di dati sanitari senza fine di lucro? Pare derivare, anche in assenza di un ristorno in senso tecnico, dai servizi forniti dalla cooperativa senza un corrispettivo e collegati al trasferimento dei dati tra gli interessati e la cooperativa. La cooperativa, infatti, rafforza la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati, laddove tali dati riguardino più interessati all'interno di tale gruppo. Si può quindi enucleare da tali rapporti tra cooperativa e socio un rapporto contrattuale ulteriore di consulenza ed eventualmente di mandato. L'accordo, poi, stabilisce il diritto degli interessati-soci ad ottenere dati meglio strutturati rispetto ai dati iniziali forniti, eventualmente anoni-

---

un prezzo o corrispondendo un salario identici a quelli di mercato, e versando ai soci, a scadenze periodiche, e tenuto conto delle operazioni fatte, somme di denaro corrispondenti alla differenza, o fra i prezzi praticati e i costi (nella cooperazione di consumo), o fra i ricavi netti e i salari, o, comunque, i corrispettivi già versati dalla cooperativa al socio. È quest'ultima soluzione quella che viene definita come pratica del ristorno, tipico compenso nel rapporto mutualistico che, pur avendo con gli utili la comune caratteristica di essere rappresentato da somme di danaro periodicamente ripartite fra i soci, ne differisce proprio per il fatto che viene corrisposto in proporzione ai rapporti mutualistici intrattenuti dal socio con la società e non (come gli utili) in proporzione alla quota di capitale conferita (cfr. L.F. Paolucci, *I ristorni nelle cooperative*, in *Società*, 2000, 43). La concreta attribuzione del vantaggio mutualistico, quindi, può aver luogo in forza di due tecniche fra loro diverse, quella del vantaggio immediato e quella del vantaggio differito (Cfr., però, F. Galgano, *Mutualità e scambio nelle società cooperative*, in *Rivista di diritto civile,* 1985, 1031, che parla di vantaggio immediato e mediato). Sulla differenza tra utili e ristorni si è espressa, con una nota sentenza, la Suprema Corte (Cass. 22 maggio 2015 n. 10641, in *Società*, 2015, 1034) affermando che: «La sola caratteristica che i ristorni hanno in comune con gli utili è la aleatorietà, in quanto la società potrà distribuirli soltanto se la gestione mutualistica dell'impresa si è chiusa con un'eccedenza dei ricavi rispetto ai costi».

mizzandoli e/o rendendoli più sicuri. Su tale aspetto, però, lo si ripete, una puntualizzazione normativa sarebbe opportuna.

Del resto, appare ormai pacifico, dopo la riforma del 2003, ed il dato testuale degli artt. 2512, 2516, 2544, co. 1, c.c., che lo scopo mutualistico delle cooperative si realizzi con la stipula di contratti di scambio separati e distinti rispetto al contratto sociale, con un evidente collegamento contrattuale, potendosi piuttosto discutere se, a seconda dei tipi cooperativi, si sia in presenza di contratti tipici o atipici. [52] È stata superata, quindi, l'idea che tendeva ad escludere che siffatto atto di scambio avesse natura contrattuale per la mancanza di

[52] Sul punto è la stessa Relazione all'art. 2516 c.c. a definire lo scambio mutualistico come «rapporto contrattuale distinto da quello societario». In dottrina, vedi V. BUONOCORE, *Rapporto mutualistico e parità di trattamento*, in *Il nuovo diritto delle società, Liber amicorum Gianfranco Campobasso*, diretto da P. ABBADESSA, G.B. PORTALE, 4, Torino, Utet, 2007, 579 ss., che, nel commentare la riforma del 2003, ha osservato come essa abbia definitivamente legittimato lo scambio mutualistico come contratto distinto dal contratto sociale. Cfr., in senso analogo G. BONFANTE, *La società cooperativa, Itinerari di giurisprudenza*, in *Società*, 2023, 102 ss.; E. TONELLI, *Scambio mutualistico e rapporto sociale: interferenze e connessioni*, in M. SANDULLI, P. VALENSISE (a cura di), *Le cooperative dopo la riforma del diritto societario*, Milano, Franco Angeli, 2005, 29; E. ROCCHI, *sub* artt. 2512-2514 c.c., in G. PRESTI (a cura di), *Società cooperative*, Milano, Egea, 2006, 28 ss.; G. RACUGNO, *La società cooperativa*, in *Tratt. dir. comm.*, diretto da V. BUONOCORE, IV, 9, Torino, Giappichelli, 2006, 15 ss.; M. C. TATARANO, *La nuova impresa cooperativa*, Milano, Giuffrè, 2011, 91 ss.; A. PIRAS, *Profili mutualistici della* governance *delle società cooperative*, in M. CAMPOBASSO, V. CARIELLO, V. DI CATALDO, F. GUERRERA A. SCIARRONE ALIBRANDI, *Società, banche e crisi di impresa, Liber amicorum Pietro Abbadessa*, Torino, Utet, 2, 2014, 2023 ss. In giurisprudenza, fra le altre, vedi Cass. civ. 28 marzo 2007, n. 7646, in *Contratti*, 2007, 673; Cass. civ. 12 dicembre 2014, n. 26222, in *Società*, 2015, 941, con nota di M. CAVANNA; Cass. civ. 31 luglio 2014, n. 17465, in *Mass. Giur. it.*, 2014; Cass. civ. 26 gennaio 2015, n. 1343, in *Società*, 2015, 1328, con commento di G. BONFANTE; Cass. civ. 13 maggio 2021, n. 12949, in *Mass. Giur. it.*, 2021, nonché Cass. civ. 2 agosto 2023, n. 23606, con nota di C. GARILLI, in *Le società*, 2024, 2, 167 ss. Nelle cooperative edilizie, la giurisprudenza da tempo ha avuto occasione di affermare che un rapporto economico-giuridico distinto da quello sociale s'instaura tra la società e il socio prenotatario nella fase della successiva attribuzione dell'unità immobiliare costruita, che si configura come vero e proprio atto traslativo

una contrapposizione di interessi fra le parti [53]. Rispetto a tali rapporti

della proprietà a titolo oneroso. In tale fase, dunque, riprendono vigore i rimedi generali volti a mantenere o ristabilire l'equilibrio sinallagmatico tra la prestazione traslativa e la controprestazione economica. Vedi per tutte Cass. Civ., 18 gennaio 2001, n. 694, in *Società*, 2001, 945 ss., con nota di L.F. Paolucci. Pur individuandosi distinti rapporti di scambio con i soci, caratterizzati dalla corrispettività delle reciproche prestazioni, il contenuto dei medesimi potrebbe essere interamente o parzialmente predeterminato nello statuto, che finisce così con l'assumere le vesti di un contratto preliminare o di un contratto normativo, a seconda delle diverse configurazioni concrete e delle differenti interpretazioni datane dalla dottrina (vedi soprattutto F. Casale, *Scambio e mutualità nella società cooperativa*, Milano, Lefebvre Giuffrè, 2005, 48 ss. e 140 ss., che propende per la tesi del contratto normativo). Anche per la disciplina della Società cooperativa europea, lo scopo mutualistico è inteso come «soddisfacimento dei bisogni e/o promozione delle attività economiche e sociali» dei soci e promozione della loro partecipazione ad attività economiche, e si realizza attraverso rapporti di scambio mutualistico, che la norma definisce come «accordi per la fornitura di beni o di servizi o l'esecuzione di lavori». In senso contrario, ma con decisione recentissima allo stato isolata, vedi però Cass. Civ., 9 agosto 2023, n. 24242, in *Società*, 2024, 22, con commento di G. Bonfante, *La "morte" del contratto di scambio nelle cooperative secondo una sentenza del Supremo Collegio*, in *Società*, 2024, 24 ss., secondo cui l'obbligo di conferimento del prodotto che grava sui soci di una cooperativa agricola di trasformazione, obbligo essenziale per il funzionamento della società, è riconducibile a un contratto di durata ad esecuzione periodica, contratto che però non avrebbe una sua autonomia, risultando essere parte integrante del contratto sociale. Conseguentemente, la consegna da parte del socio del prodotto non determinerebbe l'operatività del principio di corrispettività, ma una mera aspettativa alla remunerazione del conferimento. In particolare, non essendo la remunerazione un "prezzo" in senso tecnico, ma soltanto l'attribuzione al socio/imprenditore *pro quota* del profitto generato dalla vendita dei prodotti trasformati, non sarebbe configurabile in capo al socio un diritto di credito al percepimento di un corrispettivo. E questa conclusione troverebbe conferma, nel caso di specie, secondo la Corte, anche dal regolamento approvato dalla cooperativa, in cui si afferma che il valore definitivo dei conferimenti deve essere stabilito in base ai risultati di gestione desumibili alla chiusura dell'esercizio sociale. Dunque, secondo la Suprema Corte, il socio verrebbe remunerato dei suoi conferimenti attraverso il profitto della cooperativa, mancando il quale non avrebbe diritto ad alcun corrispettivo in quanto socio/imprenditore.

[53] Cfr., per questa risalente impostazione, Cass. Civ., 23 aprile 1957, n. 1382, in *Foro pad.*, 1957, I, 649, secondo cui la distribuzione di merce ai soci non è assimilabile a una vendita (vedi ulteriori riferimenti in R. Genco, *Scopo mutualistico e gestione*

tra cooperativa di dati e soci, allora, saranno applicabili tutti i rimedi generali volti a mantenere o ristabilire l'equilibrio sinallagmatico tra le prestazioni, come l'art. 1460 c.c., nonché le regole generali in materia di responsabilità contrattuale (art. 1218 c.c). Dovrà essere pure valutata la relazione tra un eventuale recesso del socio della cooperativa ed i rapporti mutualistici in corso, visto il collegamento contrattuale tra contratto di società e contratto di scambio, fermo restando che, anche nel caso in cui non esista alcuna disciplina nello statuto o nel regolamento a riguardo, il recesso dal contratto di società dovrebbe determinare l'estinzione dei rapporti mutualistici [54]. Non altrettanto, invece, sembra potersi dire nel caso inverso, in cui il socio intenda recedere dai contratti di servizi collegati al trasferimento dei dati, non sembrando, nella fattispecie, possa considerarsi automatico anche uno scioglimento del rapporto del socio con la società.

dell'impresa, in G. SCHIANO DI PEPE (a cura di), *Cooperative, consorzi, raggruppamenti*, Milano, Ipsoa, 1996, 30). Si è anche sostenuto che tali negozi, pur autonomi e distinti rispetto al contratto sociale, subissero una sorta di curvatura causale in ragione degli scopi mutualistici della cooperativa (cfr. P. VERRUCOLI, voce *Cooperative (Imprese)*, in *Enciclopedia del diritto*, Milano, Giuffrè, 1962, 568).

[54] Cfr., in tal senso, A. BASSI, *Delle imprese cooperative e delle mutue assicuratrici*, in *Il codice civile. Commentario* diretto da P. SCHLESINGER, Milano, Giuffrè, 1988, 606; ID., *Le società cooperative*, Torino, Utet, 1995, 192. Vedi poi, in argomento, E. BONAVERA, *Recesso parziale del socio di cooperativa tra rapporto societario e rapporto mutualistico*, in *Società*, 2022, 549 ss.

Capitolo IV

LA TUTELA DELL'INTERESSATO NELL'USO PRIMARIO E SECONDARIO DEI DATI SANITARI SECONDO IL REGOLAMENTO EUROPEO CHE ISTITUISCE UN «*EUROPEAN HEALTH DATA SPACE*»

Sommario: 1. Gli obiettivi principali del Regolamento europeo che istituisce uno spazio di condivisione di dati sanitari. – 2. L'ampliamento e l'integrazione dei diritti dell'interessato alla luce della nuova disciplina comunitaria. – 3. (*Segue*). In particolare, la regolamentazione della portabilità dei dati sanitari. – 4. L'ambito di applicazione oggettivo e soggettivo della disciplina in ordine all'uso secondario dei dati sanitari. – 5 La base giuridica nell'uso secondario dei dati sanitari tra esigenze pubblicistiche e diritti di esclusione dell'interessato. – 6. La ricostruzione dei rapporti tra i soggetti che operano nello spazio di condivisione dei dati e la natura delle loro responsabilità in caso di deviazione dalla condotta *standard*. – 7. Riflessioni conclusive.

1. *Gli obiettivi principali del Regolamento europeo che istituisce uno spazio di condivisione di dati sanitari.*

Il Regolamento generale sulla protezione dei dati (GDPR) n. 679/2016 è stato definito come un ostacolo alla condivisione dei dati personali per la ricerca [1], sia per la sua attuazione frammentata nell'ambi-

[1] Cfr. D. Peloquin, M. DiMaio, B. Bierer, M. Barnes, *Disruptive and avoidable: GDPR challenges to secondary research uses of data, in European Journal of human genetics,* 2020, 697, consultabile *on line* al seguente indirizzo: http://www.nature.com/articles/s41431-020-0596-x

to dell'Unione europea (UE), che per la mancanza di chiarezza sulle basi giuridiche utilizzabili per l'uso secondario dei dati [2]. Pur esistendo, infatti, a livello nazionale, iniziative di raccolta dati come i registri nazionali delle malattie e le statistiche sanitarie ufficiali, pochi Stati membri dispongono di un quadro giuridico specifico per consentire l'uso secondario dei dati sanitari per la ricerca o per l'elaborazione delle relative politiche. Inoltre, variano in modo significativo da uno Stato membro all'altro le interpretazioni del GDPR relative alla condivisione dei dati finalizzata all'uso secondario [3]. In questo complesso qua-

---

[2] Cfr., in tal senso, SLOKENBERGA, TZORTZATOU, REICHEL, *GDPR and biobanking - individual rights, public interest and research regulation across Europe [Internet*]. Springer, 2020, in *https://www.springer.com/gp/book/9783030493875*

[3] Ad esempio, in Svezia, da decenni, i dati sanitari raccolti a livello nazionale sono stati resi disponibili e utilizzati per la ricerca, e la loro integrazione nell'EHDS non dovrebbe porre difficoltà (*EIT Health*, Scandinavia, 2023). Tale ricchezza di dati sanitari, tuttavia, è rimasta finora in gran parte non sfruttata a causa della frammentazione delle strutture regionali di *governance* dei dati che impedisce l'estrazione e l'aggregazione a livello nazionale. Il panorama irlandese, invece, è caratterizzato da un'interpretazione protezionistica del GDPR e dalla presenza di una legislazione nazionale in materia di ricerca sanitaria, che stabilisce la *governance* dell'accesso ai dati sanitari e le norme per il consenso dei pazienti alla ricerca, invisa ai ricercatori e vista da essi come un ostacolo all'uso dei dati dei pazienti per uso secondario (EIT Health Ireland-UK, 2023). In Italia e Spagna, così come in Austria, Belgio e Germania, le strutture e le pratiche di *governance* dei dati riflettono un'organizzazione ed una gestione decentralizzata dell'assistenza sanitaria a livello regionale. Se il caso italiano è stato già ampiamente analizzato nella sua complessità nei capitoli precedenti, si può affermare che in Spagna sia mancato un coordinamento dall'alto verso il basso rispetto ai diversi sistemi sanitari pubblici delle 17 regioni autonome, in relazione all'uso secondario dei dati sanitari. La Germania, invece, ha adottato misure per prepararsi all'attuazione dell'EHDS e ha proposto diversi progetti di legislazione, per sostenere la digitalizzazione e l'uso dei dati sanitari. Tra questi si possono annoverare il DigiG, la legge sulla trasparenza ospedaliera e la legge sull'uso dei dati sanitari, che hanno l'obiettivo di sviluppare un'infrastruttura decentralizzata di dati sanitari. È prevista la creazione di un laboratorio di dati sanitari (*Forschungsdatenzentrum Gesundheit*) presso l'Istituto federale per i farmaci e i dispositivi medici, per raccogliere tutti i dati sanitari del sistema tedesco EHR e dei registri tumori nazionali e regionali disponibili per scopi di ricerca. Negli ultimi decenni, poi, in Francia si è lavorato per

dro, si colloca l'approfondimento normativo verticale o settoriale del *Data Governance Act*, in linea con gli obiettivi esplicitati nella comunicazione della Commissione europea in data 19 febbraio 2020 denominata «Una strategia europea per i dati», tesa a facilitare l'accesso e la condivisione dei dati sanitari [4], e pure sulla base di esperienze pregres-

---

consentire un migliore utilizzo dei dati sia in ambito primario che secondario, a partire dalla strutturazione di tali dati attraverso la creazione di sistemi di codifica. Più recentemente, l'*Health Data Hub*, creato nel 2019, ha centralizzato e strutturato il processo per i ricercatori e gli enti pubblici per ottenere l'accesso ai dati del sistema sanitario francese e in particolare alla banca dati centralizzata, il Sistema Nazionale per i Dati Sanitari (SNDS). L'*Health Data Hub* sta attualmente sperimentando l'infrastruttura HealthData@EU per uso secondario, quale progetto pilota per l'attuazione dell'EHDS. Per armonizzare ulteriormente la *governance* dei dati sanitari a livello locale, nel 2023, è stato istituito un comitato strategico per i dati sanitari con il compito di fornire alle istituzioni sanitarie un *data warehouse* sanitario che standardizzi le richieste di accesso e la valutazione in linea con le norme nazionali di governance (EIT Health France, 2024). È interessante menzionare, poi, l'iniziativa Gaia-X – un progetto avviato da Germania e Francia sotto l'egida dell'Unione Europea – che si pone l'obiettivo di creare una infrastruttura di dati federata e sicura, in grado di consentire ad aziende e cittadini di gestire e condividere i dati mantenendone il controllo. L'architettura di Gaia-X è basata sul principio della decentralizzazione. Fra i suoi vari ambiti di applicazione, Gaia-X si concentra sul settore salute con l'obiettivo dichiarato di sbloccare il potenziale dei dati sanitari. In questo senso, Gaia-X intende contribuire allo sviluppo dell'*Health Data Space* utilizzando il suo quadro infrastrutturale, al fine di accedere ai dati sanitari e condividerli in modo sicuro, governato e controllato in modo coerente da ogni parte interessata. Da citare infine l'*European Genome-phenome Archive* (EGA) per il decentramento delle banche dati genetiche e fenotipiche, che in origine erano una risorsa centralizzata, e l'iniziativa europea per l'*imaging* del cancro.

[4] La comunicazione della Commissione europea in data 19 febbraio 2020, denominata «Una strategia europea per i dati» (COM/2020/66 Final), ha avuto come obiettivo ultimo quello di «creare uno spazio unico europeo di dati — un autentico mercato unico di dati, aperto ai dati provenienti da tutto il mondo — nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore, riducendo nel contempo al minimo la nostra impronta di carbonio e ambientale». Cfr. in argomento, F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al*

se, episodiche ma determinanti, che hanno dimostrato l'efficacia per la salute collettiva dello sviluppo di piattaforme di dati sanitari [5]. Si tratta del Regolamento per la creazione di un *European Health Data Space* (di seguito denominato con l'acronimo EHDS), la cui proposta fu presentata dalla Commissione europea in data 3 maggio 2022, che il 24 aprile 2024, dopo l'accordo politico raggiunto con il Consiglio dell'Unione europea, il Parlamento europeo ha approvato in prima lettura e così successivamente ha fatto poi il Consiglio in data 21 gennaio 2025 [6]. Il Regolamento UE EHDS n. 327/2025, pubblicato nella Gaz-

---

Data Governance Act, in *Contratto e impresa /Europa*, 2021, 199 ss.; G. RESTA, *La regolazione digitale nell'Unione Europea - Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, 2022, 971 ss.

[5] Ci si riferisce alla *European COVID-19 Data Platform*, ossia la piattaforma europea di dati sul COVID-19, che ha avuto lo scopo, a far data dall'aprile 2020 e su iniziativa della Commissione Europea, all'interno del piano d'azione «ERAvsCorona Action Plan», di consentire la rapida raccolta e condivisione dei dati di ricerca disponibili per apprestare le migliori soluzioni sul piano terapeutico ed epidemiologico. Tuttavia, tale iniziativa ha rappresentato una soluzione di emergenza, che ha dimostrato la necessità di un approccio strutturale e coerente a livello degli Stati membri e dell'Unione, sia al fine di migliorare la disponibilità di dati sanitari elettronici per l'assistenza sanitaria, che per orientare risposte politiche efficaci e contribuire a standard elevati di salute umana (in tal senso, il Considerando n. 2 del regolamento Ue sull' EHDS. A riguardo, vedi E. TACCONELLI, A. GORSKAA, E. CARRARA, R. J. DAVISA, M. BONTENB, A. W. FRIEDRICHC, C. GLASNERC, H. GOOSSENSE, J. HASENAUERF, J. M. HARO ABADH, J. L. PEÑALVOJ, A SANCHEZ-NIUBOH, A. SIALMI., G. SCIPIONEM, G. SORIANOJ, Y. YAZDANPANAHN, E.VORSTENBOSCHH, T. JAENISCH, *Challenges of data sharing in European Covid-19 projects: A learning opportunity for advancing pandemic preparedness and response*, in *The Lancet Regional Health - Europe*, 2022, 1; BRAGAZZI HAIJIANG DAI, G. DAMIANI, M. BEHZADIFAR, M. MARTINI, J. WU, *How Big Data and Artificial Intelligence Can Help Better Manage the COVID-19 Pandemic*, in *International Journal of Environmental Research and Public Health*, 2020, 1).

[6] La *Proposal for a regulation of the European Parliament and of the Council on the European health data space com/2022/197 final*, è consultabile al seguente link: *https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF*. In argomento, vedi SHABANI, *Will the European Health Data Space change data sharing rules?* in *Science,* 2022, 1357–1359, consultabile in https://doi.org/10.1126/science.abn4874; T. SCHMITT, S. COSGROVE, V. PAJIC, K. PAPADOPOU-

zetta Ufficiale dell'Unione Europea del 5 marzo 2025[7], consentirà ai

---

los, F. Gille, *What does it take to create a European Health Data Space? International commitments and national realities*, in *Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen,* 2023, 179, 1 ss.; Piscopo, Zipponi, *European Health Data Space e uso secondario dei dati: le molte domande ancora senza risposta*, in *www.agendadigitale.eu;* E. Biasin, *EHDS, un anno dopo: i temi caldi del dibattito sullo Spazio europeo dei dati sanitari*, consultabile al link *https://www.agendadigitale.eu*; R. Hussein, L. Scherdel, F. Nicolet, F. Martin-Sanchez, *Towards the European Health Data Space (EHDS) Ecosystem: A Survey Research on Future Health Data Scenarios*, in *International Journal of Medical Informatics*, Shannon, Ireland, 170 (2023), in doi: 10.1016/j.ijmedinf.2022.104949. Nella dottrina italiana, vedi S. Corso, *Lo spazio europeo dei dati sanitari: la Commissione Europea presenta la proposta di regolamento*, in *federalismi.it*, *Osservatorio di diritto sanitario*, 10 agosto 2022, 2 ss.; Id., *European Health Data Space. La Commissione europea presenta la proposta di Regolamento sullo spazio europeo dei dati sanitari*, in *www.rivistaresponsabilitamedica.it*, 13 giugno 2022; ID., *Il parere congiunto del Comitato europeo per la protezione dei dati e del Garante europeo della protezione dei dati in merito alla proposta di Regolamento sullo spazio europeo dei dati sanitari*, in *www.rivistaresponsabilitamedica.it*, 5 settembre 2022. Cfr. C. Rapisarda, *Sul costituendo spazio europeo dei dati sanitari*, in *Responsabilità medica*, 2023, 413 ss.; P. Terzis, *Compromises and Asymmetries in the European Health Data Space*, in *European Journal of Health Law*, in *brill.com*, 27 ottobre 2022; P. Terzis, E. Santamaria Echeverria, *Interoperability and governance in the European Health Data Space regulation*, in *Medical Law International*, in *journals.sagepub.com*, 24 aprile 2023. In tema, vedi pure G. Carullo, *Dati sanitari, sistemi sanitari nazionali e riuso dei dati*, in *Sanità pubblica e privata*, 2023, 19 ss.; V. Salvatore (a cura di), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Torino, Giappichelli, 2023; L. Bolognini, S. Zipponi, *Prospettive future in sanità: spazio europeo dei dati sanitari e regolazione dei dati scientifici*, in L. Bolognini, S. Zipponi (a cura di), *Privacy e diritto dei dati sanitari*, Milano, Lefebvre Giuffrè, 2024, 261 ss.; F. Cascini, M. A. Arcuri, *Uso secondario dei dati personali relativi alla salute: panoramica della normativa europea e nazionale*, in *Diritto dell'informazione e dell'informatica*, 2024, 6, 837 ss.. Da ultimo, vedi S. Slokenberga, M. Shabani, K. Ó Cathaoir, *The European Health Data Space: Examining A New Era in Data Protection,* Londra, Routledge, 2025; C. Perlingieri, *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici*; Id., *Intelligenza artificiale in àmbito medico-sanitario: profili di ricostruzione normativa a séguito dell'*AI Act, entrambi in Id., *Innovazione tecnologica e diritto civile. Saggi*, Napoli, ESI, 2025, 159 ss. e 131 ss.

[7] È prevista dall'art. 105, reg. EHDS un'applicazione graduale delle disposizioni del Regolamento, che avverrà addirittura tra i due e i dieci anni dalla sua entrata in vigore, per la necessità dei vari stati membri di uniformarsi alle nuove specifiche tecniche condivise a livello unionale.

pazienti di accedere ai propri dati sanitari in formato elettronico, anche se generati in uno Stato membro diverso da quello di residenza, e permetterà agli operatori sanitari di consultare le cartelle cliniche dei propri pazienti [8], previo loro consenso, anche da altri Paesi dell'Unione europea, facilitando così la continuità delle cure, il tutto regolamentando il ruolo del fornitore di servizi di condivisione di dati, i formati che garantiscono la portabilità dei dati sanitari, le norme di cooperazione per l'altruismo dei dati nel settore sanitario e l'accesso a dati privati per l'uso secondario [9]. L'EHDS intende fornire regole, standard e pratiche comuni, infrastrutture e un quadro di *governance* sia per l'uso primario (l'utilizzo di dati sanitari elettronici personali per fornire servizi all'individuo) [10], che per l'uso secondario (l'utilizzo di dati sanitari

[8] Secondo l'art. 11 reg. EHDS, nel trattare i dati in formato elettronico, i professionisti sanitari hanno accesso ai dati sanitari elettronici personali pertinenti e necessari delle persone fisiche in cura presso di loro attraverso i servizi di accesso per professionisti sanitari di cui all'articolo 12, indipendentemente dallo Stato membro di affiliazione e dallo Stato membro di cura e almeno con riferimento alle categorie prioritarie dei dati sanitari elettronici personali. Tale accesso è consentito tramite mezzi di identificazione elettronica.

[9] Più precisamente, secondo il Considerando n. 1: «Il presente regolamento ha lo scopo di istituire lo spazio europeo dei dati sanitari (*European Health Data Space*, EHDS) al fine di migliorare l'accesso delle persone fisiche ai loro dati sanitari elettronici personali e il loro controllo su tali dati nel contesto dell'assistenza sanitaria, nonché per conseguire più efficacemente altre finalità che comportano l'uso dei dati sanitari elettronici nei settori sanitario e assistenziale di cui beneficerebbe la società, quali la ricerca, l'innovazione, la definizione delle politiche, la preparazione e la risposta alle minacce sanitarie, anche per quanto riguarda la prevenzione e la gestione di future pandemie, la sicurezza dei pazienti, la medicina personalizzata, le statistiche ufficiali o le attività normative. Il presente regolamento ha inoltre l'obiettivo di migliorare il funzionamento del mercato interno istituendo un quadro giuridico e tecnico uniforme, in particolare per quanto riguarda lo sviluppo, la commercializzazione e l'uso di sistemi di cartelle cliniche elettroniche (*European Health record system* – EHR) in conformità dei valori dell'Unione».

[10] Secondo l'art. 1 lett. d) del Regolamento EHDS, si intende per «uso primario», il trattamento dei dati sanitari elettronici per la prestazione di assistenza sanitaria al fine di valutare, mantenere o ripristinare lo stato di salute della persona fisica

elettronici per esigenze più ampie come la ricerca sanitaria o le politiche pubbliche) dei dati sanitari. [11] Al Considerando 7 del GDPR, quale manifesto dell'intervento dell'Unione in siffatto settore, si legge che «è opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche» [12]. Il diritto dell'Unione impone, quindi, alle

---

cui si riferiscono tali dati, comprese la prescrizione, la dispensazione e la fornitura di medicinali e dispositivi medici, nonché per i pertinenti servizi sociali, amministrativi o di rimborso. Quindi, nell'ambito dell'utilizzo primario, il diritto alla portabilità, consentito all'interessato in forma potenziata, potrà giovare ad uno strumento esiziale come la telemedicina, definito dal decreto ministeriale 23 maggio 2022, n. 77, «Regolamento recante la definizione di modelli standard per lo sviluppo dell'assistenza territoriale del Servizio Sanitario nazionale», come «una modalità di erogazione di prestazioni socio-sanitarie e di prestazioni sanitarie a distanza, abilitate dalle tecnologie dell'informazione e della comunicazione e utilizzate da un professionista della salute per fornire servizi sanitari ai pazienti (operatore sanitario di telemedicina - paziente) o per fornire consulenza e servizi di supporto ad altri professionisti della salute (operatore sanitario di telemedicina - operatore sanitario)». Cfr. L. Ferraro, *La telemedicina quale nuova (e problematica) frontiera del diritto alla salute*, in *Diritto dell'informazione e dell'informatica*, 2022, 837.

[11] Secondo l'art. 1 lett. e) reg. EHDS, per «uso secondario dei dati sanitari elettronici» si intende il trattamento dei dati sanitari elettronici per le finalità indicate al capo IV del presente regolamento, che sono diverse dalle finalità iniziali per le quali tali dati sono stati raccolti o prodotti.

[12] All'art. 10 del Reg. EHDS, denominato « Diritto delle persone fisiche di esclusione riguardo all'uso primario», si precisa però che «La legislazione degli Stati membri può prevedere che le persone fisiche abbiano il diritto di esclusione dall'accesso ai loro dati sanitari elettronici personali registrati in un sistema di cartelle cliniche elettroniche attraverso i servizi di accesso ai dati sanitari elettronici di cui agli articoli 4 e 12. In tali casi, gli Stati membri garantiscono che l'esercizio di tale diritto sia reversibile. Se uno Stato membro prevede il diritto di cui al paragrafo 1 del presente articolo, stabilisce le norme e le garanzie specifiche relative a tale meccanismo di esclusione. In particolare, gli Stati membri possono prevedere che un prestatore di assistenza sanitaria o un professionista sanitario possa accedere ai dati sanitari elettronici personali nei casi in cui il trattamento sia necessario per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica conformemente all'articolo 9, paragrafo 2, lettera c), del regolamento (UE) 2016/679, anche se il paziente ha eser-

autorità nazionali degli Stati membri di cooperare nella gestione e nello scambio dei dati personali, al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, creando un livello di protezione dei diritti e delle libertà equivalente in tutti gli Stati membri [13].

L'obiettivo è, inoltre, quello di migliorare il funzionamento del mercato interno stabilendo un quadro giuridico e tecnico uniforme, in particolare per lo sviluppo, la commercializzazione e l'uso di sistemi

---

citato il diritto di esclusione riguardo all'uso primario». In argomento, vedi L. BOLOGNINI, S. ZIPPONI, *Prospettive future in sanità: spazio europeo dei dati sanitari e regolazione dei dati scientifici*, in L. BOLOGNINI, S. ZIPPONI (a cura di), *Privacy e diritto dei dati sanitari*, Milano, Lefebvre Giuffrè, 2024, 261 ss. Al considerando n. 18 del reg. EHDS, si precisa che, a causa delle diverse sensibilità negli Stati membri per quanto riguarda il grado di controllo del paziente sui suoi dati sanitari, gli Stati membri dovrebbero poter prevedere il diritto assoluto di esclusione dall'accesso ai propri dati sanitari elettronici personali da parte di chiunque non sia il titolare del trattamento originario, senza alcuna possibilità di superare tale esclusione in situazioni di emergenza. In tal caso, gli Stati membri dovrebbero stabilire le norme e le garanzie specifiche relative a tali meccanismi di esclusione. Tali norme e garanzie specifiche potrebbero riguardare anche categorie specifiche di dati sanitari elettronici personali, ad esempio i dati genetici. Il diritto di esclusione implica che i dati sanitari elettronici personali relativi alla persona fisica che ne ha fatto uso non sarebbero resi disponibili mediante i servizi istituiti nell'ambito dello spazio europeo dei dati sanitari se non al prestatore di assistenza sanitaria che ha fornito le cure.

[13] L'approccio europeo è contrapposto a quello di altri importanti attori del mercato, come la Cina e gli Stati Uniti. Come sottolineato nella comunicazione relativa ad una strategia europea per i dati, la Cina combina la sorveglianza governativa su enormi quantità di dati con un forte controllo delle aziende *Big Tech* senza fornire sufficienti garanzie per gli individui. Negli Stati Uniti, d'altro canto, l'organizzazione dello spazio dei dati è generalmente lasciata al settore privato, con notevoli effetti di concentrazione. La Commissione europea, invece, nelle proprie intenzioni persegue una via ancorata ai valori, ai diritti e ai principi europei. Tra gli aspetti centrali compare l'equilibrio tra la protezione della *privacy* e gli obiettivi di mercato, nonché l'*empowerment* attraverso i diritti dei dati. Cfr. S. SLOKENBERGA, M. SHABANI, K. Ó CATHAOIR, *The European Health Data Space: Examining A New Era in Data Protection*, Londra, Routledge, 2025, 3 ss.

di cartelle cliniche elettroniche («sistemi EHR») in conformità dei valori dell'Unione. Tale Regolamento mira, inoltre, a creare *dataset* di dimensioni sufficienti per consentire l'analisi e l'apprendimento automatico dell'intelligenza artificiale, basandosi pure sul concetto di «altruismo dei dati».

Il Legislatore rafforza, quindi, il controllo dei pazienti sui propri dati e stabilisce norme per i sistemi di cartelle cliniche elettroniche, al fine di promuoverne l'affidabilità, la sicurezza e l'interoperabilità [14] e consentire lo scambio per uso primario dei dati dei pazienti attraverso la piattaforma europea LaMiaSalute@UE (MyHealth@EU), [15] già

[14] Si deve ricordare che alcuni paesi europei hanno creato già un'embrionale interoperabilità dei dati. L'*European Union Patient Summary*, ad esempio, è un documento che viene generato utilizzando le informazioni già presenti nella cartella clinica elettronica del paziente e consente ai professionisti sanitari provenienti da altri Paesi dell'Unione Europea di fornire assistenza non programmata a cittadini che richiedano cure al di fuori del proprio Paese d'origine.

[15] Quest'ultima è un'infrastruttura volontaria, attraverso cui gli Stati membri offrono alle persone fisiche la possibilità di condividere i loro dati sanitari elettronici personali con prestatori di assistenza sanitaria in occasione di viaggi all'estero. Secondo il Considerando n. 33, Reg. EHDS, per sostenere ulteriormente tali possibilità, la partecipazione degli Stati membri a LaMiaSalute@UE (*MyHealth@EU*) quale stabilita dal presente regolamento dovrebbe essere obbligatoria. Gli Stati membri dovrebbero essere tenuti ad aderire a LaMiaSalute@UE (*MyHealth@EU*), rispettarne le specifiche tecniche e provvedere al collegamento di prestatori di assistenza sanitaria, comprese le farmacie, in quanto ciò è necessario per consentire alle persone fisiche di esercitare i propri diritti ai sensi dal presente regolamento ad accedere ai propri dati sanitari elettronici personali e a utilizzarli indipendentemente dallo Stato membro in cui si trovano. Tale trattamento è necessario per la prestazione di assistenza sanitaria in situazioni transfrontaliere, come indicato all'articolo 9, paragrafo 2, lettera h), di tale regolamento. In base al grado di sviluppo, il portale potrà contenere vari "prodotti informativi" relativi alla salute di un cittadino, ma deve contenere almeno il *patient summary* (o profilo sanitario sintetico), recante la storia e l'identità clinica dei cittadini, comprendente informazioni come diagnosi precedenti, trattamenti medici ricevuti, interventi chirurgici, allergie e reazioni avverse ai farmaci; le prescrizioni elettroniche relative a farmaci, prestazioni di diagnostica di laboratorio, di *imaging* strumentale, le visite mediche e così via. Solo in un secondo momento è

esistente ed attualmente funzionante in undici stati membri (tra cui l'Italia). Viene precisato al Considerando n. 34 e all'art. 23 del Regolamento EHDS che LaMiaSalute@UE (MyHealth@EU), quale infrastruttura comune agli Stati membri atta a garantire la connettività e l'interoperabilità in modo efficiente e sicuro a sostegno dell'assistenza sanitaria transfrontaliera, non incide sulle responsabilità degli Stati membri prima e dopo la trasmissione di dati sanitari elettronici personali attraverso tale infrastruttura, rimanendo in tali fasi, questi ultimi titolari dei dati. Si aggiunge, nel medesimo Considerando, che tale regolamento fornisce la base giuridica per il trattamento dei dati sanitari elettronici personali in LaMiaSalute@UE (*Myhealth@EU*), come compito svolto nell'interesse pubblico assegnato dal diritto dell'Unione ai sensi dell'articolo 6, paragrafo 1, lettera e), del regolamento (UE) 2016/679, e che tale trattamento è necessario per la prestazione di assistenza sanitaria, come indicato all'articolo 9, paragrafo 2, lettera h), di tale regolamento, in situazioni transfrontaliere.

2. *L'ampliamento e l'integrazione dei diritti dell'interessato alla luce della nuova disciplina comunitaria.*

Come noto, il regolamento (UE) 2016/679 (GDPR) stabilisce disposizioni specifiche relative ai diritti delle persone fisiche in relazione al trattamento dei loro dati personali. L'EHDS, nel confermare tali di-

---

previsto che accolga anche i risultati di diagnosi sotto forma di immagini diagnostiche, risultati strutturati di laboratorio e referti. Lo sviluppo di *MyHealth@EU* sarà supportato dall'istituzione di apposite autorità nazionali di salute digitale incaricate del monitoraggio delle regole associate all'uso primario dei dati, da disposizioni relative all'interoperabilità dei *set* di dati e dalla creazione di «punti di contatto nazionali» incaricati di far rispettare gli obblighi legati all'interoperabilità e alla *privacy* associati ai dati sanitari primari. È interessante notare che l'Autorità per la salute digitale è incaricata di svolgere una serie di compiti, tra cui la gestione dei reclami da parte degli individui, ma le Autorità garanti della privacy degli Stati membri rimangono competenti per quei diritti che si basano sul GDPR. In pratica, ciò significa che i due organi coesisteranno e collaboreranno strettamente.

ritti, li integra laddove si tratti di dati sanitari elettronici personali (art. 1, comma 2 lett. a) Reg. EHDS 327/2025). L'applicazione di tali facoltà è indipendente dallo Stato membro in cui sono trattati i dati sanitari elettronici personali, dal tipo di prestatore di assistenza sanitaria, dalle fonti di tali dati o dallo Stato membro di affiliazione della persona fisica [16]. Si consideri poi che i diritti e le norme relativi all'uso primario dei dati sanitari elettronici personali ai sensi di tale regolamento riguardano tutte le categorie di tali dati, indipendentemente dal modo in cui sono stati raccolti o da chi li ha forniti, dalla base giuridica del trattamento a norma del regolamento (UE) 2016/679 o dallo *status* del titolare del trattamento in quanto organizzazione pubblica o privata [17].

Innanzitutto, l'articolo 3 reg. EHDS, nell'enunciare i diritti fondamentali della persona fisica (*rectius* dell'interessato), stabilisce che la stessa ha il diritto di accedere immediatamente, gratuitamente e in un formato facilmente leggibile, consolidato e accessibile, ai propri dati sanitari elettronici personali che rientrino nelle categorie prioritarie e che siano trattati per la prestazione di assistenza sanitaria attraverso i servizi di accesso ai dati sanitari elettronici nel formato europeo di scambio delle cartelle cliniche elettroniche. Stabilisce pure il diritto di ottenere una copia elettronica di tali dati [18]. È qui esplicito e

---

[16] Secondo il Considerando n. 20 reg. EHDS, al fine di facilitare l'esercizio dei diritti complementari di accesso e portabilità stabiliti a norma del presente regolamento, gli Stati membri dovrebbero istituire uno o più servizi di accesso ai dati sanitari elettronici. Tali servizi potrebbero essere forniti a livello nazionale, regionale o locale o dai prestatori di assistenza sanitaria, sotto forma di un portale *online* per i pazienti, tramite un'applicazione per dispositivi mobili o tramite altri mezzi. Dovrebbero essere progettati in modo accessibile, in particolare per le persone con disabilità. Fornire tale servizio, che consente alle persone fisiche di accedere facilmente ai propri dati sanitari elettronici personali, costituisce un interesse pubblico sostanziale. Il trattamento dei dati sanitari elettronici personali tramite tali servizi è necessario per lo svolgimento del compito attribuito dal presente regolamento ai sensi dell'articolo 6, paragrafo 1, lettera e), e dell'articolo 9, paragrafo 2, lettera g), del regolamento (UE) 2016/679.

[17] In tal senso, vedi il Considerando n.8 Regolamento EHDS.

[18] Gli Stati membri dovranno poi istituire servizi di delega come funzionalità dei

convinto l'intento di amplificare i diritti di accesso e controllo già previsti dal GDPR, ed in quella sede impostati, pur in maniera blanda, come strumenti diretti soprattutto alla libera circolazione dei dati per incentivare il mercato. A norma del regolamento (UE) 2016/679, infatti, i titolari del trattamento non sono tenuti a fornire immediatamente l'accesso [19]. Tale diritto stabilito dal GDPR, peraltro, riguarda tutti i dati personali detenuti da un titolare del trattamento, quindi con un diverso ambito di applicazione oggettivo, ed è esercitato nei confronti di un singolo titolare del trattamento, che dispone di un mese per rispondere a una richiesta. Come è palese, l'accesso ai dati sanitari, ritardato ai sensi della disciplina di cui al GDPR, può avere un impatto negativo sulle persone fisiche che abbiano bisogno immediatamente di tali dati a causa di circostanze urgenti relative al loro stato di salute. All'uopo, il regolamento EHDS concede invece il di-

---

servizi di accesso ai dati sanitari elettronici che consentano: a) alle persone fisiche di autorizzare altre persone fisiche di loro scelta ad accedere per loro conto ai loro dati sanitari elettronici personali, o a una parte di essi, per un periodo determinato o indeterminato e, in caso di necessità, solo per una finalità specifica, e di gestire tali autorizzazioni; e b) ai rappresentanti legali delle persone fisiche di accedere ai dati sanitari elettronici personali delle persone fisiche di cui curano gli interessi, conformemente al diritto nazionale.

[19] Il diritto di accesso è stato riconosciuto *in primis* dall'art. 8, par. 2, della Carta dei diritti fondamentali dell'Unione Europea. Tale diritto si pone in un rapporto di propedeuticità-strumentalità rispetto ad altri diritti, quali quello di chiedere la rettifica o la cancellazione dei dati, in quanto l'interessato sarà in grado di esercitare questi ultimi proprio a seguito della conoscenza delle informazioni relativa al trattamento dei propri dati personali. La finalità del diritto di accesso consiste, insomma, nel mantenere un controllo sul trattamento dei propri dati personali, di verificare la legittimità di tale trattamento ed eventualmente di modificarlo attraverso richieste di integrazione, cancellazione od opposizione (cfr. A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 183). Il diritto di accedere viene, quindi, riconosciuto a prescindere dall'esistenza di una lesione lamentata dall'interessato (vedi *European Data Protection Supervisor, Guidelines on the Rights of Individuals with regard to the Processing of Personal Data*, caso 2011-0483, in *edps.europa.eu*) e senza che possano essere fatti valere limiti temporali (CGCE, 7 maggio 2009,C-553/07, College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer).

ritto di accesso gratuito e immediato, nel rispetto della praticabilità tecnologica, ma, come detto, alle (sole) categorie prioritarie definite di dati sanitari elettronici personali, attraverso un servizio di accesso elettronico ai dati sanitari [20]. Il diritto di accesso di cui all'articolo 15 del regolamento (UE) 2016/679 continuerà invece ad applicarsi per i dati sanitari non elettronici (cartacei o scansionati successivamente) [21].

Ai sensi dell'art. 5 reg. EHDS, inoltre, le persone fisiche o i loro rappresentanti hanno il diritto di inserire informazioni nella propria cartella clinica elettronica attraverso servizi o applicazioni di accesso

[20] Attualmente, tra le categorie prioritarie sono compresi i seguenti documenti: profili sanitari sintetici dei pazienti; prescrizioni elettroniche; dispensazioni elettroniche; esami diagnostici per immagini e relativi referti di immagini; risultati degli esami medici, compresi i risultati di laboratorio e altri risultati diagnostici e relativi referti; lettere di dimissione. Sebbene importanti, tali elementi sono ben lungi dal rappresentare la totalità del contenuto delle cartelle cliniche elettroniche di un paziente. Ai sensi del medesimo articolo, gli Stati membri possono però prevedere, in virtù del diritto nazionale, che siano accessibili e scambiate ulteriori categorie di dati sanitari elettronici personali per l'uso primario. Si consideri poi che potrebbe non essere etico informare un paziente attraverso un canale elettronico della diagnosi di una malattia incurabile, che probabilmente sarà terminale, anziché prima comunicare tale informazione in un colloquio con il paziente. Pertanto, in tali situazioni, dovrebbe essere possibile ritardare la fornitura dell'accesso ai dati sanitari elettronici personali per un periodo limitato, ad esempio fino al momento in cui il professionista sanitario possa spiegare la situazione al paziente. Gli Stati membri dovrebbero essere in grado di fissare tale eccezione, laddove costituisca una misura necessaria e proporzionata in una società democratica, in linea con le limitazioni previste all'articolo 23 del regolamento (UE) 2016/679. (cfr. Considerando n.10 Reg. Ue EHDS n. 327/2025).

[21] Cfr. CGUE C-307/22 FT v DW ECLI:EU:C:2023:811, secondo cui le persone dovrebbero «avere accesso ai dati contenuti nelle loro cartelle cliniche nel modo più completo e preciso possibile, ma anche in una forma intelligibile». La fornitura di un semplice riassunto o di una compilazione di tali dati da parte del medico potrebbe comportare il rischio che alcuni dati pertinenti siano omessi o riprodotti in modo non corretto o, in ogni caso, che sia reso più difficile per il paziente verificare l'esattezza e l'esaustività di tali dati e la loro comprensione.

ai dati sanitari elettronici collegati a tali servizi. Tali informazioni inserite dall'interessato dovranno essere chiaramente distinguibili come tali. Tale diritto di inserimento è un diritto nuovo e si affianca ai diritti di rettifica e portabilità, che si basano sulla loro precedente concettualizzazione nel GDPR. A riguardo, va sottolineato che gli individui e i loro rappresentanti possono avere percezioni diverse del valore e della qualità delle informazioni che inseriscono, percezioni divergenti rispetto alle opinioni dei professionisti medici e che non possono di certo avere lo stesso valore clinico o legale. Pertanto, i medesimi dovrebbero essere chiaramente distinguibili dai dati forniti dai professionisti sanitari [22].

Peraltro, il regolamento non impone che le informazioni aggiunte all'EHR si riferiscano alla salute e non vi sono requisiti stabiliti in relazione alla qualità di tali informazioni inserite. Di sicuro, gli operatori sanitari non potranno assumersi la responsabilità di questi dati, ed anzi, onde evitare possibili responsabilità, dovranno guardarsi dal compulsarli al fine di redigere una diagnosi [23]. Le persone fisiche non hanno, ovviamente, la possibilità di modificare direttamente i dati sanitari elettronici e le relative informazioni inseriti dai professionisti sanitari, i servizi di accesso ai dati sanitari elettronici consentono però alle persone fisiche di chiedere *online* facilmente la rettifica dei loro dati sanitari elettronici personali, conformemente all'articolo 16 del GDPR 2016/679 e quale applicazione del principio di esattezza di cui all'art. 5 della medesima norma [24]. Si consideri che il diritto di rettifica stabi-

---

[22] Cfr, a riguardo, il Considerando n. 12 reg. EHDS.

[23] Per un approfondimento sui rischi di inserire da parte di un interessato *test* genetici DTC all'interno del proprio EHR, vedi A.M. PHILLIPS, *The right to insert and add information to my health record – does my doctor need to know this? A critical discussion of the right to insert information in an EHR using the example of data from direct-to-consumer genetic testing,* in S. SLOKENBERGA, K. Ó CATHAOIR, M. SHABANI, *The European Health Data Space. Examining A New Era in Data Protection*, London, Routledge, 2025, 44 ss.

[24] Nell'ordinamento italiano, relativamente all'esercizio dell'attività giornalistica, si ritrova una primigenia traccia del diritto di rettifica nell'art. 8 della legge sulla stampa, n. 47 del 1948. Specificamente, con riguardo alla tutela dei dati personali,

lito dall'art. 6 reg. EHDS si applica a tutte le informazioni contenute nei registri sanitari elettronici, incluse diagnosi, prescrizioni, risultati di test di laboratorio e qualsiasi altro dato rilevante ai fini dell'assistenza medica. La rettifica può essere richiesta in caso di errori materiali, come referti inesatti o trascrizioni errate, o per aggiornare informazioni che risultano obsolete rispetto allo stato attuale del paziente. Il regolamento EHDS prevede che gli Stati membri mettano a disposizione delle persone fisiche procedure efficaci e accessibili per presentare richieste di correzione, garantendo che le modifiche necessarie vengano apportate in tempi ragionevoli e senza complicazioni burocratiche. Un elemento centrale della normativa riguarda la validazione delle rettifiche, che deve avvenire in modo trasparente e sotto il controllo dei professionisti sanitari responsabili della gestione dei dati. L'art. 6 del regolamento EHDS stabilisce che le correzioni apportate dai pazienti devono essere verificate per garantire che non compromettano l'integrità delle informazioni cliniche. I professionisti sanitari devono valu-

---

invece, il diritto alla rettifica lo si rinviene all'art. 8, lett. c) della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, laddove si prevede appunto la possibilità di ottenere la rettifica dei dati o la loro cancellazione, qualora i medesimi siano stati elaborati in violazione delle disposizioni di diritto interno che danno attuazione alla Convenzione *de quo*. Il diritto di rettifica di cui al GDPR facoltizza e consente all'interessato una forma costante di controllo attivo sui propri dati, in modo che dagli stessi possa emergere, nel corso del tempo, una corretta ed effettiva rappresentazione della sua immagine, *rectius* della sua identità personale, non trasfigurata dalla presenza di informazioni erronee, o anche solamente incomplete alla luce di una loro naturale obsolescenza, allorché non aggiornate in funzione degli eventi della vita che possono averlo *medio tempore* riguardato (Cfr. in argomento M. Tampieri, *L'identità personale: il nostro documento esistenziale*, in *Europa e diritto privato*, 2019, 4, 1198 ss.; vedi pure F. Calisai, *I diritti dell'interessato*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 327). Del resto, se l'identità «è sintesi di tanti elementi di natura diversa che la compongono, essa non è certo una sintesi statica. Il tempo gioca un ruolo essenziale: la persona è ciò che è in un determinato momento e l'identità muta col tempo» (Cfr., in tal senso, G. Finocchiaro, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, *Diritto dell'informazione e dell'informatica*, 2012, 389).

tare le richieste di rettifica e confermare l'accuratezza delle modifiche prima che vengano integrate nei sistemi digitali. Questo processo evita il rischio di manipolazione dei dati e garantisce che le informazioni contenute nelle cartelle cliniche elettroniche restino affidabili e conformi agli *standard* medici [25].

Secondo l'art. 8 reg. EHDS, poi, le persone fisiche hanno il diritto di limitare l'accesso dei professionisti sanitari e dei prestatori di assistenza sanitaria alla totalità o a parte dei loro dati sanitari elettronici personali di cui all'articolo 3. Tale limitazione non è visibile ai prestatori di assistenza sanitaria [26]. Nell'esercitare tale diritto, le persone fisiche dovranno essere informate del fatto che la limitazione dell'accesso potrebbe avere un impatto sulla prestazione dell'assistenza sanitaria, che non si gioverà di un'anamnesi completa della persona, con intuibili e già vagliate in precedenza complessità nell'individuazione della colpa in un eventuale trattamento medico non di successo [27].

3. *(Segue) In particolare, la regolamentazione della portabilità dei dati sanitari*

Il diritto alla portabilità, già riconosciuto dal GDPR, assume, per certo, maggiore rilevanza nel regolamento UE sull'EHDS e ottiene

---

[25] Cfr., in tal senso, M. IASELLI, *Le nuove regole per l'uso primario e secondario dei dati sanitari. Reg. UE 11 febbraio 2025, n. 327 (EHDS)*, Santarcangelo di Romagna, Maggioli, 2025.

[26] Con riferimento al diritto di limitazione nel GDPR, vedi F. DI CIOMMO, *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2018, 367 ss.; G. GIANNONE CODIGLIONE, *La tutela della riservatezza*, in S. SICA, V. ZENO ZENCOVICH, *Manuale di diritto dell'informazione e della comunicazione*, Milano-Padova, Wolters Kluwer, 2019, 281-310; E. PELINO, *I diritti dell'interessato*, in L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Lefebvre Giuffrè, 2016, 225-235.

[27] Vedi a riguardo quanto già scritto nel paragrafo quarto del capitolo primo del presente lavoro.

un ampliamento del suo ambito di applicazione, finora francamente limitato. Si ricorda che esso, anche in considerazione della sua collocazione sistematica nell'ambito del GDPR, è prima di tutto un diritto personale dell'individuo teso a realizzare la sua identità digitale e segna in tal senso la strada europea nel settore [28]. Il principale obiettivo di tale diritto consiste nel rafforzare il controllo sui propri dati personali quando siano detenuti da altri (considerando 7 e 68 GDPR), e ciò in base al principio – largamente accettato nella dottrina europea – che la protezione dei dati personali serva interessi che eccedono la tutela della *privacy* e si estendano all'«autodeterminazione informativa». Il diritto alla portabilità intende promuovere, insomma, il controllo degli interessati, facilitando così la circolazione, la copia o la trasmissione da un ambiente digitale all'altro, in linea con il principio della libera circolazione dei dati personali nel panorama UE [29]. Si tratta di un diritto

[28] La portabilità dei dati è un diritto che spetta solo alle persone fisiche (con esclusione quindi di persone giuridiche, associazioni, ecc. che non sono titolari del diritto alla tutela dei dati personali sulla base della CEDU, Carta dei diritti fondamentali e TFEU) ed è esercitabile unicamente dall'interessato. Vedi però, sotto il profilo della delegabilità di tale diritto, il caso *Weople*, app italiana che promette ai propri iscritti una remunerazione in cambio della cessione dei propri dati personali. Il Garante italiano della Privacy, con lettera in data 1 agosto 2019 (in *www.garanteprivacy.it*), successivamente revocata, ha investito della questione il Comitato europeo per la protezione dei dati personali (EDPB), denunciando, da un canto, la corretta applicazione, da parte di tale società, del diritto alla portabilità dei dati introdotto dal GDPR, esercitato mediante delega e con il rischio di possibili duplicazioni delle banche dati oggetto di portabilità, e, dall'altro, il tema stesso della commerciabilità dei dati, «causata dall'attribuzione di un vero e proprio controvalore al dato personale». Cfr., a riguardo F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa/Europa*, 2021, 247, A. Morace Pinelli, *La circolazione dei dati personali tra tutela della persona, contratto e mercato*, in *Nuova giurisprudenza civile commentata,* 2022, 1322 ss. Cfr. poi sul punto la delibera AGCM del 14.7.2022, caso *Google vs Weople*, consultabile all'indirizzo *www.agcm.it* e inerente al carattere abusivo di talune pratiche della società californiana ritenute in grado di ostacolare l'esercizio del diritto alla portabilità dei dati previsto all'art. 20 GDPR, in quanto possibile soltanto per il tramite dell'applicativo *Google Takeout* e previa autenticazione tramite ID e *password*.

[29] Cfr. S. Troiano, *Il diritto alla portabilità dei dati personali*, in N. Zorzi Galgano

complesso, che risulta dal combinato disposto dei paragrafi 1 e 2 dell'art. 20 GDPR e consta del diritto dell'interessato di «ricevere (...) i dati personali che lo riguardano forniti a un titolare di trattamento», del «diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti» e del «diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile» (par. 2) [30]. Il GDPR riconosce all'interessato la possibilità di ricevere dal titolare le informazioni che lo riguardano «in formato strutturato, di uso comune e leggibile da dispositivo automatico» (art. 20, par. 1, GDPR), ed è stato da taluni considerato assimilabile a un diritto di accesso con modalità vincolate [31]. Da tale diritto deriva, da un lato,

---

(a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR* (a cura di), Milano, Wolters Kluwer, 2019, 199. Sulle differenze tra diritto di accesso e diritto alla portabilità, cfr.: W. LI, *A tale of two rights: exploring the potential conflict between right to data portability and right to be forgotten under the General Data Protection Regulation*, in *International Data Privacy Law*, 2018, 8, 4, 309, 315; R. STOYKOVAR, *The Right to Data Portability. Data protection scope and technical feasibility*, in *Computer Law Review International*, 2018, 3, 65, 66-67.

[30] Ritengono che la portabilità dei dati comprenda tali tre pretese, G. MALGIERI, *Il diritto alla portabilità dei dati personali,* in G. COMANDÉ, G. MALGIERI (a cura di)*, Manuale per il trattamento dei dati personali*, Milano, Il sole 24 ore, 2019, 54; S. TROIANO, *Il diritto alla portabilità dei dati personali, in* N. ZORZI GALGANO (a cura di)*, Persona e mercato dei dati. riflessioni sul GDPR*, Milano, Wolters Kluwer, 2019, 195. Parlano, invece, di un diritto a duplice contenuto, F. PEZZA, *Diritto alla portabilità dei dati*, in G.M. RICCIO, G. SCORZA, E. BELISARIO, (a cura di) *Gdpr e normativa privacy. commentario*, Milano, Giuffrè Lefebvre, 2022, 201 ss.; G. M. RICCIO, *Portabilità dei dati personali e interoperabilità,* in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 397 ss.; A. RICCI, *I diritti dell'interessato*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da G. FINOCCHIARO, Bologna, Zanichelli, 2019, 179 ss.; L. R. BIANCHI, *Il diritto alla portabilità dei dati,* in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (codice privacy), scritti in memoria di Stefano Rodotà*, Milano, Lefebvre Giuffrè, 2019, 225 ss.; E. BATTELLI, G. D'IPPOLITO, *Il diritto alla portabilità dei dati personali*, in E. TOSI (a cura di), *Privacy digitale. riservatezza e protezione dei dati personali tra GDPR e nuovo codice privacy*, Milano, Lefebvre Giuffrè, 2019, 185 ss..

[31] Per «formato strutturato», dovrebbe intendersi un formato che mantiene for-

un ampliamento della protezione dei dati personali, con rafforzamento della facoltà di scelta dell'utente, dall'altro, un più spiccato stimolo agli aspetti concorrenziali del mercato digitale, volto a favorire la competitività tra i fornitori dei servizi della società dell'informazione.

L'idea di fondo è semplice: si vuole consentire a ciascun individuo che utilizzi servizi *on-line* di trasferire i propri dati personali da un servizio o da un fornitore all'altro, in modo da poterli riutilizzare in piena autonomia, senza perdere il patrimonio di informazioni creato in precedenza.

Si tratta però di una tutela riconosciuta dalla disciplina del GDPR con specifico riguardo ai trattamenti automatizzati che richiedono il consenso espresso dell'interessato ovvero in presenza di un contratto intercorrente tra le parti [32]. In questi casi, all'interessato, è riconosciuta

---

mattazione e organizzazione delle informazioni (Così E. Pelino, *I diritti dell'interessato*, in L. Bolognini, E. Pelino, C. Bistolfi, *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Lefebvre Giuffrè, 2016, 250). Per «formato di uso comune», dovrebbe intendersi un formato che consente modifiche o comunque la facile estrapolazione delle informazioni in esso contenute. Infine, per «formato leggibile», dovrebbe intendersi la possibilità di intervenire sulle informazioni in esso contenute e di modificarle.

[32] Ciò è sottolineato da E. Bani, E. Macchiavello, *Il diritto alla portabilità dei dati nell'ambito della nuova economia dei dati*, in V. Falce, *Financial Innovation tra disintermediazione e mercato*, Torino, Giappichelli, 2021, 137 ss. Già nella Comunicazione sull'economia dei dati del 2014, la Commissione ha sottolineato l'importanza della portabilità dei dati per la costruzione di un mercato interno dei dati (Cfr. Commissione Europea, *Verso una florida economia basata sui dati*, (2 luglio 2014), COM(2014) 442 final, 13; Commission, *A Digital Single Market Strategy for Europe (Communication)* COM(2015) 192 final 6. Cfr. anche, European Commission, *Turning fair into reality Final Report of the European Commission Expert Group on FAIR Data*, EU, Brussels, 2018, in https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf. Il precedente logico e storico, in ambito europeo, è dato dalla portabilità del numero telefonico da un operatore all'altro e dalla portabilità dei mutui (In argomento, vedi S. Troiano, *Il diritto alla portabilità dei dati*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, Wolters Kluwer, 2019, 195 ss.; E. Battelli, G. D'Ippolito, *Il diritto alla portabilità dei dati personali*, in E. Tosi (a cura di), *Riservatezza e protezione dei dati tra GDPR e nuovo Codice Privacy*, Milano, Lefebvre Giuffrè, 2019, 187 ss.; R. H. Weber, *Data portability and big data analytics. New competition*

la possibilità di ricevere dal titolare del trattamento le informazioni che lo riguardano e trasferirle ad altro titolare, senza che possa essere opposto alcun tipo di impedimento, se non di carattere tecnico. Si tratta quindi di un diritto dotato di una duplice anima: da un lato l'accesso ai propri dati, cui consegue il rilascio di una riproduzione della documentazione che contenga quanto espressamente richiesto nell'istanza; dall'altro, si delinea una rafforzata facoltà di scelta dell'utente, che potrà decidere di trasferire ad altro titolare del trattamento le informazioni che lo riguardano. La portabilità dei dati è considerata proprio un'evoluzione dell'accesso ai dati [33]. Se il diritto di accesso, disciplinato dall'art. 15 del GDPR, è un diritto avente natura conoscitiva e statica, il diritto alla portabilità, invece, rientra fra i diritti di controllo sui dati e la sua tutela è pertanto dinamica [34].

Inoltre, l'esercizio del diritto alla portabilità dei dati lascia impregiudicato il diritto alla cancellazione o «diritto all'oblio» ai sensi dell'art. 17 del GDPR (art. 20, par. 3). Questo significa che la trasmissione dei dati da un titolare ad un altro non determina un vero e proprio

---

policy challenges, in *Concorrenza e mercato*, 2016, 59; I. GRAEF, J. VERSHAKELEN, P. VALCKE, *Putting the right to data portability into a competition law perspective*, in *Law: The Journal of the Higher School of Economics*, in *Annual Review*, 2013, 53). Sulle origini del diritto alla portabilità, cfr. European Data Protection Supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy – Preliminary Opinion* (March 2014), 15; I. GRAEF, *Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union*, in *Telecommunications Policy*, 2015, 39, 6, 502.

[33] In tal senso, si rinvia alle *Guidelines on the right of data portability* (WP 242), adottate dal WP29 – oggi *European Data Protection Board* – il 13 dicembre 2016, versione emendata e adottata il 5 aprile 2017, secondo cui «l'obiettivo ultimo è accrescere il controllo degli interessati sui propri dati personali....seppure il diritto alla portabilità possa fungere da fattore di promozione della concorrenza fra i singoli servizi proprio perché facilita il passaggio da un servizio all'altro, il Regolamento disciplina il trattamento dei dati personali e non la concorrenza fra imprese».

[34] Si vedano a riguardo A. RICCI, *I diritti dell'interessato*, cit., 219-220; S. TROIANO, *Il diritto alla portabilità dei dati*, cit., 202, ss., il quale individua la novità proprio nella «intrinseca polifunzionalità» della portabilità, uno strumento dalla «qualità ibrida e complessa», che si traduce in «un'irrisolta ambiguità».

trasferimento e non comporta, quindi, la cancellazione dei dati presso il primo titolare. In questo caso, l'interessato esercita, infatti, soltanto il suo diritto di riutilizzare i dati. L'art. 20, par. 4, stabilisce, inoltre, che il diritto alla portabilità dei dati «non deve ledere i diritti e le libertà altrui». Al fine di non pregiudicare i diritti e le libertà di altre persone, il Regolamento prevede, in altri termini, una limitazione dell'oggetto [35]. Dai parr. 1 e 4 dell'art. 20 GDPR, in particolare, si ricava quali dati possano essere «portabili»: si tratta dei dati personali che «riguardano l'interessato» e sono stati «forniti» dall'interessato ad un titolare [36]. L'interpretazione dell'espressione «forniti» viene intesa in senso ampio, per cui il diritto non si limita ai soli dati personali comunicati dall'interessato al titolare del trattamento, ma si estende anche ai dati personali generati dalle attività dell'interessato (es. i dati di localizzazione, la storia delle ricerche, i dati di navigazione, il battito cardiaco registrato da un dispositivo, l'intensità dell'esercizio, la dieta quotidiana e il programma sonno-veglia, spesso raccolti da varie app per il benessere e lo stile di vita o dispositivi indossabili) [37]. I dati creati dal titolare non possono, invece, formare oggetto del diritto alla portabilità,

---

[35] Si veda, in tal senso, A. Ricci, *I diritti dell'interessato*, in G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 223.

[36] Cfr. le Linee guida sul diritto alla portabilità dei dati, cit., 10 ss. Sul punto si veda anche E. Battelli, G. D'Ippolito, *Il diritto alla portabilità dei dati personali*, in E. Tosi (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Lefebvre Giuffrè, 2019, 194 ss.

[37] Il WP29 sottolinea che i «dati forniti dall'interessato» non solo equivalgono a «dati forniti attivamente e consapevolmente dall'interessato», ma comprendono anche «i dati osservati forniti dall'interessato in virtù dell'uso del servizio o del dispositivo». (WP29 (n 16) 9-10). In senso contrario, vedi l'interpretazione restrittiva e più letterale che esclude, invece, i dati osservati: *Centre For Information Policy Leadership*, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability*", 8 (ove si afferma che i dati non forniti attivamente, ma "osservati" rientrerebbero nell'ambito del diritto alla portabilità solo qualora inestricabilmente legati ai primi). Non sono compresi, poi, i dati generati dal titolare sulla base dell'analisi di quelli forniti o raccolti dall'interessato (*inferred and derived data*), proprio perché essi

perché non sono «forniti dall'interessato», anche se possono essere a lui riferiti o riferibili, ma l'interessato può chiedervi l'accesso ai sensi dell'art. 15 del GDPR.[38] Ciò esclude tutte le altre forme di dati personali secondari che sono derivate da ulteriori trattamenti, in particolare, nel settore dei dati sanitari, tutte le forme di dati dedotti, come, ad esempio i risultati di varie forme di analisi che sono state effettuate sui dati originali. Tale limitazione risulta grave ed anacronistica, se si riflette sul fatto che, allo stato attuale, i trattamenti complessi che utilizzano, tra l'altro, varie forme di intelligenza artificiale sono sempre più frequenti e necessari (compreso il settore della salute), e ciò comporta l`esclusione di analisi, deduzioni e conclusioni utili basate su ulteriori elaborazioni di dati che l'interessato aveva originariamente fornito.

---

non sono «forniti direttamente dall'interessato», anche se possono essere a lui riferiti o riferibili.

[38] Ciò fermo restando comunque che i dati dei terzi, pur oggetto di portabilità, non potranno essere utilizzati né dall'interessato, né dall'eventuale nuovo titolare che li riceva, a meno che non vi sia una base specifica, diversa e autonoma, che legittimi il loro trattamento e della quale – ove non coincida col consenso di cui all'art. 6, lett. a) e art. 9 del GDPR – i terzi dovranno essere esplicitamente informati ai sensi dell'art. 14 del GDPR. Cfr. anche G. MALGIERI, *Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data, Privacy, in Germany* – PinG, 2016, 4, 133, 143; G. MALGIERI, *User-provided personal content' in the EU: digital currency between data protection and intellectual property* in IRLCT 2018, 32, 1, 118, 130; B. VAN DER AUWERMEULEN, *How to attribute the right to data portability in Europe: A comparative analysis of legislations*, in *Computer Law & Security Review* 2017, 33, 57, 61. Cfr. G. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali – Il Regolamento europeo 2016/679*, in G. PIZZETTI (a cura di), *I diritti nella "rete" della rete*, Torino, Giappichelli, 2016; cfr. anche R. STOYKOVAR, *The Right to Data Portability. Data protection scope and technical feasibility*, in *Computer Law Review International*, 2018, 3, 65, 67. Per una disamina della classificazione dei dati nelle quattro categorie – *provided data, observed data, derived data e inferred data* – basata non sul grado di "sensibilità" dei dati, né sulla loro modalità di utilizzo, bensì sulla modalità in cui gli stessi originano, vedi, fra i primi, OECD, *Privacy Expert Roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, 21 marzo 2014, disponibile su: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg%282014%293&doclanguage=en.

In raffronto alla disciplina appena evidenziata e relativa al GDPR, nel Regolamento EHDS n. 327/2025 sono inserite importanti innovazioni che, ovviamente, tengono conto della natura dei dati personali oggetto della medesima norma.

Secondo l'art. 7, reg. EHDS, «le persone fisiche hanno il diritto di concedere l'accesso alla totalità o a parte dei loro dati sanitari elettronici personali a un altro prestatore di assistenza sanitaria di loro scelta o di chiedere a un prestatore di assistenza sanitaria di trasmettere la totalità o parte dei loro dati sanitari elettronici a un altro prestatore di assistenza sanitaria di loro scelta immediatamente, gratuitamente e senza ostacoli da parte del prestatore di assistenza sanitaria o dei fabbricanti dei sistemi utilizzati dal prestatore di assistenza sanitaria. Qualora i prestatori di assistenza sanitaria si trovino in Stati membri diversi, le persone fisiche hanno il diritto di chiedere la trasmissione dei loro dati sanitari elettronici personali nel formato europeo di scambio delle cartelle cliniche elettroniche di cui all'articolo 15 attraverso l'infrastruttura transfrontaliera di cui all'articolo 23. Il prestatore di assistenza sanitaria ricevente deve accettare tali dati ed è in grado di leggerli. Le persone fisiche hanno il diritto di chiedere a un prestatore di assistenza sanitaria di trasmettere una parte dei loro dati sanitari elettronici personali a un destinatario chiaramente identificato del settore della sicurezza sociale o dei servizi di rimborso. Tale trasmissione avviene immediatamente, gratuitamente e senza ostacoli da parte del prestatore di assistenza sanitaria o dei fabbricanti dei sistemi utilizzati dal prestatore di assistenza sanitaria ed è solo unidirezionale. Qualora abbiano scaricato una copia elettronica delle loro categorie prioritarie di dati sanitari elettronici personali in conformità dell'articolo 3, paragrafo 2, le persone fisiche sono in grado di trasmettere tali dati ai prestatori di assistenza sanitaria di loro scelta nel formato europeo di scambio delle cartelle cliniche elettroniche di cui all'articolo 15. Il prestatore di assistenza sanitaria ricevente deve accettare tali dati e, se del caso, essere in grado di leggerli» [39].

[39] Sembra seguire la medesima direzione di potenziamento di tale diritto, il *Data Act* (Regolamento Ue n. 2023/2854), avente ad oggetto l'armonizzazione delle norme

L'inclusione esplicita in tale disciplina della portabilità dei dati desunti appare come un'integrazione necessaria anche alla luce della loro utilizzabilità nei *set* di dati necessari per il "*training*" e l'utilizzo dell'intelligenza artificiale. Di più, tali tipi di dati devono essere in un formato interoperabile, vale a dire nel formato europeo di scambio delle cartelle cliniche elettroniche (Cfr. Considerando 15 e articolo 7 dell'EHDS). Qui si nota una rilevante differenza rispetto alla disciplina dell'articolo 20 del GDPR, che non stabiliva un obbligo di «interoperabilità» [40]. Lo stesso WP29 nel proprio parere puntualizzava che i ter-

---

in materia di accesso equo ai dati e al loro utilizzo, che definisce i diritti di accesso ai dati generati dall'uso di prodotti connessi o servizi "universali" e cioè correlati e gestibili da vari dispositivi, nonché le condizioni per il loro uso e per la loro condivisione. Secondo il Considerando 35 del *Data Act*, tale regolamento impone e garantisce la fattibilità tecnica dell'accesso di terzi a tutti i tipi di dati che rientrano nel suo ambito di applicazione, siano essi personali o non personali, assicurando in tal modo che l'accesso a tali dati non sia più ostacolato o impedito da limiti tecnici. Consente inoltre ai titolari dei dati di fissare compensi ragionevoli a carico di terzi, ma non dell'utente, per i costi sostenuti per fornire un accesso diretto ai dati generati dal prodotto connesso dell'utente. Se un titolare dei dati e un terzo non sono in grado di concordare le condizioni di tale accesso diretto, all'interessato non dovrebbe essere in alcun modo impedito di esercitare i diritti di cui al regolamento (UE) 2016/679, compreso il diritto alla portabilità dei dati, esperendo i mezzi di ricorso in conformità a tale regolamento. Anche il Regolamento relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali – *Digital market act*, Regolamento n. 2022/1828) ha inteso dare un impulso maggiore al principio di portabilità dei dati. L'art. 6, comma 9, prevede infatti che i fornitori di servizi di piattaforma di base designati come *gatekeeper*, ovvero "controllori dell'accesso" ai mercati digitali, garantiscano, su richiesta e a titolo gratuito, agli utenti finali e a terzi autorizzati da un utente finale l'effettiva portabilità dei dati forniti dall'utente finale o generati mediante l'attività dell'utente finale nel contesto dell'utilizzo del pertinente servizio di piattaforma di base, anche fornendo a titolo gratuito strumenti per agevolare l'effettivo esercizio di tale portabilità dei dati, nonché fornendo un accesso continuo e in tempo reale a tali dati. In questo modo, viene favorita la commutazione di dati da un fornitore ad un altro (*switching*) ed il collegamento ad una varietà di connessioni o porte dati (*multi-homing*), il che incentiva la competizione tra le grandi piattaforme digitali.

[40] Si consideri che, come sottolineato dal WP29 durante la discussione dell'articolo 20 del GDPR, «la portabilità mira a produrre sistemi interoperabili, non sistemi com-

mini previsti nell'art. 20 GDPR «strutturato», «di uso comune» e «leggibile meccanicamente» sono «un insieme di requisiti minimi che dovrebbero facilitare l'interoperabilità del formato dei dati fornito dal titolare del trattamento» [41]. Se tali tre mezzi sono obbligatori nel GDPR, il risultato dell'interoperabilità è, in realtà, solo suggerito [42].

---

patibili». Cfr. *Article 29 Data Protection Working Party (WP29), Guidelines on the right to data portability'* (2017) 17), adottate il 13 dicembre 2016, emendate e adottate il 5 aprile 2017, consultabile su *http://ec.europa.eu*. Sulla differenza tra interoperabilità (dei dati, dei sistemi, ecc.) e compatibilità, cfr. anche *http://www.testingstandards.co.uk/interop_et_al.htm*. La compatibilità comporterebbe l'obbligo per il responsabile del trattamento di garantire che i dati forniti siano (appunto) direttamente compatibili con le finalità e i sistemi di trattamento previsti dal nuovo responsabile del trattamento proposto (al quale i dati devono essere trasmessi). Ciò rappresenterebbe un onere pesante (se non impossibile da sostenere) che ricadrebbe quasi interamente sul titolare del trattamento originario, che dovrebbe garantire la compatibilità dei dati con qualsiasi sistema di elaborazione utilizzato dal nuovo controllore. Un siffatto obbligo fungerebbe probabilmente da deterrente per il trattamento dei dati in generale, dato che i responsabili del trattamento dovrebbero assicurarsi di avere la capacità (in termini di personale e di competenze tecniche) di apportare tali modifiche qualora fossero richieste. Cfr., in tal senso, W. Li, P. Quinn, *The European Health Data Space: An expanded right to data portability?*, in *Computer Law & Security Review*, V. 52, 2024, 105913, consultabile in https://doi.org/10.1016/j.clsr.2023.105913. Rispetto alla «compatibilità», l'«interoperabilità» rappresenta una soglia inferiore e, di conseguenza, comporta un onere minore per il responsabile del trattamento originario, essendo stata definita dalla Commissione europea come «la capacità di organizzazioni disparate e diverse di interagire verso obiettivi comuni reciprocamente vantaggiosi e concordati, che comportano la condivisione di informazioni e conoscenze tra le organizzazioni, attraverso i processi aziendali che supportano, mediante lo scambio di dati tra i rispettivi sistemi ICT». Cfr., a riguardo, European Commission, Directorate-General for Informatics, *European interoperability framework (EIF): towards interoperability for European public services, 2*011, in https://data.europa.eu/doi/10.2799/17759. Secondo l'art. 2, lett. f, Reg. EHDS, per interoperabilità si intende la capacità delle organizzazioni, nonché delle applicazioni *software* o dei dispositivi dello stesso fabbricante o di fabbricanti diversi, di interagire tra loro attraverso i processi che supportano, il che comporta lo scambio di informazioni e conoscenze tra tali organizzazioni, applicazioni *software* o dispositivi, senza che sia modificato il contenuto dei dati.

[41] Cfr. WP29 (n 16) 17

[42] Cfr. P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez,

Di più, l'interessato ha il diritto di chiedere il trasferimento diretto a un altro titolare del trattamento ove «tecnicamente fattibile». (art. 20, par. 2, del GDPR).

Tuttavia, anche in contrasto con tale atteggiamento del GDPR, l'EHDS, come visto, impone un obbligo esplicito ai produttori (e agli importatori) di sistemi EHR di garantire l'interoperabilità dei medesimi [43].

Nel regolamento EHDS, un altro aspetto fondamentale è stato innovato. La portabilità non è limitata ai soli dati trattati sulla base del consenso o di un contratto sottostante, come stabilito ai sensi dell'art. 20 del Regolamento (UE) 2016/679. Infatti, secondo tale norma, sono oggetto di portabilità solo i dati trattati dopo aver ottenuto il consenso (esplicito) dell'interessato o, in alternativa, se il trattamento è stato «necessario per l'esecuzione di un contratto di cui l'interessato è parte o per l'esecuzione di misure precontrattuali adottate su richiesta dell'interessato». Secondo il regolamento EHDS, invece, tale diritto dovrà applicarsi ai dati sanitari elettronici trattati da titolari del trattamento pubblici o privati [44], a prescindere dalla base giuridica per il

---

The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services, in *Computer Law & Security Review*, 2018, 193

[43] Tali requisiti sono stabiliti nell'allegato II del Regolamento come parte dei «requisiti essenziali» per i sistemi EHR. La Commissione europea sarà inoltre incaricata di elaborare «specifiche comuni», comprese le specifiche tecniche, per l'interoperabilità dei sistemi EHR. In particolare, i pazienti potranno accedere e condividere i dati tramite il sistema che memorizzerà ovunque in Europa i dati sanitari digitali (la cosiddetta "cartella clinica elettronica" – EHR). La mancanza di standardizzazione e interoperabilità tra i diversi sistemi sanitari nazionali rappresenta una delle principali sfide nell'implementazione dell'*European Health Data Space* (EHDS), poiché senza di essa si possono verificare discrepanze nei dati sanitari raccolti dai diversi sistemi nazionali, compromettendo la qualità e l'affidabilità delle informazioni disponibili. Ciò può aumentare il rischio di errori di diagnosi, decisioni cliniche sbagliate e inefficienze nel sistema sanitario e può rendere più difficile garantire la sicurezza e la privacy dei dati sanitari condivisi nell'EHDS.

[44] Questo ampliamento dell'ambito di applicazione oggettiva ha il sapore quasi di una rivoluzione copernicana, se si valuta che il Considerando n. 68 del GDPR, invece, precisa che «per sua stessa natura, tale diritto non dovrebbe essere esercitato

trattamento dei dati. Pertanto, sembra potersi affermare che il diritto alla portabilità non provenga più solo da un atto negoziale, che sottenda un rapporto giuridicamente rilevante di natura patrimoniale avente ad oggetto il dato personale, diritto che potrebbe essere, quindi, esercitato solo nell'ambito di una relazione interindividuale [45], o se il con-

---

nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche. Non dovrebbe pertanto applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento». La Commissione non accolse, del resto, il suggerimento dell'*European Data Protection Supervisor* di far coincidere l'ambito di copertura del diritto di accesso e quello di portabilità, stabilendo dunque di limitare quest'ultimo ai soli casi di consenso e contratto (Cfr.: EDPS, *Opinion 3/2015 (with addendum) Europe's big opportunity – EDPS recommendations on the EU's options for data protection reform*, (9 October 2015), 12 (nota 34). In materia, cfr. anche EDPB, *Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati*, (8 ottobre 2019), in https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_it.pdf. Cfr., anche Shah-Khan, *Secondary Use of Electronic Health Record: Opportunities and Challenges* (2020), in *IEEE Access,* consultabile in Doi 10.1109/ACCESS.2020.3011099; G. Bincoletto, *A Data Protection by Design Model for Privacy Management in Electronic Health Records,* 161 ss. in M. Naldi, G.F. Italiano, K. Rannenberg, M. Medina, A. Bourka, *Privacy Technologies and Policy,* Berlino, Springer, 2019).

[45] Cfr. V. Ricciuto, *L'equivoco della* privacy. *Persona vs dato personale,* Napoli, ESI, 2022, 137 ss.; G. Versaci, *La contrattualizzazione dei dati personali dei consumatori,* Napoli, ESI, 2020, *passim*; S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali,* Milano, *Ledizioni,* 2018; I. Speziale, *L'ingresso dei dati personali nella prospettiva causale dello scambio: i modelli contrattuali di circolazione,* in *Contratto e impresa*, 2021, 602 e ss. In argomento, vedi pure E. Tosi, *Circolazione dei dati personali tra contratto e responsabilità,* Milano, Lefebvre Giuffrè, 2023, 78 ss. Secondo V. Ricciuto, *L'equivoco della privacy,* cit. 137 ss., che però si riferisce alla disciplina del GDPR, prova della natura giuridica «contrattuale» del diritto alla portabilità nel rapporto tra interessato e titolare è che il contratto sottoscritto con l'interessato fa sorgere l'obbligo del titolare del trattamento (ex art. 20 del GDPR) di trasferire, su richiesta dell'interessato, i dati di quest'ultimo ad un secondo titolare. In una prospettiva, dunque, che sarebbe ben diversa da quella extracontrattuale e,

senso al trattamento si collochi fuori dal contratto, da un atto giuridico, di carattere autorizzatorio, del quale la legge stabilirà i caratteri e gli effetti che rendono lecita l'operazione che abbia ad oggetto i dati personali. Laddove le basi giuridiche siano altre, come ora previsto dal regolamento EHDS, la fonte dell'obbligazione a carico del titolare dei dati di rendere portabili i dati sanitari dell'interessato non potrà che essere il fatto della ricezione originaria dei dati da parte del titolare dei dati, fatto che obbliga, secondo la norma, il medesimo a trasferire tali dati ad altro soggetto su richiesta dell'interessato. In maniera meramente descrittiva, si potrà affermare che tale obbligazione (perché pur sempre di obbligazione si tratta) derivi dalla legge, considerato che, in questo caso, lo scopo della norma (l'art. 20 reg. EHDS) è tutelare un diritto garantito e, direi, costituzionalmente rilevante (ex art. 2 e 32 della Costituzione), quale quello di poter controllare i propri dati sanitari, in linea con il principio di autodeterminazione informativa [46]. Ed in caso di inadempimento di tale obbligazione, dato il ruolo

---

invece, tutta interna a pretese originate da una fattispecie negoziale. Al di là dell'evidente fenomeno circolatorio del dato, è chiaro per l'Autore che una pretesa siffatta, che impone al titolare di un trattamento l'esecuzione della prestazione a soddisfazione dell'interessato (qual è l'interesse a fornire dati personali ad un secondo titolare) è pienamente riconducibile alla nozione di obbligazione (art.1174 c.c.). In senso contrario, pare essere M. GIORGIANNI, *Il «nuovo» diritto alla portabilità dei dati personali. Profili di diritto comparato*, in *Contratto e impresa*, 2019, 1387 ss., secondo cui il legislatore europeo ha voluto tutelare, con la norma in esame, non tanto la «libera circolazione dei dati personali», quanto piuttosto la persona dell'interessato, prevedendo in modo espresso un «controllo sulla circolazione dei dati personali». La conferma si avrebbe, innanzitutto, da un punto di vista sistematico, per la scelta della sua collocazione all'interno del Regolamento fra i «diritti dell'interessato», che sono diretti a conferire maggiori poteri all'individuo.

[46] La Suprema Corte (cfr. Cass. civ. Sez. I, Ord., 27 marzo 2020, n. 7559, in *Danno e Responsabilità*, 2020, 6, 732, nota di NAPOLITANO), ha espressamente chiarito che il principio dell'autodeterminazione informativa corrisponde ad un "potere" dell'interessato di controllare i propri dati consapevolmente, che trova il suo fondamento primo, per diritto nazionale, nella norma dell'art. 2 della Costituzione, e che ha spazio concettuale e operativo distinto dal diritto alla riservatezza, che si collega invece alla tutela dell'intimità della propria vita contro ingerenze esterne.

che ricopre il titolare dei dati, ente pubblico con funzioni di carattere sanitario, e la relazione previamente creatasi con l'interessato, potrà individuarsi, a carico del primo, una responsabilità da contatto sociale o quantomeno da inadempimento di un'obbligazione, sempre ai sensi dell'art. 1218 c.c., con relativa disciplina in ordine al riparto probatorio e al termine prescrizionale decennale [47].

Per quanto riguarda l'ambito di applicazione soggettiva della disciplina, va segnalato che l'art. 7 del Regolamento EHDS limita l'obbligo di ricevere e soddisfare una richiesta di trasferimento dei dati di una persona fisica ai soli prestatori di assistenza sanitaria. Ciò sembra restringere l'applicazione del diritto alla portabilità ad una parte dei potenziali titolari dei dati e può creare dubbi interpretativi [48].

---

[47] Mi si consenta, per approfondimenti a riguardo, il rinvio a S. Faillace, *La responsabilità da contatto sociale*, Padova, Cedam, 2004, *passim* e, da ultimo, a Id., *La controversa categoria delle obbligazioni ex lege*, Milano, Wolters Kluwer, 2023, 190 ss.

[48] Cfr., a riguardo, il parere congiunto emesso dal Comitato europeo per la protezione dei dati (EDPB) e dal Garante europeo della protezione dei dati (GEPD), che ha già sottolineato ciò. Cfr., in tal senso, EDPB-EDPS, *Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*, in https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf. Cfr. anche Terzis *Compromises and Asymmetries in the European Health Data Space,* 2022, in *European Journal of Health Law,* 2022, 345 ss., consultabile *online*, doi: 10.1163/15718093-bja10099. Tre esempi possono essere proposti per illustrare le ambiguità che si creano a riguardo. Il primo concerne le imprese e i servizi che non sono strettamente assistenziali, ma più orientati al benessere: quali quelle che forniscono consigli nutrizionali. In molti Stati membri, non si riconosce che tali servizi rientrino nella definizione di pratica medica (i nutrizionisti possono, ad esempio, non avere qualifiche formali come i professionisti medici). Il secondo tipo è relativo ad applicazioni, servizi o prodotti digitali commerciali che, pur non rientrando nel concetto di assistenza sanitaria, sono collegati ad essa, visto che i dati utilizzati (ad esempio, i dati genetici per servizi di genealogia *on line*) possono essere usati anche per scopi sanitari. Tali servizi possono richiedere un uso intensivo dei dati (sia per quanto riguarda i dati di *input* che richiedono, sia per i dati dedotti che generano). Allo stato attuale, sembra che tali ambiti non rientrino nell'ambito del «settore sanitario o sociale», il che significa che le persone fisiche non potrebbero invocare un diritto alla portabilità per trasferire i loro dati a soggetti che svolgono tali attività.

Va poi considerato, per converso, che i dati ammissibili alla richiesta di portabilità dovrebbero derivare da attività rientranti nell'uso primario ed essere trasmessi ad un soggetto anch'esso rientrante nella medesima area. Ciò si evince dal modo in cui il termine «destinatario dei dati» è definito come rientrante nel contesto dell'uso primario (cfr. art. 7, comma 3, reg. EHDS). Un approccio così restrittivo appare però infelice, in quanto è apparentemente in contrasto con l'obiettivo generale dell'EHDS di migliorare il controllo individuale sui propri dati sanitari elettronici e di facilitare l'uso secondario di questi dati attraverso i meccanismi proposti. Infatti, si consideri che il Regolamento EHDS prevede disposizioni per l'attuazione dell'altruismo dei dati nel settore sanitario [49]. E il diritto alla portabilità dei dati può sembrare, almeno ad una prima analisi, uno strumento idoneo per l'interessato a trasferire efficacemente i dati dal titolare del trattamento ad un'organizzazione per l'altruismo dei dati o a un istituto di ricerca in conformità con le proprie preferenze. Ma, il regolamento EHDS, come visto, limita i trasferimenti basati sulla richiesta di portabilità dei dati al settore sanitario e assistenziale, mentre le finalità di ricerca non sembrano essere incluse, in tale definizione. Pertanto, le finalità di ricerca potranno essere assolte solo attraverso i meccanismi previsti

---

Un terzo esempio riguarda le potenziali richieste di trasferimento di dati dalle cartelle cliniche elettroniche agli istituti di ricerca che conducono ricerche scientifiche in ambito sanitario. Si potrebbe immaginare che individui motivati (ad esempio, cittadini scienziati) possano voler proattivamente trasferire i loro dati verso determinati istituti di ricerca (cioè, in effetti, aggirando la necessità per tali istituzioni di presentare nuove domande attraverso gli Organismi di accesso ai dati sanitari).

[49] È stato il *Data governance act* a definire per la prima volta giuridicamente il termine «altruismo dei dati». È interessante notare che tale Regolamento europeo non usa il termine «donazione» e il richiamo a tale istituto pare sia stato deliberatamente evitato dal legislatore, in quanto implica il trasferimento di proprietà, mentre il diritto fondamentale alla protezione dei dati personali non può essere ceduto. Il concetto di altruismo dei dati sottende un consenso volontario e proattivo degli interessati all'uso dei loro dati per obiettivi di interesse generale, come la ricerca scientifica o il miglioramento dei servizi pubblici. In argomento, si rimanda a BRAVO, *Il principio di solidarietà tra data protection e data governance*, in *Diritto dell'informazione e dell'informatica*, 2023, 481 ss.

dal Regolamento EHDS per l'uso secondario dei dati sanitari (oggetto di approfondimento nei prossimi paragrafi), vale a dire per mezzo di apposita autorizzazione pubblicistica.

4. *L'ambito di applicazione oggettivo e soggettivo della disciplina in ordine all'uso secondario dei dati sanitari*

Il regolamento EHDS, come ricordato, mira a istituire un meccanismo comune per l'accesso ai dati sanitari elettronici per uso secondario in tutta l'Unione europea, meccanismo comune, se pur non esclusivo, considerato che l'art. 1, paragrafo 8, del Regolamento stabilisce, in parte vanificandone la portata generale, che tale disciplina «lascia impregiudicato l'accesso ai dati sanitari elettronici per l'uso secondario concordato nel quadro di accordi contrattuali o amministrativi tra soggetti pubblici o privati». [50]

Secondo la definizione di cui all'art. 2, Reg. EHDS, per «uso secondario dei dati sanitari elettronici», si intende il trattamento dei dati sanitari elettronici per le finalità di cui al capo IV del presente regolamento, finalità diverse da quelle iniziali per le quali sono stati raccolti o prodotti. L'aggregazione di dati sanitari in *pool* di dati più ampi a livello nazionale e dell'UE facilita l'estrazione di nuove informazioni sui prodotti sanitari, sui servizi e sulle prestazioni dei fornitori di servizi, informazioni che non possono essere ottenute da *set* di dati frammentati, e soprattutto promuove l'innovazione nei servizi sanitari, creando un mercato dei servizi più trasparente che stimola la concorrenza. L'accesso ai dati per uso secondario dovrebbe quindi contribuire all'interesse generale della società, in particolare, per lo sviluppo di nuovi medicinali, dispositivi medici, prodotti e servizi sanitari a prezzi

[50] Vedi, in argomento, C. Perlingieri, *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici*, cit., 492 ss. S. Corso, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, in *Le nuove leggi civili commentate*, 2025, 577.

equi e accessibili per i cittadini dell'Unione, e dovrebbe migliorare l'accesso a tali prodotti e servizi e la loro disponibilità in tutti gli Stati membri (Considerando n. 41, Reg. EHDS).

Nello scenario progettato dal legislatore europeo, i titolari dei dati devono mettere a disposizione i dati in loro possesso sulla base di un'autorizzazione o di una richiesta [51]. E ciò in antitesi rispetto a quan-

[51] A tal proposito, il Considerando n. 59 del Reg. EHDS ricorda, che «i soggetti pubblici o privati ricevono spesso finanziamenti pubblici, da fondi nazionali o dell'Unione, per raccogliere e trattare dati sanitari elettronici per la ricerca, le statistiche sia ufficiali che non ufficiali, o altre finalità simili, anche in ambiti in cui la raccolta di tali dati è frammentata o difficile, quali quelli relativi alle malattie rare o al cancro. Tali dati, raccolti e trattati dai titolari dei dati sanitari con il sostegno di finanziamenti pubblici nazionali o dell'Unione, dovrebbero essere messi a disposizione degli organismi responsabili dell'accesso ai dati sanitari al fine di massimizzare l'impatto dell'investimento pubblico e sostenere la ricerca, l'innovazione, la sicurezza dei pazienti o la definizione delle politiche, a beneficio della società..». Al considerando n. 55, si rileva che, nel contesto dello spazio europeo dei dati sanitari, i dati sanitari elettronici esistono già e sono raccolti, tra gli altri, da prestatori di assistenza sanitaria, associazioni professionali, istituzioni pubbliche, regolatori, ricercatori e assicuratori nel corso delle loro attività. Tali dati dovrebbero essere resi disponibili anche per l'uso secondario, vale a dire per il trattamento di dati per finalità diverse da quelle per le quali sono stati raccolti o prodotti; tuttavia, ciò non avviene. Al fine di sfruttare pienamente i benefici derivanti dall'uso secondario, tutti i titolari di dati sanitari dovrebbero invece contribuire rendendo disponibili per l'uso secondario le differenti categorie di dati sanitari elettronici in proprio possesso, purché tale sforzo avvenga tramite processi efficaci e sicuri, nel debito rispetto degli obblighi professionali, quali quello di riservatezza. Si consideri che il regolamento EHDS n. 327/2025 obbliga le autorità sanitarie pubbliche e private a mettere i dati sanitari a disposizione delle imprese commerciali private per un uso secondario, ma non predispone alcun obbligo corrispondente alle imprese commerciali di rendere disponibili i propri dati. Questo approccio rischia di esacerbare le asimmetrie informative tra le imprese commerciali e il settore pubblico. Si veda, invece, l'art. 14 del *Data Act* (Regolamento europeo sull'accesso equo ai dati e sul loro utilizzo n. 2854/2023), che, nel rivolgersi ai fabbricanti di prodotti connessi immessi sul mercato dell'Unione europea e ai fornitori di servizi correlati, indipendentemente dal loro luogo di stabilimento, prevede l'obbligo in capo ai titolari dei dati di mettere i medesimi dati a disposizione di enti pubblici, della Commissione europea, della Banca centrale europea e degli

to previsto nel DGA, che non crea un obbligo per gli enti pubblici di mettere a disposizione i dati, limitandosi ad un'esortazione decisa [52].

Per quel che concerne l'ambito di applicazione soggettiva di tale normativa, va considerato che la definizione di titolare dei dati, secondo l'articolo 2, par. 2 lett. t) EHDS, si differenzia da quella di cui al GDPR, oltre che da quella di cui al *Data governance act* e di cui al *Data Act* [53]. Viene, infatti, in tale sede, definito in maniera pletorica e sovrabbondante,

---

organismi dell'Unione che ne facciano motivata richiesta, enunciando, al capo V, le condizioni al verificarsi delle quali può dirsi sussistente una necessità eccezionale, come tale limitata nel tempo e nella portata, di utilizzare determinati dati per finalità di pubblico interesse, a favore di enti pubblici e istituzioni, agenzie e organismi dell'Unione. Il dovere di cui all'art. 14 del suddetto regolamento non rappresenta tuttavia un obbligo generalizzato, ma è previsto in caso di emergenza pubblica e l'ente pubblico, la Commissione, la Banca centrale europea o l'organismo dell'Unione non sia in grado di procurarsi i dati necessari per fronteggiarla, prevenirla o favorire la ripresa con mezzi alternativi, in modo tempestivo ed efficace. In argomento, vedi A. Ricci, *Introduzione al Regolamento europeo sull'accesso equo ai dati e sul loro utilizzo*, in *Le Nuove Leggi Civili Commentate*, 2024, 799; A Morace Pinelli, *Data Act (reg. UE 2023/2854): la circolazione dei dati nell'interesse privato e generale*, in *Nuova giurisprudenza civile commentata*, 2025,1, 218.

[52] Il DGA si limita a stabilire le condizioni, ad esempio le tariffe che possono essere addebitate e le tempistiche per la fornitura dei dati. L'ambito dei destinatari è peraltro diverso: il capo II della DGA si applica agli enti pubblici di tutti i settori (con alcune eccezioni), mentre l'EHDS si applica ai titolari di dati sanitari, che possono essere sia enti pubblici che soggetti del settore privato.

[53] Secondo l'art. 2 del Regolamento (UE) 2023/2854, conosciuto come *Data Act*, pubblicato in GUUE in data il 22 dicembre 2023, norma che disciplina la condivisione dei dati generati dall'uso di prodotti connessi o di servizi correlati (ad esempio, l'internet delle cose e i macchinari industriali) e consentirà agli utenti di accedere e verificare i dati che generano, il titolare è «una persona fisica o giuridica che ha il diritto o l'obbligo, conformemente al presente regolamento, al diritto applicabile dell'Unione o alla legislazione nazionale adottata conformemente al diritto dell'Unione, di utilizzare e mettere a disposizione dati, compresi, se concordato contrattualmente, dati del prodotto o di un servizio correlato che ha reperito o generato nel corso della fornitura di un servizio correlato». Secondo l'art. 2 del *Data Governance act*, per titolare dei dati si intende «una persona giuridica, compresi gli enti pubblici e le organizzazioni internazionali, o una persona fisica che non è l'interessato rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o

«titolare dei dati sanitari», una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo del settore dell'assistenza sanitaria o delle cure assistenziali, compresi, ove necessario, i servizi di rimborso, nonché una persona fisica o giuridica che sviluppi prodotti o servizi destinati al settore sanitario, dell'assistenza sanitaria o delle cure assistenziali, sviluppi o fabbrichi applicazioni per il benessere [54], svol-

---

nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli».

[54] L'aspirazione dell'UE di includere i sistemi di benessere nell'EHDS può essere vista come il riconoscimento di un elemento di trasformazione della medicina moderna. Come affermato in S. GILBERT, K. BACA-MOTES, G. QUER, M. WIEDERMANN, D. BROCKMANNAND, *Citizen Data Sovereignty Is Key to Wearables and Wellness Data Reuse for the Common Good* (2024) 7 npj Digital Medicine, l'EHDS si basa sulla premessa che la salute e i dati sulla salute non iniziano dal cancello della clinica e i dati sul benessere descrivono, in dettagli, la salute degli individui. Ciò contribuisce allo spostamento del baricentro, lontano dal perimetro della clinica e verso il divano, la tasca, il polso e il cerotto cutaneo del cittadino. A condizione che si trovino approcci accettabili e praticabili per collegare questi dati ai dati personali delle cartelle cliniche elettroniche, non solo si può aumentare la comprensione della medicina, ma anche la sviluppo di nuovi approcci per l'assistenza medica e preventiva, per una migliore salute pubblica e per l'erogazione di cure mediche. Per sostenere questa trasformazione, i dati sul benessere sono stati inclusi nel regime di uso secondario e sono state prescritte regole di etichettatura e interoperabilità delle applicazioni per il benessere. Secondo l'art. 48 reg. EHDS, l'interoperabilità di tali applicazioni con i sistemi di cartelle cliniche elettroniche non implica la condivisione o la trasmissione automatica di tutti questi dati sanitari con il sistema di cartelle cliniche elettroniche. La condivisione o la trasmissione di tali dati è possibile solo se conforme all'articolo 5 e previo consenso della persona fisica interessata e l'interoperabilità è limitata esclusivamente ai fini della condivisione e della trasmissione. I fabbricanti di applicazioni per il benessere che dichiarano l'interoperabilità con un sistema di cartelle cliniche elettroniche garantiscono che la persona fisica interessata possa scegliere quali categorie dei dati sanitari dell'applicazione per il benessere inserire nel sistema di cartelle cliniche elettroniche e le circostanze per la loro condivisione o trasmissione. In ordine alle sovrapposizioni e le questioni di coordinamento applicabili nel caso dell'IoT medico, indagando su cosa accadrà quando i dati generati dall'IoT saranno condivisi per creare nuovi prodotti o servizi secondo il quadro ora delineato dal *Data Act* e dallo Spazio europeo dei dati sanitari, vedi F. CASAROSA, F. GENNARI, *Data Sharing in the Internet of Medical Things: Between the Data Act and the EHDS*, in *Giornale*

ga attività di ricerca in relazione al settore dell'assistenza sanitaria o delle cure assistenziali o funga da registro della mortalità, nonché un'istituzione, un organo o un organismo dell'Unione che abbia: i) il diritto o l'obbligo, conformemente al diritto dell'Unione o nazionale applicabile e in qualità di titolare o contitolare del trattamento, di trattare dati sanitari elettronici personali per la prestazione di assistenza sanitaria o cure assistenziali o a fini di sanità pubblica, rimborso, ricerca, innovazione, definizione delle politiche, statistiche ufficiali o sicurezza dei pazienti o a fini di regolamentazione; o ii) la capacità di rendere disponibili dati sanitari elettronici non personali, mediante il controllo della progettazione tecnica di un prodotto e dei servizi correlati, anche in termini di registrazione, fornitura, limitazione dell'accesso o scambio.

In sintesi, i titolari dei dati sanitari, nel contesto dell'uso secondario dei dati sanitari elettronici, dovrebbero pertanto essere i fornitori di servizi sanitari o di assistenza o svolgere attività di ricerca nei settori dell'assistenza sanitaria o sviluppare prodotti o servizi destinati a tale settore. In linea con tale definizione, pure soggetti privati quali le case di cura, i centri diurni, coloro che forniscono servizi alle persone con disabilità, le attività commerciali e tecnologiche connesse all'assistenza, come l'ortopedia e le aziende che forniscono servizi di assistenza dovrebbero essere compresi in tale categoria. Pure le persone giuridiche che sviluppano applicazioni per il benessere dovrebbero essere titolari di dati sanitari, così le istituzioni, gli organi o gli organismi dell'Unione che trattano le categorie di dati sanitari [55]. Gli Stati membri dovranno determinare quali titolari di dati di enti pubblici e privati

---

europeo della regolamentazione dei rischi, 2025, 1-23, consultabile al seguente link: https://doi.org/10.1017/err.2025.18

[55] Ai sensi dell'art. 50 reg. EHDS, al fine di evitare un onere sproporzionato a loro carico, di norma le persone fisiche, compresi i singoli ricercatori e le microimprese dovrebbero essere esentate dagli obblighi dei titolari di dati sanitari. Gli Stati membri hanno tuttavia la possibilità di estendere gli obblighi dei titolari di dati sanitari a tali categorie. Al fine di ridurre gli oneri amministrativi e alla luce dei principi di efficacia ed efficienza, gli Stati membri dovrebbero poter richiedere nel loro diritto nazionale che, per talune categorie di titolari di dati sanitari, le funzioni siano svolte da entità di intermediazione di dati sanitari. Tuttavia, la possibilità per gli Stati

del settore sanitario o assistenziale (ad eccezione delle microimprese) saranno obbligati a rendere disponibili quindici categorie di dati, anche se protetti da diritti di proprietà intellettuale e segreti commerciali (articolo 33(4) EHDS), inclusi EHR e dati genetici [56]. A ben vedere, si tratta di una vera e propria obbligazione prevista dal Regolamento a carico dei titolari dei dati per i fini superiori della sanità pubblica nazionale e sovranazionale, obbligazione che, se inadempiuta, porterà a conseguenze di cui si discuterà nel prosieguo.

Alla definizione di «titolare dei dati», francamente troppo estesa, ne corrisponde una altrettanto ampia dell' «utente dei dati sanitari», indicato come una persona fisica o giuridica, comprese le istituzioni, gli organi o gli organismi dell'Unione, cui è stato concesso l'accesso legittimo ai dati sanitari elettronici ai fini dell'uso secondario in virtù di un'autorizzazione ai dati, di un'approvazione di una richiesta di dati sanitari o di un'approvazione di accesso da parte di un partecipante autorizzato alla piattaforma DatiSanitari@UE (HealthData@EU) (reg. EHDS art. 2 lett. u).

È prevista poi l'istituzione di uno o più organismi per l'accesso ai dati sanitari, che sostengano l'accesso ai dati sanitari elettronici negli Stati membri. Si tratta di una componente essenziale per promuovere l'uso secondario dei dati sanitari. Nel contesto dello Spazio economico europeo, si prevede, inoltre, la creazione di una struttura centralizzata, DatiSanitari@UE (HealthData@EU), che svolgerà il ruolo di intermediario tra i diversi organismi degli stati membri di accesso ai dati sanitari [57].

---

membri di modificare tale esonero mediante normative nazionali introduce un elemento di frammentazione potenziale all'interno dell'Unione Europea.

[56] Secondo il Considerando n. 60 reg. EHDS, i dati sanitari elettronici protetti da diritti di proprietà intellettuale o segreti commerciali, compresi i dati relativi a sperimentazioni cliniche, indagini e studi, possono essere molto utili per l'uso secondario e possono promuovere l'innovazione all'interno dell'Unione a beneficio dei pazienti dell'Unione. Tali dati dovrebbero essere resi disponibili per quanto possibile, adottando nel contempo tutte le misure necessarie per proteggere i diritti di proprietà intellettuale e i segreti commerciali.

[57] Ai sensi dell'art. 75 EHDS, ciascuno Stato membro designa un punto di con-

Secondo l'art. 61 reg. EHDS, gli utenti dei dati sanitari possono accedere ai dati sanitari elettronici di cui all'articolo 51 e trattarli per l'uso secondario solamente sulla base di un'autorizzazione ai dati rilasciata a norma dell'articolo 68 o di una richiesta di dati sanitari approvata a norma dell'articolo 69 o, nelle situazioni di cui all'articolo 67, paragrafo 3, di un'approvazione dell'accesso da parte del pertinente partecipante autorizzato a DatiSanitari@UE (HealthData@EU). Gli utenti dei dati sanitari devono rendere pubblici i risultati o gli esiti dell'uso secondario, comprese le informazioni pertinenti per la prestazione di assistenza sanitaria, entro 18 mesi dal completamento del trattamento dei dati sanitari elettronici nell'ambiente di trattamento sicuro o dal ricevimento della risposta alla richiesta di dati sanitari.

Gli organismi per l'accesso ai dati sanitari [58] decidono di concedere l'accesso ai dati sanitari elettronici, ai sensi dell'art. 68 reg. EHDS solo

---

tatto nazionale per l'uso secondario. Il punto di contatto nazionale per l'uso secondario è uno sportello organizzativo e tecnico, che permette la messa a disposizione dei dati sanitari elettronici per l'uso secondario in un contesto transfrontaliero e ne ha la responsabilità. Il punto di contatto nazionale per l'uso secondario può essere l'organismo responsabile dell'accesso ai dati sanitari che funge da coordinatore a norma dell'articolo 55, paragrafo 1. Il servizio di accesso ai dati sanitari dell'Unione funge da punto di contatto delle istituzioni, degli organi e degli organismi dell'Unione per l'uso secondario ed è responsabile della messa a disposizione dei dati sanitari elettronici per l'uso secondario. I punti di contatto nazionali per l'uso secondario di cui al paragrafo 1 e il servizio di accesso ai dati sanitari dell'Unione di cui al paragrafo 2 si connettono all'infrastruttura transfrontaliera per l'uso secondario, vale a dire DatiSanitari@UE (HealthData@EU). I punti di contatto nazionali per l'uso secondario e il servizio di accesso ai dati sanitari dell'Unione agevolano l'accesso transfrontaliero ai dati sanitari elettronici per l'uso secondario di diversi partecipanti autorizzati a DatiSanitari@UE (HealthData@EU).

[58] Una rilevante esperienza pratica in materia può essere rinvenuta all'interno di organismi nazionali esistenti, come l'autorità finlandese per il rilascio dei dati sociali e sanitari Findata, l'LNDS lussemburghese o l'*Health Data Hub* francese, ma anche infrastrutture regionali avanzate come quelle realizzate in Spagna e Svezia. Tali esempi potrebbero essere determinanti per lo sviluppo di un quadro di *governance* comune praticabile per l'EHDS e fornire modelli per consentire ad altri Stati membri di sviluppare le loro infrastrutture e processi nazionali per l'uso secondario.

se sono soddisfatti i seguenti criteri cumulativi: la finalità descritta nella domanda di accesso ai dati corrisponde ad una o più delle finalità considerate lecite dal regolamento EHDS *ex* art. 53; i dati richiesti sono necessari, adeguati e proporzionati alle finalità descritte nella domanda di accesso ai dati sanitari, tenendo conto delle disposizioni relative alla minimizzazione dei dati e alla limitazione delle finalità; il trattamento è in linea con l'art. 6, par. 1, del reg. (UE) 2016/679, e, nel caso di dati pseudonimizzati, vi deve essere una giustificazione sufficiente per il fatto che la finalità non sia conseguibile con dati anonimizzati; il richiedente deve essere qualificato per quanto riguarda le finalità previste per l'uso dei dati e deve possedere competenze adeguate, comprese qualifiche professionali nei settori dell'assistenza sanitaria, dell'assistenza, della sanità pubblica, della ricerca, in linea con la prassi etica e le disposizioni legislative e regolamentari applicabili; il richiedente deve dimostrare misure tecniche e organizzative sufficienti per prevenire l'uso improprio dei dati sanitari elettronici e per tutelare i diritti e gli interessi del titolare dei dati e delle persone fisiche interessate; le informazioni sulla valutazione degli aspetti etici del trattamento, se del caso, sono in linea con il diritto nazionale. Se i requisiti per il rilascio di un'autorizzazione ai dati non sono soddisfatti, ma sono soddisfatti i requisiti per fornire una risposta in formato statistico anonimo [59], allora l'organismo per l'accesso ai dati sanitari potrà decidere di fornirla in tale formato, sempre che il richiedente i dati sanitari accetti tale modifica della procedura.

Gli organismi responsabili di accesso ai dati sanitari (Cfr. gli articoli 66 e 67 reg. EHDS) decidono in merito alle domande di accesso ai dati, determinando se i dati debbano essere resi accessibili in forma anonimizzata o pseudonimizzata, sulla base di una valutazione approfondita dei motivi addotti dal richiedente [60]; poi, a loro volta, tali or-

[59] Ai sensi dell'art. 69 reg. EHDS, infatti, il richiedente può presentare una richiesta di dati sanitari al fine di ottenere una risposta solo in formato statistico anonimizzato.

[60] Secondo il Considerando n. 72, data la sensibilità dei dati sanitari elettronici, è

ganismi richiedono i dati sanitari elettronici ai titolari; trattano i dati sanitari elettronici, comprese la combinazione, la preparazione, l'anonimizzazione e la pseudonimizzazione e la divulgazione di tali dati per l'uso secondario, garantendo altresì un'adeguata sicurezza dei medesimi, monitorano e vigilano sul rispetto delle prescrizioni stabilite nel regolamento da parte degli utenti e dei titolari di dati sanitari; e mettono i dati sanitari elettronici pertinenti a disposizione degli utenti in un ambiente di trattamento sicuro e conservandoli per il periodo stabilito nell'autorizzazione concessa. Si consideri che, nel fornire accesso a una serie di dati pseudonimizzati o anonimizzati, l'organismo responsabile dell'accesso ai dati sanitari dovrebbe utilizzare una tecnologia e norme di pseudonimizzazione o anonimizzazione all'avanguardia, garantendo nella misura massima possibile che una persona fisica non possa essere reidentificata dagli utenti dei dati sanitari. Senonché, ciò presuppone che vi sia uno *standard* europeo condiviso sulla definizione di dato anonimo [61]. Le definizioni giuridiche e i requisiti per l'a-

necessario ridurre i rischi per la riservatezza delle persone fisiche applicando il principio della minimizzazione dei dati. Pertanto, è opportuno mettere a disposizione dati sanitari elettronici non personali in tutti i casi in cui la fornitura di tali dati sia sufficiente. Se l'utente dei dati sanitari avesse bisogno di utilizzare dati sanitari elettronici personali, dovrebbe indicare chiaramente nella richiesta la giustificazione per l'uso di questo tipo di dati e l'organismo responsabile dell'accesso ai dati sanitari dovrebbe valutare se tale giustificazione sia valida. I dati sanitari elettronici personali dovrebbero essere resi disponibili solo in formato pseudonimizzato. Tenendo conto delle finalità specifiche del trattamento, i dati sanitari personali elettronici dovrebbero essere pseudonimizzati o anonimizzati il prima possibile nel processo di messa a disposizione dei dati per l'uso secondario. La pseudonimizzazione e l'anonimizzazione dovrebbero poter essere effettuate dagli organismi responsabili dell'accesso ai dati sanitari o dai titolari dei dati sanitari. In qualità di titolari del trattamento, agli organismi responsabili dell'accesso ai dati sanitari e ai titolari dei dati sanitari dovrebbe essere consentito delegare tali compiti ai responsabili del trattamento.

[61] Il Comitato europeo per la protezione dei dati dovrebbe adottare a breve linee guida aggiornate rispetto al Parere sulle tecniche di anonimizzazione adottato nel 2014 dal suo predecessore, il Gruppo di lavoro «Articolo 29», mentre sulla pseudonimizzazione sono state di recente adottate (cfr. Guidelines n.1/2025 on Pseudonymisation del 16 January 2025, consultabili al *link* https://www.edpb.europa.eu/our-

nonimizzazione e la pseudonimizzazione variano, infatti, notevolmente da un paese all'altro [62]. Ciò è in contrasto non solo con il modo in

work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_it . Sul tema v. anche Corte di giustizia dell'Unione europea, sentenze del 20 dicembre 2017, Peter Nowak contro Data Protection Commissioner, causa C-434/16, ECLI:EU:C:2017:582 e del 19 ottobre 2016, Patrick Breyer contro Bundesrepublik Deutschland, causa C-582/14, ECLI:EU:C:2016:779).

[62] I Garanti europei hanno chiarito come l'anonimizzazione rappresenti un processo che consiste in un ulteriore trattamento dei dati che non consente più l'identificazione dell'interessato in maniera irreversibile (WP29, Parere 05/2014 sulle tecniche di anonimizzazione, 10 aprile 2014,[WP 216],7). Tale ulteriore trattamento è considerato dai Garanti europei compatibile con le finalità originarie del trattamento ed implica che, rispetto ai dati resi irreversibilmente anonimi (a seguito del trattamento di anonimizzazione) il GDPR non sia più applicabile (considerando 26 GDPR). Riguardo all'anonimizzazione, come rimarcato dai Garanti europei, non può non tenersi conto del rischio residuo di re-identificazione (WP29, Parere 05/2014 sulle tecniche di anonimizzazione, cit. 11). Invero, in ossequio al principio di *accountability* (art.5.2 GDPR), tale rischio specifico deve necessariamente essere valutato (art. 32 GDPR), tenendo in considerazione tutti i mezzi di cui il titolare o i terzi possano ragionevolmente avvalersi per re-identificare la persona fisica a cui le informazioni si riferiscono, le risorse disponibili in termini di tempo, costi, ed eventuali nuovi sviluppi tecnologici (considerando 26 GDPR). In merito alla predetta valutazione sul rischio di re-identificazione, occorre richiamare il citato parere sulle tecniche di anonimizzazione nella parte in cui i Garanti precisano che «nei casi in cui i fattori e le caratteristiche in questione siano tali da comportare un rischio inaccettabile di identificazione delle persone interessate, il trattamento rientra nuovamente nell'ambito di applicazione della normativa in materia di protezione dei dati». Si ricorda che la pseudonimizzazione è invece una misura che riduce la correlabilità delle informazioni all'identità della persona cui si riferiscono. Tale misura, come noto, non è un metodo di anonimizzazione, in quanto i dati ad essa sottoposti si considerano personali, perché non è esclusa la loro attribuzione a una persona fisica (che quindi rimane identificabile attraverso l'utilizzo di informazioni aggiuntive conservate separatamente) ai sensi dei considerando 26, 28 e 29 e art. 4.5 del GDPR. Riguardo alla pseudonimizzazione, è stata recentemente emanata una decisione della Corte di Giustizia Europea, che afferma come non si consideri «dato personale», perché indirettamente identificabile, il dato pseudonimizzato trasmesso a un destinatario terzo che non abbia i mezzi tecnici o legali ragionevoli per ottenere la chiave di decrittazione dal titolare che comunica i dati (CGUE, 26 aprile 2023 C-T 557/20, CRU v GEPD).

cui operano le aziende farmaceutiche, digitali e di tecnologia sanitaria, in particolare nelle loro attività di ricerca e sviluppo concepite a livello globale, ma anche con l'obiettivo fondamentale dell'EHDS di consentire l'uso secondario dei dati senza soluzione di continuità a livello transfrontaliero. Sono necessari quindi orientamenti più precisi a livello dell'UE su come soddisfare i requisiti del GDPR in questo settore, in modo da conseguire un ragionevole equilibrio tra rischi e benefici, per eliminare l'incertezza giuridica e il conseguente timore di controversie per gli utenti secondari dei dati. Peraltro, l'anonimizzazione, soprattutto se particolarmente rigorosa, può ridurre l'utilità dei dati per la ricerca scientifica. Inoltre, non è del tutto chiaro chi dovrà anonimizzare i dati, cioè se debba farlo il titolare dei dati prima di condividerli con l'organismo responsabile dell'accesso ai dati sanitari, ovvero questo stesso organismo (cfr. Considerando n. 49 EHDS).

Con riferimento all'ambito di applicazione oggettivo del Regolamento, considerato che l'EHDS crea un doppio canale di tutela, l'uno per i dati sanitari *tout court* e l'altro per i dati sanitari elettronici, va da sé che le definizioni di tali elementi saranno diverse. Se per la definizione di «dati relativi alla salute», si utilizza l'approdo sicuro del GDPR (l'articolo 2, paragrafo 1, lettera a), del regolamento EHDS fa riferimento, infatti, all'articolo 4, punto 15, del GDPR), per il quale i dati sanitari sono i «dati personali relativi alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni sul suo stato di salute»[63], l'art. 2,

[63] La locuzione «stato di salute» non si riferisce solo a quello attuale, con la conseguenza che anche le informazioni riconducibili ad una malattia pregressa o futura sono sussumibili in tale definizione, a nulla rilevando che la patologia sia stata definitivamente superata o che presumibilmente si svilupperà sulla base di una determinata sintomatologia (cfr. Considerando n. 35 GDPR). In senso contrario, vedi F. Di Ciommo, *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e responsabilità,* 2022, 121 ss. Di recente, Cass. Ord. 11 ottobre 2023, n. 28417, in *Tecnologia e diritto*, 2024, 603 ss., con nota di M. Ziccardi, *La rivelazione non autorizzata dei "dati relativi alla salute" tra tutela dell'interessato e adeguatezza del rimedio sanzionatorio*, ha confermato l'ampliamento dell'orizzonte ermeneutico del concetto di «dati relativi

par. 2, lett. a) reg. EHDS, definisce i «dati sanitari elettronici personali» includendo oltre ai suddetti «dati relativi alla salute», anche i dati genetici (di cui all'art. 4, punto 13, del GDPR) che sono trattati in formato elettronico. Di più, il regolamento EHDS definisce, all'art. 51, come «dati sanitari elettronici a disposizione per l'uso secondario» un'ampia gamma di categorie di dati che vanno ben oltre ciò che sono le informazioni sulla salute o sulle cure mediche dei pazienti, comprendendo, ad esempio dei determinanti socioeconomici, ambientali e comportamentali della salute, dati amministrativi relativi all'assistenza sanitaria, anche in relazione alle dispensazioni, alle domande di rimborso, dati sui fattori ambientali, quali l'inquinamento, le radiazioni o l'uso di determinate sostanze chimiche [64]. Ciò in linea con quanto af-

---

alla salute», in modo da ricomprendere qualsiasi notizia potenzialmente idonea a svelare le condizioni di salute di una persona. Nel caso di specie, la comunicazione da parte dell'operatrice sanitaria della necessità di svolgere una terapia si è ritenuto costituire un'informazione pertinente allo stato di salute della paziente, in quanto rivelatrice dell'esistenza di una malattia, seppur intesa in senso ampio.

[64] I titolari dei dati sanitari, secondo l'art. 51 reg. EHDS n. 327/2025, devono mettere a disposizione le seguenti categorie di dati elettronici per uso secondario, conformemente alle disposizioni del presente capo: a) dati sanitari elettronici provenienti da cartelle cliniche elettroniche; b) dati su fattori con un'incidenza sulla salute, compresi i determinanti socioeconomici, ambientali e comportamentali della salute (ad esempio, analisi dei fattori dello stile di vita quali fumo, consumo di alcol, interventi chirurgici, incidenti...); c) dati aggregati sulle esigenze di assistenza sanitaria, sulle risorse assegnate all'assistenza sanitaria, sulla prestazione di assistenza sanitaria e sul suo accesso, sulla spesa per l'assistenza sanitaria e sul suo finanziamento; d) dati sugli agenti patogeni che incidono sulla salute umana; e) dati amministrativi relativi all'assistenza sanitaria, anche relativamente alle dispensazioni, alle domande di rimborso e ai rimborsi; f) dati genetici, epigenomici e genomici umani; g) altri dati molecolari umani, quali quelli provenienti dalla proteomica, dalla trascrittomica, dalla metabolomica, dalla lipidomica e altri dati omici; h) dati sanitari elettronici personali generati automaticamente mediante dispositivi medici; i) dati provenienti dalle applicazioni per il benessere; j) dati relativi allo status e alla specializzazione e all'istituzione dei professionisti sanitari coinvolti nella cura di una persona fisica; k)dati provenienti da registri dei dati sanitari basati sulla popolazione, come i registri di sanità pubblica; l)dati provenienti da registri medici e da registri della mortalità; m) dati provenienti da sperimentazioni cliniche, studi clinici, indagini cliniche

fermato al Considerando n. 56 reg. EHDS, secondo cui le categorie di dati sanitari elettronici che possono essere trattate per uso secondario dovrebbero essere sufficientemente ampie e flessibili da soddisfare le esigenze in evoluzione degli utenti dei dati sanitari, pur rimanendo limitate ai dati relativi alla salute o noti per influenzare la salute. L'art. 54 EHDS prevede poi che gli utenti dei dati sanitari trattino solamente i dati sanitari elettronici per l'uso secondario sulla base e in conformità delle finalità previste in un'autorizzazione ai dati rilasciata. Le finalità per le quali i dati sanitari possono essere trattati per usi secondari (cfr. art. 53 del Regolamento EHDS) sono numerose e forse sovrabbondanti. Si tratta in linea generale di compiti svolti da organismi pubblici, quali l'esercizio di funzioni pubbliche, compresi la sorveglianza sanitaria pubblica, i compiti di pianificazione e comunicazione, l'elaborazione delle politiche sanitarie, la garanzia della sicurezza dei pazienti, la qualità dell'assistenza, la sostenibilità dei sistemi sanitari, la ricerca scientifica[65]. Il carattere poco definito di alcune finalità di

---

e studi delle prestazioni soggetti al regolamento (UE) n. 536/2014, al regolamento (UE) 2024/1938 del Parlamento europeo e del Consiglio, al regolamento (UE) 2017/745 e al regolamento (UE) 2017/746; n) altri dati sanitari provenienti da dispositivi medici; o) dati provenienti da registri di medicinali e dispositivi medici; p) dati provenienti da coorti di ricerca, questionari e indagini in materia di salute, dopo la prima pubblicazione dei risultati; q) dati sanitari provenienti da biobanche e banche dati associate. Gli Stati membri possono introdurre misure più rigorose e garanzie supplementari a livello nazionale intese a tutelare la sensibilità e il valore dei dati che rientrano nel paragrafo 1, lettere f), g), i) e q). Gli Stati membri possono, inoltre, stabilire nel loro diritto nazionale che categorie aggiuntive di dati sanitari elettronici siano messe a disposizione per l'uso secondario in conformità del presente regolamento.

[65] Secondo l'art. 53 EHDS, «Gli organismi responsabili dell'accesso ai dati sanitari concedono l'accesso ai dati sanitari elettronici di cui all'articolo 51 per l'uso secondario a un utente dei dati sanitari solo se il trattamento dei dati da parte dell'utente è necessario per una delle finalità seguenti: a) pubblico interesse nell'ambito della sanità pubblica o della medicina del lavoro, come nel caso delle attività per la protezione da gravi minacce per la salute a carattere transfrontaliero, della sorveglianza della sanità pubblica o delle attività per la garanzia di elevati livelli di qualità e sicurezza dell'assistenza sanitaria, inclusa la sicurezza dei pazienti, e di medicinali o

accesso ai dati sanitari, come la produzione di beni e servizi e l'addestramento dei sistemi AI in ambito sanitario a sostegno delle politiche sanitarie e a fini di ricerca scientifica, soprattutto se si pensa alla definizione di utente dei dati sanitari, molto ampia e comprendente pure le imprese private, può creare qualche fondata preoccupazione di possibili abusi. D'altra parte, è in questa materia che si contrappongono frontalmente le esigenze di protezione individuale riguardanti dati personalissimi, con quelle collettive che potrebbero privilegiare un'interpretazione ampia della nozione di finalità di ricerca scientifica, che comprenda ad esempio lo sviluppo e la dimostrazione tecnologica, la ricerca fondamentale, la ricerca applicata, la ricerca finanziata privatamente e la ricerca di base [66]. Sono poi indicate nell'art. 54 EHDS una

---

dispositivi medici; b) definizione delle politiche e attività regolamentari a sostegno di enti pubblici o di istituzioni, organi e organismi dell'Unione, comprese le autorità di regolamentazione, del settore sanitario o dell'assistenza affinché svolgano i compiti definiti nei rispettivi mandati; c) statistiche quali definite all'articolo 3, punto 1), del regolamento (UE) n. 223/2009, come le statistiche ufficiali a livello nazionale, multinazionale e dell'Unione, relative al settore sanitario o dell'assistenza; d) attività d'istruzione o d'insegnamento nel settore sanitario o dell'assistenza al livello della formazione professionale o dell'istruzione superiore; e) ricerca scientifica nel settore sanitario o dell'assistenza che contribuisce alla sanità pubblica o alla valutazione delle tecnologie sanitarie o che garantisce elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di favorire gli utenti finali, quali i pazienti, i professionisti sanitari e gli amministratori sanitari, tra cui: i) attività di sviluppo e innovazione per prodotti o servizi; ii) attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, dispositivi medico-diagnostici in vitro, sistemi di IA e applicazioni di sanità digitale; f) miglioramento della prestazione di assistenza, ottimizzazione delle cure ed erogazione di assistenza sanitaria sulla base dei dati sanitari elettronici di altre persone fisiche. L'accesso ai dati sanitari elettronici per le finalità di cui al paragrafo 1, lettere a), b) e c), è riservato agli enti pubblici e alle istituzioni, agli organi e agli organismi dell'Unione che esercitano i compiti loro affidati dal diritto dell'Unione o dal diritto nazionale, anche quando il trattamento dei dati per lo svolgimento di tali compiti è effettuato da terzi per conto di tali enti pubblici o delle istituzioni, degli organi e degli organismi dell'Unione».

[66] E in effetti il Considerando n. 61 reg. EHDS, afferma che «La nozione di ricerca scientifica dovrebbe essere interpretata in senso ampio, che ricomprenda lo

serie di finalità vietate in relazione al trattamento dei dati sanitari elettronici per l'uso secondario [67], e tale elenco, letto attentamente, appare limitato ai casi d'uso che implichino danni diretti ai pazienti. Si afferma, infatti, al Considerando 62, che dovrebbe essere vietato qualsiasi tentativo di utilizzare i dati sanitari elettronici per eventuali misure pregiudizievoli per le persone fisiche, ad esempio per aumentare i pre-

---

sviluppo tecnologico e la dimostrazione, la ricerca fondamentale, la ricerca applicata e la ricerca finanziata da soggetti privati. Le attività correlate alla ricerca scientifica comprendono le attività di innovazione quali l'addestramento di algoritmi di intelligenza artificiale che potrebbero essere utilizzati nell'assistenza sanitaria o nella cura delle persone fisiche, nonché la valutazione e l'ulteriore sviluppo di algoritmi e prodotti esistenti a tali fini. È necessario che lo spazio europeo dei dati sanitari contribuisca anche alla ricerca fondamentale e, sebbene i suoi benefici per gli utilizzatori finali e i pazienti possano risultare meno diretti, tale ricerca è fondamentale per i benefici per la società a lungo termine. In taluni casi le informazioni di alcune persone fisiche, come le informazioni genomiche delle persone fisiche con una determinata malattia, potrebbero contribuire alla diagnosi o la cura di altre persone fisiche».

[67] In particolare, sono vietati l'accesso ai dati sanitari elettronici per l'uso secondario ottenuti mediante un'autorizzazione ai dati rilasciata a norma dell'articolo 68 o una richiesta di dati sanitari approvata a norma dell'articolo 69 e il trattamento di tali dati per gli usi seguenti: a) adottare decisioni pregiudizievoli per una persona fisica o un gruppo di persone fisiche sulla base dei loro dati sanitari elettronici; per essere considerate «decisioni» ai fini della presente lettera, esse devono produrre effetti giuridici, sociali o economici o incidere in modo analogo significativamente su tali persone fisiche; b) adottare decisioni, in relazione a una persona fisica o a un gruppo di persone fisiche, per quanto riguarda offerte di lavoro, offrire condizioni meno favorevoli nella fornitura di beni o servizi, compresa l'esclusione di tali persone o gruppi dal beneficio di un contratto di assicurazione o di credito, la modifica dei loro contributi e premi assicurativi o le condizioni dei prestiti, o adottare altre decisioni, in relazione a una persona fisica o a un gruppo di persone fisiche, che risultino in una discriminazione nei loro confronti sulla base dei dati sanitari ottenuti; c) svolgere attività pubblicitarie o di marketing; d) sviluppare prodotti o servizi in grado di danneggiare le persone, la sanità pubblica o la società in generale, quali droghe illecite, bevande alcoliche, prodotti del tabacco e della nicotina, armi o prodotti o servizi concepiti o modificati in modo da creare dipendenza, violare l'ordine pubblico o la moralità o causare un rischio per la salute umana; e) svolgere attività in contrasto con le disposizioni etiche a norma del diritto nazionale.

mi assicurativi, per intraprendere attività potenzialmente dannose per le persone fisiche concernenti l'occupazione, le pensioni o l'attività bancaria, compresa l'ipoteca sulle proprietà, per pubblicizzare prodotti o cure, per automatizzare il processo decisionale individuale, per reidentificare le persone fisiche o per sviluppare prodotti nocivi.

È poi prevista una procedura semplificata per l'accesso ai dati sanitari elettronici da parte di un titolare di dati sanitari affidabile (*trusted data holder*), che abbia determinati requisiti, al fine di alleviare l'onere amministrativo per gli organismi di accesso ai dati sanitari di gestire le richieste di dati da essi trattati. Se un organismo responsabile dell'accesso ai dati sanitari riceve una domanda di accesso a norma dell'art. 67, o una richiesta a norma dell'art. 69, che riguarda solo i dati sanitari elettronici detenuti da un titolare di dati sanitari affidabile designato, si applica appunto una procedura semplificata *ex* art. 72 reg. EHDS [68].

Il regolamento EHDS prevede che gli utenti abbiano accesso per uso secondario a dati pertinenti e limitatamente a quanto necessario rispetto allo scopo del trattamento richiesto, in linea con l'autorizzazione rilasciata dall'organismo responsabile. Dovrebbe inoltre essere proibito fornire l'accesso ai dati sanitari elettronici, oppure renderli di-

[68] Gli Stati membri, infatti, possono istituire una procedura mediante la quale i titolari dei dati sanitari possono chiedere di essere designati come titolari di dati sanitari affidabili, a condizione che i titolari di dati sanitari soddisfino le condizioni seguenti: a) siano in grado di fornire l'accesso ai dati sanitari tramite un ambiente di trattamento sicuro conforme all'articolo 73; b) dispongano delle competenze necessarie per valutare le domande di accesso ai dati sanitari e le richieste di dati sanitari; c) forniscano le garanzie necessarie per garantire il rispetto del regolamento EHDS n. 327/2025. Il titolare di dati sanitari affidabile valuta la domanda di accesso ai dati, ex art. 67 reg. EHDS, o la richiesta di dati, ex art. 69, e presenta la sua valutazione, corredata di una proposta di decisione non vincolante, all'organismo per l'accesso ai dati sanitari. Entro due mesi dal ricevimento della valutazione, l'organismo responsabile dell'accesso ai dati sanitari adotta una decisione in merito alla domanda di accesso ai dati sanitari o alla richiesta di dati sanitari.

sponibili in altro modo, a terzi non menzionati nell'autorizzazione ai dati.

Gli organismi responsabili dell'accesso ai dati sanitari, ai sensi dell'art. 58 reg. EHDS, dovranno fornire agli interessati informazioni che integrano quelle previste dall'art. 14 del GDPR, tra cui la base giuridica in virtù della quale l'accesso ai dati sanitari elettronici è concesso all'utente dei dati sanitari; le misure tecniche e organizzative adottate per tutelare i diritti delle persone fisiche; i diritti delle persone fisiche applicabili in relazione all'uso secondario; le modalità di esercizio dei diritti da parte delle persone fisiche conformemente al capo III del regolamento (UE) 2016/679; l'identità e i dati di contatto dell'organismo responsabile dell'accesso ai dati sanitari; chi ha ottenuto l'accesso a serie di dati sanitari elettronici e a quali serie di dati ha ottenuto l'accesso, nonché i dettagli dell'autorizzazione ai dati riguardo alle finalità del trattamento di tali dati di cui all'articolo 53, paragrafo 1; i risultati o gli esiti dei progetti per i quali i dati sanitari elettronici sono stati utilizzati. Non può non rilevarsi come la valutazione effettiva dei requisiti di tutela dei dati per il rilascio di un'autorizzazione ai dati sia disciplinata solo a un livello minimo, con lacune che dovranno essere colmate dal diritto nazionale. Di conseguenza, tali norme varieranno da uno Stato membro all'altro, con inevitabili inerenti problematiche [69].

[69] Sul fatto che vi sia il rischio che la procedura sia efficiente solo sulla carta, vedi J. Reichel, *Administrative tools for balancing societal and individual interests – data protection safeguards and administrative procedural guarantees in secondary use in the European Health Data Space*, in S. Slokenberga, K. Ó Cathaoir, M. Shabani, *The European Health Data Space. Examining A New Era in Data Protection*, London, Routledge, 2025, 207 ss. In Finlandia, in effetti, ove è stato introdotto un simile regime di accesso centralizzato ai dati sanitari, si segnala che la procedura risulta lunga e costosa.

5. *La base giuridica nell'uso secondario dei dati sanitari tra esigenze pubblicistiche e diritti di esclusione dell'interessato.*

Il regolamento EHDS attribuisce agli organismi di accesso ai dati sanitari compiti di interesse pubblico ai sensi dell'articolo 6, par. 1, lett. e), del GDPR, e soddisfa i requisiti di cui all'art. 9, par. 2, lett. g), h), i) e j), del medesimo testo e dell'art. 10, par. 2, lett. g), h), i) e j), del regolamento (UE) 2018/1725 (Regolamento sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE), per l'uso secondario dei dati sanitari elettronici personali, comprese le garanzie per consentire il trattamento di categorie particolari di dati, fornendo, quindi, una base giuridica [70], in termini di finalità lecite e *governance* affidabile. L'elenco

[70] La lett. g) dell'art. 9, par. 2, GDPR, riguarda il caso in cui il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; la lettera h) descrive il trattamento necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; la lettera i) riguarda il trattamento necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; la lettera j) concerne il trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede

delle finalità consentite che il regolamento include per l'uso secondario dei dati sanitari può fungere da indicatore per comprendere quali usi sono considerati di interesse pubblico. Tra di esse si annoverano le attività di protezione contro gravi minacce transfrontaliere per la salute o la ricerca scientifica connessa ai settori della salute o dell'assistenza, o attività che contribuiscono alla sanità pubblica o alle valutazioni delle tecnologie sanitarie, o garantiscano elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di andare a vantaggio degli utenti finali [71].

Uno sguardo all'attuale Codice *Privacy* italiano permette di comprendere quanto le norme presenti nel testo del Regolamento EHDS possano costituire una vera rivoluzione nel nostro Paese. Gli articoli 110 e 110-*bis* del Codice Privacy, già passati in rassegna, impongono regole decisamente stringenti e collegate, tranne che per eccezioni particolari, all'espressione di un consenso [72]. Il nuovo Regolamento

misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

[71] Il regolamento stabilisce specificamente che l'obiettivo di tale disciplina è migliorare l'accesso ai dati sanitari per «scopi che andrebbero a vantaggio della società», chiarendo che l'uso secondario dei dati sanitari dovrebbe essere di interesse pubblico. Questo approccio è stato adottato in alcuni paesi, come la Finlandia e l'Estonia, che hanno esplicitamente dichiarato nelle loro leggi nazionali che la ricerca scientifica condotta con dati sanitari in assenza del consenso dell'interessato è di interesse pubblico. (M. Kruus, *The Public Interest Requirement In the Secondary Use of Health Data In Scientific Research: The Examples of Estonia and Finland* (2023) 32, *Juridica International,* 64).

[72] Si veda però, da ultimo, la legge italiana sull'IA n. 132/2025, che al suo articolo 8, autorizza l'uso secondario di dati sanitari privi degli elementi identificativi, senza un consenso degli interessati, da parte di soggetti pubblici e privati senza scopo di lucro, dagli Istituti di ricovero e cura a carattere scientifico (IRCCS), di cui al decreto legislativo 16 ottobre 2003, n.288, nonché da soggetti privati operanti nel settore sanitario nell'ambito di progetti di ricerca a cui partecipano soggetti pubblici e privati senza scopo di lucro o IRCCS, per le seguenti attività dichiarate di rilevante interesse pubblico, ex art. 9, comma 2 GDPR: la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale per finalità di a) prevenzione; diagnosi e cura di malattie; b) sviluppo di farmaci; terapie e tecnologie riabi-

EHDS, invece, permette, seppur a determinate condizioni ed entro certi limiti, agli utenti dei dati, di avere la base normativa necessaria a far sì che tali dati, fonte inestimabile di attività di ricerca, possano effettivamente essere utilizzati senza il consenso (*opt-in*) dell'interessato. Si stabilisce, infatti, nel Considerando n. 52 reg. EHDS che gli Stati membri non dovrebbero più poter mantenere o introdurre, a norma dell'articolo 9, paragrafo 4, del regolamento (UE) 2016/679, ulteriori condizioni, comprese limitazioni e disposizioni specifiche che richiedano il consenso delle persone fisiche, per quanto riguarda il trattamento per l'uso secondario dei dati sanitari elettronici personali, ad eccezione dell'introduzione di misure più rigorose e garanzie supplementari a livello nazionale intese a tutelare la sensibilità e il valore di taluni dati. Ciò è giustificato sulla base del fatto che il consenso è sostituito con una *governance* affidabile e a costi inferiori

---

litative; c) realizzazione di apparati medicali, incluse protesi e interfacce fra il corpo e strumenti di sostegno alle condizioni del paziente; d) salute pubblica, incolumità della persona, salute e sicurezza sanitaria, nonché studio della fisiologia, della biomeccanica e della biologia umana anche in ambito non sanitario, in quanto necessari ai fini della realizzazione e dell'utilizzazione di banche di dati e modelli di base. Per questa materia molto delicata, inopinatamente viene quindi legittimato l'uso secondario di dati sanitari pseudonimizzati, con l'eliminazione del requisito del consenso preventivo dell'interessato, senza che sia prevista una governance pubblicistica ed un meccanismo di *opt out*, quali quelli invece presenti nel regolamento EHDS. Volgendo lo sguardo all'estero, va poi registrato come anche in Irlanda sia applicato un requisito generale di consenso esplicito ai sensi del GDPR sia per la ricerca primaria che per quella secondaria. Studi comparatistici hanno rivelato che anche in Irlanda è applicato un requisito generale di consenso esplicito ai sensi del GDPR, sia per la ricerca primaria che per quella secondaria. Studi comparatistici hanno rilevato che, in realtà, il consenso è base giuridica privilegiata in Europa (J. CHEN, E. S. DOVE, H. BHAKUNI, *Explicit Consent and Alternative Data Protection Processing Grounds for Health Research* in E. KOSTA, R. LEENES, I. KAMARA (eds), *Research Handbook on EU Data Protection Law* (Elgar, 2022). Pertanto, mentre il GDPR facoltizza (e possibilmente incoraggia) gli utenti dei dati a fare affidamento su basi giuridiche diverse dal consenso, la realtà mostra che il consenso come base giuridica è ancora applicato. E la posizione dell'EHDS riguardo gli usi secondari dei dati sanitari rappresenterà un cambiamento significativo nell'approccio di molti Stati membri alla regolamentazione del trattamento dei dati.

rispetto all'affidamento sul consenso. L'EHDS sembra proporre quindi un nuovo paradigma per l'uso secondario dei dati sanitari per la ricerca scientifica, non più basato sul consenso come regola generale, ma sulle nozioni di interesse generale della società e di interesse pubblico.

Per il trattamento dei dati sanitari elettronici detenuti dai titolari dei dati sanitari, l'art. 60 del regolamento EHDS, come anticipato, stabilisce l'obbligo giuridico per questi ultimi, ai sensi dell'art. 6, par. 1, lett. c), conformemente all'art. 9, par. 2, lett. i) e j) GDPR, di mettere a disposizione i dati sanitari elettronici personali agli organismi di accesso ai dati sanitari, mentre la base giuridica per lo scopo del trattamento iniziale (ad es. fornitura di assistenza sanitaria) rimane inalterata. Ai sensi dell'art. 60, quindi, il titolare dei dati sanitari deve mettere a disposizione dell'organismo preposto i dati sanitari elettronici entro tre mesi dal ricevimento della richiesta. In casi giustificati, l'organismo per l'accesso ai dati sanitari può prorogare tale periodo fino a tre mesi [73].

Nel fornire l'accesso a una serie di dati [74] anonimizzata o pseudo-

---

[73] Ai sensi dell'art. 63 EHDS, gli organismi responsabili dell'accesso ai dati sanitari, inclusi i servizi di accesso ai dati sanitari dell'Unione, o i titolari dei dati sanitari affidabili di cui all'art. 72 possono imporre tariffe per la messa a disposizione di dati sanitari elettronici per l'uso secondario. Le tariffe sono proporzionate ai costi di messa a disposizione dei dati e non limitano la concorrenza. Esse coprono totalmente o in parte i costi relativi alla procedura per la valutazione di una domanda di accesso ai dati sanitari o di una richiesta di dati sanitari, per il rilascio, il diniego o la modifica di un'autorizzazione ai dati a norma degli artt. 67 e 68 o per fornitura di una risposta a una richiesta di dati presentata a norma dell'art. 69, inclusi i costi relativi al consolidamento, alla preparazione, alla pseudonimizzazione, all'anonimizzazione e alla fornitura dei dati sanitari elettronici.

[74] Per «serie di dati», il regolamento EHDS (art. 2) intende «una raccolta strutturata di dati sanitari elettronici»; per «serie di dati ad alto impatto per l'uso secondario», ci si riferisce alle serie di dati il cui riutilizzo è associato a benefici significativi in ragione della sua rilevanza per la ricerca sanitaria; «catalogo di serie di dati» è definita una raccolta di descrizioni delle serie di dati, organizzata in modo sistematico e comprendente una parte pubblica orientata all'utente, in cui le informazioni relative ai singoli parametri delle serie di dati sono accessibili per via elettronica attraverso

nimizzata, l'organismo per l'accesso ai dati sanitari dovrebbe utilizzare tecnologie e norme all'avanguardia, garantendo per quanto possibile che le persone fisiche non possano essere reidentificate dagli utenti dei dati sanitari, per non incorrere in sanzioni amministrative, civili e penali, nel caso in cui il diritto nazionale lo preveda. Quando rilascia un'autorizzazione ai dati, poi, l'organismo per l'accesso ai dati sanitari stabilisce le condizioni generali applicabili all'utente dei dati sanitari [75].

Se l'organismo per l'accesso ai dati sanitari è informato da un utente dei dati sanitari di un risultato significativo relativo alla salute di una persona fisica, l'organismo per l'accesso ai dati sanitari ne dovrà informare il titolare dei dati, che, a sua volta, alle condizioni stabilite dal diritto nazionale, informerà la persona fisica o il professionista sanitario curante [76]. Le persone fisiche hanno il diritto di chiedere di non essere informate di tali risultati.

---

un portale *online*. Si afferma, infatti, al Considerando 84 reg. EHDS, che dovrebbe essere istituito un catalogo dell'UE delle serie di dati per facilitare la reperibilità delle serie di dati disponibili nell'EHDS, per aiutare i titolari dei dati a pubblicare le loro serie di dati, per fornire a tutte le parti interessate, compreso il pubblico in generale, tenendo conto anche delle persone con disabilità, informazioni sulle serie di dati inserite nell'EHDS (come le etichette di qualità e di utilità, le schede informative sulle serie di dati), per fornire agli utenti dei dati informazioni aggiornate sulla qualità dei dati e sull'utilità delle serie di dati.

[75] L'autorizzazione ai dati deve contenere i seguenti elementi: (a) le categorie, la specifica e il formato dei dati sanitari elettronici a cui accedere contemplati dall'autorizzazione ai dati, comprese le relative fonti e, l'eventuale indicazione che l'accesso ai dati sanitari elettronici dovrà essere effettuato in forma pseudonimizzata nell'ambiente di trattamento sicuro; b) una descrizione dettagliata della finalità della messa a disposizione dei dati sanitari elettronici; c) qualora sia previsto un meccanismo di attuazione di un'eccezione e questo sia applicabile a norma dell'articolo 71, paragrafo 4, informazioni che indichino se è stata applicato e il motivo della relativa decisione; d) l'identità delle persone autorizzate, in particolare l'identità del ricercatore principale, con il diritto di accedere ai dati sanitari elettronici nell'ambiente di trattamento sicuro; e) durata dell'autorizzazione ai dati; f) informazioni sulle caratteristiche tecniche e sugli strumenti a disposizione dell'utente dei dati sanitari nell'ambiente di trattamento sicuro; g) tariffe a carico dell'utente dei dati sanitari; h)eventuali condizioni specifiche.

[76] Al Considerando 57 reg. EHDS, si afferma poi che gli utenti dei dati sanitari che beneficiano dell'accesso a serie di dati fornite ai sensi del presente regolamento

Punto focale di tale regolamento, che disciplina la materia dell'uso secondario dei dati, sorvolando sul consenso dell'interessato, ed utilizzando le altre basi giuridiche permeate dall'interesse pubblico, è stata l'introduzione, all'art. 71 del regolamento EHDS, della possibilità per l'interessato di procedere all'*opt-out*. Tale norma così stabilisce: «Le persone fisiche hanno il diritto di escludere in qualsiasi momento, e senza dover fornire una motivazione, il trattamento dei dati sanitari elettronici personali che le riguardano per l'uso secondario a norma del presente regolamento. L'esercizio di tale diritto è reversibile. Gli Stati membri prevedono un meccanismo di esclusione accessibile e facilmente comprensibile ai fini dell'esercizio del diritto stabilito al paragrafo 1, in base al quale le persone fisiche possono esplicitamente esprimere la propria volontà di escludere il trattamento dei loro dati sanitari elettronici personali per l'uso secondario»[77].

---

potrebbero arricchire i dati con varie correzioni e annotazioni e altri miglioramenti, integrando ad esempio i dati mancanti o incompleti, migliorando in tal modo l'accuratezza, la completezza o la qualità dei dati nelle serie di dati. Gli utenti dei dati sanitari dovrebbero essere incoraggiati a segnalare errori critici nelle serie di dati agli organismi responsabili dell'accesso ai dati sanitari. Per favorire il miglioramento della banca dati iniziale e l'ulteriore utilizzo della serie di dati arricchita, gli Stati membri dovrebbero poter stabilire norme per il trattamento e l'uso dei dati sanitari elettronici contenenti miglioramenti per il loro trattamento. La serie di dati migliorata dovrebbe essere messa a disposizione del titolare dei dati sanitari originario gratuitamente assieme a una descrizione dei miglioramenti. Il titolare dei dati sanitari dovrebbe rendere disponibile la nuova serie di dati, a meno che non fornisca all'organismo responsabile dell'accesso ai dati sanitari un'opposizione giustificata a tale operazione, ad esempio in casi in cui l'arricchimento da parte degli utenti dei dati sanitari sia di bassa qualità.

[77] Un approccio tradizionale in materia di trattamento dei dati personali distingue tra un modello cd. di «*opt-out*» e un modello di «*opt-in*». Si tratta di una terminologia sviluppata soprattutto nell'ambito del *marketing,* ma suscettibile di applicazione più generale. La differenza tra i due modelli è che, nel primo, il titolare può liberamente iniziare il trattamento ma l'interessato può decidere di "uscirne" (*opt-out*), facendolo così cessare; nel secondo, il trattamento di dati non può essere iniziato senza la preventiva volontà dell'interessato di "farne parte" (*opt-in*). L'esercizio dell'opposizione al trattamento, così come il diritto di esclusione, risponde a un modello tendenzialmente di *opt-out*, mentre la prestazione del consenso ad un modello di *opt-in*. I modelli convivono nell'assetto giuridico del GDPR, poiché rispondono a

Insomma, il regolamento EHDS demanda agli Stati membri l'introduzione di meccanismi per l'esercizio di un diritto di *opt-out* da parte degli interessati [78]. Ed è imperativo fornire alle persone fisiche informazioni sufficienti e complete su tale loro diritto, compresi i vantaggi e gli svantaggi dell'esercizio del medesimo (Considerando 54 reg. EHDS) [79].

L'uso del termine «esclusione» evoca, in prima approssimazione, scenari ormai superati (il *ius excludendi omnes alios*) e da archiviare quali

---

esigenze diverse, che dipendono dalle finalità per le quali i dati sono trattati. Ad esempio, una finalità di trattamento per l'esecuzione di compiti di pubblico interesse non può che essere costruita sul modello dell'*opt-out*, laddove un trattamento per finalità di invio di una *newsletter* (*marketing*) trova il giusto bilanciamento di diritti sulla base di un modello di *opt-in*, vale a dire basato su un consenso preventivo.

[78] Cfr. T. SOKOL, *European health data space, use of data and data subject's control over their own health data: can an opt-out restore the balance?*, in *European journal of health law*, vol. 31, n. 4, 2024, 365 ss. Si tratta di un meccanismo che ha precedenti nell'esperienza di alcuni stati membri, con risultati contrastanti. In Danimarca, ad esempio, è stata introdotta, e successivamente revocata, una clausola di non partecipazione all'identificazione dei partecipanti alla ricerca attraverso il loro numero di registrazione civile, sulla base del fatto che aveva un impatto negativo sulla rappresentatività della ricerca (Cfr. F. NORDFALK, K. HOEYER, *'The Rise and Fall of an Opt-out System'* (2020), 48, *Scandinavian Journal of Public Health,* 400) Più recentemente, una clausola nazionale di non partecipazione in Inghilterra, che consentiva alle persone di impedire l'uso dei propri dati sanitari per scopi diversi dall'assistenza diretta, ha registrato un forte aumento del numero di *opt-out* in risposta a un'iniziativa guidata dal governo per creare un *database* centralizzato pseudonimizzato composto dalle cartelle cliniche codificate dei pazienti (cfr. J. TAZARE, A. D. HENDERSON, J. MORLEY, H. A. BLAKE, H. I. MCDONALD, E. J. WILLIAMSON, H. STRONGMAN, *NHS National Data Opt-Outs: Trends and Potential Consequences for Health Data Research* (2024) BJGP Open).

[79] Secondo C. STAUNTON, M. SHABANI, D. MASCALZONI, S. MEZINSKA, S. SLOKENBERGA, *Ethical and social reflections on the proposed European Health Data Space*, in *European Journal of Human Genetics,* 32, 498–505 (2024), consultabile al *link https://doi.org/10.1038/s41431-024-01543-9*, sarà necessario sviluppare un sistema che faciliti la comunicazione con gli interessati per descrivere lo scopo per il quale verrà utilizzato l'accesso ai loro dati e consentire una risposta. Occorrerà un'interfaccia dinamica che consenta di fornire informazioni agli interessati sull'uso dei dati e un processo che consenta loro di rinunciare attivamente.

quelli cari all'originaria accezione del *right to privacy* inteso come diritto assoluto [80]. Analizzando la disciplina di tale istituto, però, la medesima pare in linea con le esigenze di bilanciamento tra le contrapposte situazioni giuridiche, in cui si incanala la libera circolazione dei dati, funzionale sia alla piena realizzazione del mercato interno, sia al processo di coesione sociale e istituzionale dell'UE, come suggerito dal Considerando n. 4 GDPR, secondo cui «(...) il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità». Dopo essere stato debitamente reso edotto circa i propri diritti, l'interessato, consapevole degli effetti del proprio silenzio, può decidere quindi di rimanere inerte ovvero di assolvere l'onere che la legge gli impone al fine di impedire l'uso secondario, esplicitando il suo rifiuto. In ciascun caso, dunque, il soggetto considerato dovrebbe esprimere una volontà, informata e consapevole dei propri effetti, che è espressione dell'autonomia individuale di determinare il destino dei propri dati sanitari.

L'interessato si ritrova, quindi, ad avere una facoltà [81], quello di azionare il proprio diritto di *opt-out* rispetto all'uso secondario dei propri da-

---

[80] Cfr., a riguardo, S. Warren, L. Brandeis, *The right to privacy*, in *Harvard Law Review*, 1890, 5, 193 ss.

[81] Secondo V. Ricciuto, *Base giuridica del trattamento del dato sanitario nell'ottica dell'EHDS*, relazione al Convegno: *Sanità digitale. Regolamento sullo spazio europeo dei dati sanitarie fonti interne*, tenutosi in Roma 21-22 marzo 2025, si tratterebbe di un onere. Cfr. per la teoria generale di questa figura, T.O. Scozzafava, voce *Onere (nozione)*, in *Enc. dir.*, XXX, Milano, Giuffrè, 1980, 99 s. L'onere ricorrerebbe tutte le volte in cui «un soggetto per ottenere un risultato è tenuto a conformare la propria condotta a specifiche regole giuridiche». O meglio l'onere è da intendere non come dovere attenuato, ma, nel suo significato proprio, di comportamento prescritto dalla norma, non doveroso, strumentale rispetto al conseguimento di un fine libero, l'inosservanza del quale non costituisce illecito, non lede interessi altrui, non comporta responsabilità (ma, semmai, autoresponsabilità). Cfr. a riguardo V. Caredda, *L'onere e la norma: prove di accesso al diritto*, in *Giustizia civile*, 2019, 51 ss., e, soprattutto, tra le opere monografiche, vedi di recente sempre V. Caredda, *La questione dell'onere*, Torino, Giappichelli, 2024, *passim*. Sulla differenza tra onere e obbligo, si veda pure V. Du-

ti sanitari, e la mancata manifestazione di volontà del medesimo si riduce ad un consenso presunto informato, in qualche modo assimilabile a quello previsto dall'articolo 4, comma 1, della legge 1° aprile 1999 n. 91, «Disposizioni in materia di prelievi e di trapianti di organi e di tessuti» [82], considerato che viene equiparata la mancata risposta del soggetto interessato ad una positiva dichiarazione di volontà, in ossequio a quel principio di solidarietà sociale che permea il regolamento EHDS [83]. Una reazione esplicita negativa dell'interessato si configura, invece, come una dichiarazione ostativa, atta ad impedire l'uso secondario dei propri dati sanitari elettronici altrimenti inevitabile.

Sempre secondo l'art. 71 reg. EHDS, per determinate finalità che presentano un forte legame con l'interesse pubblico, come le attività di protezione contro gravi minacce per la salute a carattere transfrontaliero o la ricerca scientifica per importanti motivi di interesse pubblico, gli Stati membri possono istituire, in relazione al loro contesto nazionale, in via di eccezione, un meccanismo per fornire l'accesso ai dati delle persone fisiche che si sono avvalse del diritto di esclusione, per garantire che in tali situazioni possano essere comunque resi disponibili *set* di dati completi. La ricerca scientifica per importanti motivi di interesse pubblico potrebbe ad esempio includere la ricerca che affronta

---

RANTE, voce "*Onere*", in *Enc. giur. Treccani*, vol. XXI, Roma, 1990, 3, e la bibliografia ivi citata.

[82] Tale norma così dispone: «Entro i termini, nelle forme e nei modi stabiliti dalla presente legge e dal decreto del Ministro della sanità di cui all'articolo 5, comma 1, i cittadini sono tenuti a dichiarare la propria libera volontà in ordine alla donazione di organi e di tessuti del proprio corpo successivamente alla morte, e sono informati che la mancata dichiarazione di volontà è considerata quale assenso alla donazione, secondo quanto stabilito dai commi 4 e 5 del presente articolo».

[83] Cfr., sul consenso presunto informato nella materia del trapianto d'organo da cadavere, F.D. BUSNELLI, P*er uno statuto del corpo umano inanimato, in* S. CANESTRARI, G. FERRANDO, C.M. MAZZONI, S. RODOTÀ, P. ZATTI (a cura di), *Il governo del corpo,* in RODOTÀ, ZATTI, *Trattato di biodiritto,* II*,* Milano, Lefebvre Giuffrè, 2011, 2137 ss.; G. GIAIMO, *Natura e caratteristiche del consenso al prelievo di organi e tessuti da cadavere. un raffronto tra Italia ed Inghilterra*, in *Europa e diritto privato*, 2018, 215 ss.; R. ROLLI, *Antiche e nuove questioni sul silenzio come tacita manifestazione di volontà*, in *Contratto e Impresa*, 2000, 206.

esigenze mediche insoddisfatte, anche per le malattie rare, o per le minacce sanitarie emergenti. Tale eccezione dovrebbe essere disponibile solo per gli utenti dei dati sanitari che siano un ente pubblico o un'istituzione, un organo o un organismo dell'Unione che dispone di un mandato per svolgere compiti nel settore della sanità pubblica, o per altro soggetto incaricato di svolgere compiti pubblici nel settore della sanità pubblica, o che agisce per conto di un'autorità pubblica o da essa incaricato. Non è chi non possa vedere come questa eccezione possa depotenziare la forza autodeterminativa dell'interessato, sull'altare di un non sempre ben precisato interesse pubblico. D'altra parte, come più volte evidenziato, il rischio contrario sarebbe quello di non rendere accessibile una quantità significativa di dati utili per il bene collettivo.

Una volta che una persona fisica abbia esercitato il proprio diritto di esclusione e se i dati sanitari elettronici personali che la riguardano possono essere identificati in una serie di dati, tali dati non sono messi a disposizione, né sono trattati in altro modo. Ciò comunque non pregiudica il trattamento per l'uso secondario dei dati sanitari elettronici personali riguardanti tale persona fisica conformemente alle autorizzazioni ai dati rilasciate o alle richieste di dati sanitari rilasciate o approvate prima che la persona fisica esercitasse il proprio diritto di esclusione.

Alcuni interrogativi, però, sorgono con evidenza. È chiaro, innanzitutto che la possibilità per gli Stati membri di introdurre eccezioni all'*opt-out* per motivi di interesse pubblico (considerando 54) possa determinare notevoli divergenze nel modo in cui tale limitazione è applicata da uno Stato membro all'altro, soprattutto in considerazione della mancanza di un'interpretazione comune di ciò che è nell'interesse pubblico. Inoltre, mentre è stata evidenziata l'importanza di rendere comprensibile e accessibile il processo di *opt-out*, resta da vedere come ciò verrà attuato nella pratica. In che modo le persone saranno informate del loro diritto di *opt-out*? Cosa includerà questa notifica [84]?

[84] In tal senso, vedi anche P. Cervera De La Cruz, M. Shabani, in *Fair enough? Exploring the role of fairness in secondary uses of health data in the European Health Data*

Occorre poi distinguere, a mio avviso, il diritto di esclusione dal diritto di opposizione presente nel GDPR [85].

L'opposizione, come noto, è una manifestazione di volontà recettizia a vocazione inibitoria che ha l'effetto di far cessare, in via permanente, un determinato trattamento di dati personali, ed è esercitabile nel caso in cui tale trattamento sia necessario all'esecuzione di un compito di interesse pubblico, o comunque connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento o se il trattamento è necessario per il perseguimento di un legittimo interesse del titolare del trattamento o di terzi. Tale diritto, infatti, ha una valenza sussidiaria: esso soccorre laddove la presenza di un interesse particolarmente qualificato allo svolgimento del trattamento, non basato sul consenso, impedisca l'ordinario potere di controllo dell'interessato.

Ebbene, confrontando brevemente il diritto di esclusione e quello di opposizione, le due figure non sembrano assimilabili *in toto*, in quanto per lo strumento disciplinato nell'EHDS non è richiesto, almeno *ex ante*, un bilanciamento di interessi. Non è richiesto insomma che siano espressi da parte dell'interessato motivi connessi alla sua situazione particolare, diversamente da quanto previsto dall'art. 21 GDPR [86]. Inoltre, l'opposizione si fa valere nei confronti di un tratta-

---

Space, in S. SLOKENBERGA, K. Ó CATHAOIR, M. SHABANI, *The European Health Data Space; Examining A New Era in Data Protection*, London, Routledge, 2025, 136 ss.

[85] Il diritto di opposizione era stato evocato sulla base della proposta EHDS, quale traduzione del termine *opt out*. Cfr. E. PELINO, in E. PELINO, L. BOLOGNINI (a cura di) *Codice della disciplina privacy*, Milano, Lefebvre Giuffrè, 2024, 156;

[86] Nella disciplina del GDPR, i legittimi interessi fondano il bilanciamento compiuto *ex ante* dal titolare del trattamento, mentre i motivi connessi alla situazione particolare fondano i diritti *ex post* dell'interessato di contestare la validità del bilanciamento. Tale contestazione avvia un nuovo *test* di bilanciamento, effettuato secondo i parametri (diversi e nuovi) dell'art. 21 e non più dell'art.6 del GDPR. Cfr., in tal senso, G. COMANDÈ, sub art. 21, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA, *Codice della privacy e data protection*, Milano, Lefebvre Giuffrè, 2021, 366 ss. La natura del titolare e pure dell'interesse perseguito rilevano, ad esempio, per legittimare o meno il rigetto di un'opposizione ad un trattamento per finalità di ricerca; così la natura dei dati (sensibili o meno) o il ruolo pubblico dell'interessato che siano tali da giustificare l'interesse generale a quei dati hanno un peso importante (WP29, (2014),

mento già iniziato, mentre l'esclusione pare riferirsi anche a trattamenti non ancora intrapresi. [87]

6. *La ricostruzione dei rapporti tra i soggetti che operano nello spazio di condivisione dei dati e la natura delle loro responsabilità in caso di deviazione dalla condotta standard.*

Come noto, al fine di accertare le responsabilità per un eventuale trattamento di dati sanitari non conforme, occorre individuare preliminarmente il titolare del trattamento, nella definizione di cui all'art. 4 GDPR [88]. Ed opportunamente, il Considerando n. 79 reg. EHDS definisce nel dettaglio i ruoli del trattamento nelle varie fasi del procedimento volto alla circolazione dei dati sanitari per uso secondario. Esso precisa che, nell'ambito di un trattamento di dati sanitari elettro-

---

Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González", C-131/12, WP 225, Brussels, 26 novembre 2014). Ricorda la WP29 che «In generale, il fatto che un responsabile del trattamento agisca non solo nel proprio interesse legittimo (per esempio, nell'interesse dell'impresa), ma anche nell'interesse della collettività, può attribuire maggior "peso" a tale interesse. Quanto più preminenti saranno l'interesse pubblico o l'interesse della collettività e quanto più la collettività e gli interessati riconosceranno che il responsabile del trattamento può intervenire e trattare i dati al fine di perseguire tali interessi, tanto maggiore sarà il peso di questo interesse legittimo nel bilanciamento» (WP29, 2014, 42). In argomento, vedi anche A. Ricci, *I diritti dell'interessato*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Bologna, Zanichelli, 2019, 392 ss.

[87] Cfr., in senso adesivo, S. Corso, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, in *Le nuove leggi civili comm.*, 2025, 590.

[88] A riguardo, non può che rinviarsi alle Linee guida EDPB 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento, ai sensi del GDPR, versione 2.0, adottate il 7 luglio 2021, nelle quali si ricorda che i concetti di titolare del trattamento, di contitolare del trattamento e di responsabile del trattamento sono funzionali, in quanto mirano a ripartire le responsabilità in funzione dei ruoli effettivi delle parti, e autonomi, nel senso che dovrebbero essere interpretati principalmente ai sensi del diritto dell'UE in materia di protezione dei dati.

nici iniziato a seguito di un'autorizzazione ai dati o di una richiesta di dati sanitari, in base ai rispettivi ruoli che svolgono e per una specifica parte del processo, devono essere considerati titolari dei dati sanitari gli organismi responsabili dell'accesso ai dati sanitari e gli utenti dei dati sanitari. Ai sensi dell'art. 74 reg. EHDS, il titolare dei dati sanitari è considerato titolare del trattamento per la messa a disposizione dei dati sanitari richiesti in favore dell'Organismo responsabile. L'organismo responsabile dell'accesso ai dati sanitari è considerato, invece, titolare del trattamento dei dati sanitari nello svolgimento dei suoi compiti [89]. Si considera poi che l'organismo responsabile dell'accesso ai dati sanitari agisca in qualità di responsabile del trattamento per conto dell'utente dei dati sanitari, qui titolare del trattamento dei dati sanitari elettronici personali, ai sensi di un'autorizzazione ai dati rilasciata a norma all'art. 68 nell'ambiente di trattamento sicuro, quando fornisce dati attraverso tale ambiente o per il trattamento di tali dati. I punti di contatto nazionali per l'uso secondario agiscono in qualità di contitolari del trattamento nelle operazioni di trattamento eseguite all'interno di DatiSanitari@UE (HealthData@EU) cui partecipano e la Commissione agisce in qualità di responsabile del trattamento per conto di tali punti di contatto nazionali per l'uso secondario, senza pregiudicare i compiti degli organismi responsabili dell'accesso ai dati sanitari e a seguito di tali operazioni di trattamento.

Se questi paiono punti fermi, non è chiaro, in quanto non ancora disciplinato, il rapporto del Reg. EHDS n. 327/2025 con l'erigendo Ecosistema dei dati sanitari, per il quale la titolarità dei dati è in capo al Ministero della Salute. Pare potersi dire però che fino al trasferimento dei dati all'Organo di accesso, il Ministero della Salute sia da

[89] Anche il titolare di dati sanitari affidabile, ai sensi dell'art. 72 reg. EHDS, nel fornire l'accesso ai dati sanitari elettronici agli utenti dei dati sanitari sulla base di un'autorizzazione ai dati in un ambiente di trattamento sicuro, tratta i dati sanitari elettronici, tramite il ricevimento, la combinazione, la preparazione e la compilazione di tali dati e per la pseudonimizzazione o l'anonimizzazione di tali dati, è considerato titolare del trattamento.

considerare titolare del trattamento, trasferendo poi tale qualifica ai suddetti enti.

Per far valere i diritti eventualmente lesi da un trattamento dei dati sanitari non corretto, nel regolamento EHDS esiste una tutela che, come per il GDPR, si prefigura come concorrente e non alternativa [90]. Vi è infatti sia una tutela amministrativa, attraverso il reclamo all'autorità di sanità digitale competente o all'organismo responsabile dell'accesso ai dati sanitari (a seconda della tipologia di pregiudizio relativo o meno all'uso primario o secondario dei dati sanitari), che una tutela giurisdizionale affidata all'autorità giudiziaria di ogni Stato membro. Infatti, secondo gli articoli. 21 e 81 reg. EHDS, relativi ad altrettanti capi della norma europea, fatti salvi eventuali altri ricorsi amministrativi o giurisdizionali, le persone fisiche e giuridiche hanno il diritto di presentare un reclamo, purché i loro diritti o interessi siano influenzati negativamente.

Se il reclamo riguarda i diritti delle persone fisiche a norma degli articoli 3 e da 5 a 10 del regolamento EHDS, le suddette autorità trasmetteranno il medesimo alle autorità di controllo competenti di cui al Regolamento (UE) 2016/679.

Accanto alla previsione di sanzioni amministrative, per la violazione del regolamento EHDS, vi è pure una norma che regola la responsabilità civilistica, l'art. 100, che, inevitabilmente, dovrà essere confrontata con quanto previsto dalla norma omologa di cui all'art. 82, GDPR. Esso afferma che «Qualsiasi persona fisica o giuridica che subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere un risarcimento, conformemente al diritto dell'Unione e nazionale» [91]. Per quanto riguarda

---

[90] Cfr. F. Balducci Romano, in R. Sciaudone, E. Caravà (a cura di), *Il codice della privacy: commento al d.lgs. 196/2003 e al d.lgs. 101/2018 alla luce del Regolamento (UE) 2016/679 (GDPR)*, Pisa, Pacini, 2019, 732; A. Candini, *Gli strumenti di tutela*, in G. Finocchiaro (diretto da), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 569 ss.; R. Giordano, *La tutela amministrativa e giurisdizionale dei dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1001 ss.

[91] L'art. 101 EHDS, afferma poi che «Qualora una persona fisica ritenga che sia-

l'ambito di applicazione soggettivo, balza subito all'occhio la presenza della persona giuridica, quale soggetto suscettibile di subire un danno. Il regolamento EHDS, del resto, prevede una serie di obblighi di condotta o prescrizioni che, direttamente o indirettamente, tutelano pure gli utenti dei dati sanitari e i titolari di dati sanitari, che ben possono essere persone giuridiche, che si rapportano con l'Organismo di accesso ai dati sanitari o l'autorità sanitaria digitale, e subire un pregiudizio da un comportamento scorretto o in conseguenza della violazione di una norma da parte di quest'ultimi.

L'art. 100 reg. EHDS, poi, a differenza di quanto previsto nel GDPR, non individua esplicitamente i soggetti su cui grava l'obbligo risarcitorio. Il Considerando n. 101, all'uopo, soccorre l'interprete, precisando che a risarcire i danni dovrebbero essere «l'autorità di sanità digitale, l'organismo responsabile dell'accesso ai dati sanitari, il titolare dei dati sanitari o l'utente dei dati sanitari».

Vista la mancanza di un qualsiasi accenno alla natura della responsabilità, si ripropongono in tale sede alcuni interrogativi sulla medesima già venuti alla luce per l'art. 82 GDPR [92]. Ciò consapevoli del fatto

---

no stati violati i diritti di cui gode a norma del presente regolamento, ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro, costituiti in conformità del diritto nazionale, con obiettivi statutari di pubblico interesse e attivi nel settore della protezione dei dati personali, per proporre reclamo per suo conto o esercitare i diritti di cui agli articoli 21 e 81».

[92] Tra i contributi più recenti a riguardo, vedi, V. CUFFARO, voce *Risarcimento del danno e trattamento dei dati personali*, in *Enc. dir.*, *I tematici*, VII, *Responsabilità civile*, diretto da C. SCOGNAMIGLIO, Milano, Lefebvre Giuffrè, 2024, 1360 ss.; B. PARENZO, *Note sparse in tema di responsabilità da illecito trattamento dei dati personali (a partire da due premesse)*, in *Rassegna di diritto civile*, 2024, 870 ss.; U. SALANITRO, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di giustizia*, in *Rivista di diritto civile*, 2023, 426 ss. Nell'ambito di una configurazione della natura extracontrattuale della responsabilità ex art. 82 GDPR, è discusso se la regola attuale dell'imputazione si ponga sul piano della dimostrazione della mancanza di colpa (presunzione di colpa) (in tal senso, tra gli altri, vedi M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1048 ss.; E. PALMERINI, sub art. 82 GDPR , in E. NAVARRETTA (a cura di), *Codice della responsabilità civile*, Milano, Lefebvre Giuffrè, 2021, 2497 ss.; R. CATERINA

che l'art. 100 reg. EHDS è come l'art. 82 GDPR, norma di fonte eu-

---

, S. Thobani, *Il diritto al risarcimento dei danni*, in *Giurisprudenza italiana*, 2019, 2807 s.; D. Barbierato, *Trattamento dei dati personali e «nuova» responsabilità civile*, in *Responsabilità civile e previdenza*, 2019, 2157; R. Senigaglia, *Reg. Ue 2016/679 e diritto all'oblio nella comunicazione telematica. identità informazione e trasparenza nell'ordine della dignità personale*, in *Nuove leggi civili commentate,* 2017, 1060) ovvero richieda un evento estraneo al rischio tipico di impresa (responsabilità oggettiva per rischio). In tale ultimo senso, tra gli altri, vedi S. Sica, *Verso l'unificazione del diritto europeo alla tutela dei dati personali*, in S. Sica, V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Milano, Wolters Kluwer, 2016, op. cit., 893, che pretende la dimostrazione di un fatto terzo generatore del danno, munito dei caratteri dell'imprevedibilità e di inevitabilità propri del caso fortuito e della forza maggiore; E. Tosi, *Diritto privato delle nuove tecnologie digitali*, Milano, Lefebvre Giuffrè, 2021, 599, che individua una «responsabilità oggettiva per rischio d'impresa derivante dall'attività di trattamento di dati personali in violazione delle regole di condotta conformative, protettive dell'interessato-danneggiato»; C. Camardi, *Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea*, in *Nuova giurisprudenza civile commentata*, 2023, 795 ss., che si esprime in termini di responsabilità oggettiva e nega che il titolare del trattamento possa limitarsi a dimostrare la propria diligenza; esprime il dubbio se la norma si riferisca alla mancanza del nesso causale o ad una esimente di tipo oggettivo, E. Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali*, in *Contratto e impr*esa, 2018, 124 s.. Cfr., da ultimo, in argomento, D.M. Locatello, *Adeguata gestione del rischio e presunzione di colpa nell'imputazione del danno da illecito trattamento di dati personali*, in *Contratto e impresa*, 2024, 1215 ss.; A. Maietta, *La prova del danno da illecito trattamento dei dati personali*, Bari, Cacucci, 2023, 86. In un dibattito tanto ricco e complesso, si è di recente inserita la decisione della Corte di Giustizia sulla quinta questione pregiudiziale di *Krankenversicherung Nordrhein*, sollevata dal *Bundesarbeitsgericht*. Essa ha accreditato la tesi che ricostruisce l'imputazione della responsabilità, al titolare o al responsabile del trattamento, come fondata su un «meccanismo di responsabilità per colpa accompagnato da un'inversione dell'onere della prova» (§ 98) (CGUE, III sez., 21 dicembre 2023, ZQ c. *Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts*, C-667/21, in *www.curia.europa.eu*). Non spetta, dunque, al danneggiato provare il dolo o un profilo di negligenza nell'attività di trattamento, essendo questi aspetti "soggettivi" presunti sino a prova contraria, per il fatto che v'è stata un'attività di trattamento violativa del GDPR dannosa. La Corte europea, nel caso in esame, si è concentrata sul coordinamento tra regole di prevenzione e regole di responsabilità, sostanzialmente ribadendo le considerazioni già sviluppate nel di poco precedente caso *Natsionalna agentsia za prihodite* (CGUE, III sez., 14 dicembre 2023, VB c. Natsionalna agentsia za prihodite, C-340/21, in www.curia.europa.eu.) e che si ritrovano, peraltro, anche nel successivo ar-

ropea, ma con la precisazione, per la prima disposizione normativa, che «il diritto ad ottenere il risarcimento del danno è sancito conformemente al diritto dell'Unione e nazionale»[93]. Questa specificazione

---

resto *MediaMarktSaturn* (CGUE, III sez., 25 gennaio 2024, BL c. *MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, §§ 35 ss., in *www.curia.europa.eu*). In sintesi, per la Corte, il dovere di mettere in campo misure tecnico-organizzative e di sicurezza adeguate ai rischi inerenti al trattamento, desumibile dagli artt. 24 e 32 GDPR (letti alla luce dei Considerando nn. 74, 76 e 83), i quali ribadiscono e precisano l'obbligo generale, sancito all'art. 5, par. 2, di conformarsi al Regolamento e di essere in grado di offrirne la prova (*principio di accountability*), tende ad una prevenzione di tali rischi non ad ogni costo, bensì proporzionata alla relativa probabilità e gravità, da apprezzare in relazione alla natura, al contesto, all'ambito applicativo e alla finalità del trattamento stesso.

[93] Cfr., riguardo all'art. 82 GDPR ed al fatto che esso debba essere interpretato secondo gli orientamenti unionali, G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove leggi civili commentate*, 2017, 1 ss., 6; U. SALANITRO, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di Giustizia*, in *Rivista di diritto civile*, 2023, 430, secondo cui occorre abbandonare l'impostazione localista e porsi alla ricerca del sistema e delle categorie a livello sovranazionale per cogliere le peculiari caratteristiche di un sistema europeo della responsabilità; G. NAVONE, *Ieri, oggi e domani della responsabilità civile da illecito trattamento dei dati personali*, in *Nuove leggi civili comm*entate 2022, 132 ss. Quest'ultimo Autore sottolinea che le decisioni della Corte lussemburghese, per comune consenso munite di autorità di cosa interpretata *ultra partes* sono le sole idonee a disciplinare i profili trascutati dalla regola scritta, e i *dicta* resi in sede di rinvio pregiudiziale, vincolanti per tutti i giudici nazionali cui venga sottoposta un'analoga questione, introdurrebbero gocce di diritto uniforme che s'insinuano negli spazi lasciati vuoti dalla fonte regolamentare, colmandoli. Chi scrive ritiene sia più condivisibile quanto affermato da chi (L. NIVARRA, *Il disordine delle fonti e l'ordine del diritto*, in *Rivista critica di diritto privato*, 2021, 158 s.), pur riconoscendo la centralità della Corte del Lussemburgo nel «processo di armonizzazione degli ordinamenti nazionali» e nella messa a punto delle «tecniche grazie alle quali il primato del diritto europeo, una volta proclamato *in apicibus*, è andato progressivamente guadagnando di effettività», dubita dell'idea «oggi molto diffusa, che la giurisprudenza della Corte di Giustizia possieda dignità di fonte del diritto». Il medesimo Autore afferma che la straordinaria concentrazione di potere in capo alla Corte del Lussemburgo (i cui giudici sono nominati di comune accordo dai governi degli Stati membri, senza il coinvolgimento del Parlamento europeo e di quelli nazionali), suscita più di una perplessità in ordine alla legittimità democratica di questo «inedito e "complesso" demiurgo» (sempre NIVARRA, *Il disordine delle fonti e l'ordine del diritto*, cit., 159). Ci si permette di

non significa che venga meno l'unità della nozione nel diritto dell'Unione, anzi la sua esistenza trova conferma nel richiamo successivo all'opera interpretativa della Corte di Giustizia per quanto riguarda il concetto di «danno»[94]. È però evidente che una norma così generica non aiuti la costruzione di una responsabilità civile europea, dovendosi appoggiare la medesima alla stampella dei diritti nazionali. E di qui sorge il chiaro rischio di un'eterogeneità di tutele, ancor più grave, considerato che la materia trattata dal regolamento EHDS si riferisce a rapporti perlopiù extradomestici[95].

In linea generale, e in mancanza di chiari riferimenti in un senso o nell'altro, la disciplina della responsabilità contrattuale o di quella extracontrattuale dovrà poi essere scelta, distinguendo i casi, a seconda dell'inquadramento che si dà del rapporto tra le parti[96]. Si tratta di una valutazione ermeneutica necessaria e doverosa, considerando che

---

aggiungere che fino a che la normativa unionale sarà così scarna e laconica sul fronte della responsabilità, un sistema europeo rischia di poggiare sulle spalle troppo leggere della giurisprudenza europea, spesso condizionata dalla decisione del caso concreto e quindi con il rischio di risultare ondivaga o incerta.

[94] Nello stesso senso, vedi S. Corso, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, cit., 595.

[95] Sulla frammentarietà e incompletezza del formante legislativo europeo, si rinvia agli studi di H. W. Micklitz, *Il fascino del diritto privato europeo*, in *Contratto e impresa/Europa*, 2021, 103 ss.

[96] Per quanto riguarda il GDPR, in maniera discutibile, vedi Cass., sez. I, 17 settembre 2020, n. 19328, in *Dejure*, che pure decideva riguardo un fatto al quale era applicabile la disciplina previgente di cui all'art. 15 D.Lgs. n. 196 del 2003, e che incidentalmente ha rilevato che lo schema della predetta disciplina ha trovato parziale conferma nell'art. 82 del GDPR, «che sulla base del principio di responsabilizzazione addossa al titolare del trattamento dei dati il rischio tipico di impresa (art. 2050 c.c.)». In dottrina, si è poi ritenuto di poter fare riferimento al modello di responsabilità, inteso in senso non pienamente oggettivo, delineato nell'art. 1218 c.c., sull'assunto che, quasi sempre, la violazione di cui alla regola del GDPR consisterebbe nell'inadempimento di una vera e propria obbligazione. Cfr. F. Bravo, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in N. Zorzi Galgano (a cura di) *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, Wolters Kluwer, 2019, 384 ss., il quale parla di responsabilità "ancipite", riferendo il regime aquiliano all'ipotesi di danno cagionato dal responsabile che si sia discostato dalle legit-

manca una puntuale regolamentazione di aspetti rilevanti in materia di responsabilità, come un qualsivoglia accenno all'elemento soggettivo, alla prova liberatoria, al termine di prescrizione dell'azione risarcitoria ed al perimetro della risarcibilità del danno (e tale laconicità testuale, lo si ripete, appare il motivo del riferimento ancillare al diritto degli Stati membri).

Nell'ambito di una qualificazione del rapporto come extracontrattuale, occorre valutare se sia sufficiente, per ritenersi sussistente un danno, la sola condotta, vale a dire, la «violazione del Regolamento», oppure se sia altresì necessaria l'individuazione di una specifica lesione di un interesse giuridicamente protetto, come previsto dal nostro art. 2043 c.c. Secondo l'interpretazione preferibile dell'art. 82 GDPR, traslabile in questo contesto, pur non essendo il danno aggettivato come ingiusto, la sola violazione di una disposizione del Regolamento non può aprire immediatamente, di per sé sola, le porte al risarcimento, giacché la funzione selettiva dei danni risarcibili, svolta dogmaticamente dalla clausola dell'ingiustizia, è sostituita dagli esiti selettivi dell'eventuale bilanciamento tra ragioni della persona e ragioni pubblicistiche/solidaristiche e/o del mercato [97]. Anche in caso di responsabilità contrattuale, non ogni violazione sarà qualificabile alla stregua di inadempimento di un obbligo specificamente connotante il rapporto tra le parti, giacché non ogni regola di condotta prevista nell'impianto regolamentare corrisponde a una prestazione *ex lege* imposta per l'immediata soddisfazione dell'interesse che vanta il soggetto leso.

Ciò considerato, il regolamento EHDS disegna il formarsi di un rapporto che prevede la presenza di quattro parti: chi genera i dati (l'interessato), chi li detiene per fini di cura (titolare dei dati), chi ne

time istruzioni fornitegli dal titolare del trattamento, e richiamando il regime contrattuale per il resto.

[97] Cfr., in modo analogo, con riferimento alla disciplina di cui all'art. 82 GDPR, C. CAMARDI, *Illecito trattamento dei dati e danno non patrimoniale,* in *Nuova giurisprudenza civile commentata,* 2023, 1141.

gestisce l'accesso (l'autorità per l'accesso ai dati) e chi ne chiede e poi ne ottiene la disponibilità per fini di riutilizzo (utente dei dati).

Profili di responsabilità si possono verificare nelle deviazioni rispetto ai termini e alle condizioni di accesso e riuso del flusso di dati ovvero laddove si verifichi una violazione nel trattamento dei dati personali (accesso non autorizzato, perdita o alterazione delle informazioni). In questo contesto, si può configurare alla base un rapporto *lato sensu* contrattuale sia tra l'interessato e il titolare dei dati, che tra l'interessato e l'Organismo per l'accesso ai dati sanitari.[98] Appare palese, infatti, che si instauri, anche al di fuori di una vera relazione contrattuale, un rapporto di fiducia tra le parti sopramenzionate, fiducia che è uno dei principali obiettivi dichiarati di questa normativa. Tale fiducia è puntellata e rafforzata, sia dalla posizione di soggetto pubblico ricoperta, che da una serie di obblighi già più volte menzionati e

[98] Quando si fa riferimento alla natura «contrattuale» della responsabilità di cui all'art. 1218 c.c., in realtà, si utilizza una semplificazione del linguaggio giuridico, in quanto – a ben guardare – si tratta di una responsabilità diversa da quella aquiliana e che ha come presupposto la violazione di un'«obbligazione» o di un altro «obbligo» di eseguire una «prestazione» non necessariamente di fonte contrattuale (cfr. M.C. Bianca, *Diritto civile*, 5, *La responsabilità*, 2a ed., Milano, Giuffrè, 2012, 1, ove si precisa che «la responsabilità per inadempimento è detta contrattuale a prescindere dalla fonte contrattuale o non contrattuale dell'obbligazione inadempiuta». Nello stesso senso, anche G. Visintini, L. Cabella Pisu, *L'inadempimento delle obbligazioni*, in *Tratt. dir. priv.*, diretto da P. Rescigno, vol. 9, *Obbligazioni e contratti*, tomo I, Torino, Utet, 1984, 155, per le quali la regola generale in materia di responsabilità del debitore, contenuta nell'art. 1218 c.c., viene «preferibilmente definita "contrattuale" dalla dottrina a causa del prevalere delle obbligazioni derivanti da contratto e rappresenta il tentativo del legislatore di riassumere in una disciplina uniforme una casistica, a dire il vero, molto varia a causa della diversa natura dei contratti e dei diversi modi di inadempimento»). Nel caso in cui fosse accertata una responsabilità *lato sensu* contrattuale, la scarna disciplina presente nel regolamento EHDS dovrà poi essere integrata con le norme generali che regolano nel nostro ordinamento la responsabilità per inadempimento di un'obbligazione, applicando la relativa ripartizione dell'onere probatorio, i limiti di risarcibilità di cui all'art. 1225 c.c. ed il termine prescrizionale decennale, tenendo conto che, in ogni modo, dovrà essere garantito un pieno ed effettivo risarcimento per il danno subito.

indicati dalla normativa europea a carico sia del titolare dei dati sanitari, che dell'Organismo per l'accesso ai dati sanitari, che proiettano tali relazioni nella dimensione del rapporto obbligatorio. In queste ipotesi, quindi, la responsabilità sarà disciplinata dall'art. 1218 c.c., che disciplina l'inadempimento di obblighi di natura contrattuale. [99] Profili di responsabilità di natura extracontrattuale, invece, non rinvenendosi un previo rapporto tra le parti, sono attribuibili al *data user* nei confronti dell'interessato, se si verifichi una sua violazione volontaria o colposa nel trattamento dei dati, da cui derivi una fuga di dati potenzialmente o concretamente capace di re-identificare l'interessato medesimo, condotta esplicitamente vietata dal Regolamento, in coerenza con la tutela dei diritti fondamentali tutelati dal GDPR, e ad essa potrà affiancarsi, in concorso, una responsabilità dell'Organismo per l'accesso ai dati sanitari, che male abbia valutato le capacità dell'utente dei dati, anche dal punto di vista della sicurezza dell'ambiente proposto, in fase di richiesta di autorizzazione.

Invece, la relazione tra il *data user* che formuli richiesta di accesso e riuso e l'Organismo di accesso ai dati sanitari, che dovrebbe autorizzare il trattamento, per la sua complessità, viene approfondita qui di seguito.

Per «autorizzazione ai dati», secondo il reg. Ue EHDS (art. 2, par.

---

[99] *Amplius*, sulla natura «contrattuale» di tale tipo di rapporti, mi si consenta il rinvio a S. FAILLACE, *La controversa categoria delle obbligazioni ex lege*, Milano, Wolters Kluwer, 2023, 177 ss.; ID., *La natura e la disciplina delle obbligazioni di cui all'art. 25 del GDPR, espressione dei principi di privacy by design e di privacy by default*, in *Contratto e impresa*, 2022, 1123 ss. Ma in tal senso, vedi anche F. BRAVO, *L' «architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 775-854. Vedi pure F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Le nuove leggi civili commentate*, 2017, 390; B. PARENZO, *Note sparse in tema di responsabilità da illecito trattamento dei dati personali (a partire da due premesse)*, in *Rassegna di diritto civile*, 2024, 882. Tale posizione origina dalla nota teoria di Carlo Castronovo (a partire da C. CASTRONOVO, *L'obbligazione senza prestazione, ai confini tra contratto e torto*, in *Le ragioni del diritto. Scritti in onore di L. Mengoni*, Milano, Giuffrè, 1995, I, 148 ss.

2, lett. v), si intende «una decisione amministrativa emessa nei confronti di un utente dei dati sanitari da un organismo responsabile dell'accesso ai dati sanitari per il trattamento di determinati dati sanitari elettronici specificati nell'autorizzazione di cui trattasi per finalità specifiche correlate all'uso secondario, sulla base delle condizioni stabilite al capo IV del presente regolamento». In linea generale, l'autorizzazione si può definire come un atto provvedimentale volto a definire presupposti, limiti e condizioni per l'avvio e per il successivo svolgimento di un'attività privata in maniera rispondente alle esigenze degli interessi pubblici coinvolti [100]. Più nel dettaglio, alle autorizzazioni preesiste un diritto soggettivo, allo stato, puramente potenziale, che potrà essere esercitato solo quando la pubblica amministrazione riterrà sussistenti i presupposti fissati dalla legge, in relazione all'interesse pubblico coinvolto. L'autorizzazione risponde dunque essenzialmente ad una funzione di tutela e conservatrice dell'interesse pubblico, di talché i limiti posti dalle norme di legge allo svolgimento di determinate at-

[100] Cfr. R. Villata, *Autorizzazioni amministrative e iniziativa economica privata*, Milano, Giuffrè, 1974, 34, che su questo punto si pone in coerenza con la ricostruzione del Ranelletti (O. Ranelletti, *Scritti giuridici scelti*, a cura di E. Ferrari, B. Sordi, Napoli, Jovene, 1992, III, 37 ss., 77 ss., 235 ss.) e degli altri studiosi dell'istituto autorizzatorio. Cfr. anche G. Zanobini, *Corso di diritto amministrativo*, Milano, 1958, I, 262; A. Sandulli, *Notazioni in tema di provvedimenti autorizzativi*, in *Rivista trimestrale di diritto pubblico*, 1957, 784 ss.; Id., *Abilitazioni, autorizzazioni, licenze*, in *Rassegna di diritto pubblico*, 1958, 3 ss.; F. Franchini, *Le autorizzazioni amministrative costitutive di rapporti giuridici fra l'amministrazione e i privati*, Milano, Giuffrè, 1957, nonché, più di recente, F. Fracchia, *Autorizzazione amministrativa e situazioni giuridiche soggettive*, Napoli, Jovene, 1996; Id., *Autorizzazioni amministrative*, in S. Cassese (a cura di), *Dizionario di diritto pubblico*, Milano, Lefebvre Giuffrè, 2006, I, 598 ss., e gli ampi riferimenti dottrinali e giurisprudenziali ivi contenuti. Vedi poi Orsi Battaglini, che fonda la propria ricostruzione innanzitutto sul considerare – come già Villata – una contraddizione il fatto che l'attività di un privato possa essere oggetto di un diritto soggettivo e, al tempo stesso, contraria all'ordinamento (e spesso addirittura penalmente illecita) se posta in essere in assenza o in contrasto con un atto amministrativo «permissivo» (cfr. Cfr. A. Orsi Battaglini, *Autorizzazione amministrativa*, in *Digesto delle discipline pubblicistiche*, II, Torino, Utet, 1987, 1 ss.).

tività vengono rimossi, perché le condizioni della persona richiedente, e dell'atto od opera che essa vuol compiere, danno sufficiente garanzia che tutte le esigenze giuridiche e sociali, in nome delle quali quei limiti furono posti all'attività individuale, saranno rispettate.

L'autorizzazione viene quindi ricondotta all'interno della categoria dei provvedimenti di carattere accrescitivo o migliorativo delle posizioni giuridiche dei destinatari, e, in particolare, dei diritti soggettivi, non creandoli *ex novo*, poiché essi originano e si radicano nella Costituzione, bensì consentendo alle facoltà in essi potenzialmente insite di essere esercitate in atto e in concreto [101].

Come noto, il diritto alla protezione dei dati personali è diritto fondamentale, ma nel contesto giuridico europeo vive in relazione con altri diritti di pari livello, va con essi bilanciato e pertanto non è pre-

---

[101] L'Unione europea ha disciplinato direttamente, tramite Regolamenti o più frequentemente tramite Direttive, alcune delle autorizzazioni o atti di assenso (la distinzione non assume particolare rilievo nell'ottica eurounitaria) funzionali alla cura e alla tutela di interessi pubblici diversi da quelli economici e commerciali, eppure ritenuti fondamentali dallo stesso ordinamento eurounitario, quali ad esempio gli interessi ambientali. A questo riguardo, basti pensare alle valutazioni ambientali (valutazione ambientale strategica, valutazione di impatto ambientale, valutazione di incidenza sugli *habitat* e sulle specie prioritari), all'autorizzazione integrata ambientale, alle autorizzazioni alle emissioni industriali. La normazione eurounitaria, e, in particolare la Direttiva 2006/123/CE sulla libera circolazione dei servizi e il diritto di stabilimento (la c.d. «Direttiva Bolkestein»), elabora una nozione amplissima e sostanzialmente neutra di autorizzazione, come si evince dal Considerando 39, secondo cui «la nozione di regime di autorizzazione dovrebbe comprendere, in particolare, le procedure amministrative per il rilascio di autorizzazioni, licenze, approvazioni o concessioni, ma anche l'obbligo, per potere esercitare l'attività, di essere iscritto in un albo professionale, in un registro, ruolo o in una banca dati, di essere convenzionato con un organismo o di ottenere una tessera professionale [...]», nozione pienamente avallata dalla Corte di Giustizia dell'Unione Europea, che vi ha ricondotto addirittura le concessioni di beni demaniali marittimi, lacuali e fluviali. La medesima Direttiva però ammette regimi di tipo autorizzatorio (nell'accezione ampia e neutra appena riferita) solo qualora siano necessari per "motivi imperativi di interesse generale", tra i quali non possono rientrare ragioni di tipo economico, e comunque nel rigoroso rispetto dei principi di proporzionalità e di non discriminazione.

dicabile una sua aprioristica prevalenza, tale da imporlo ad altre situazioni soggettive. Ciò emerge anche dal già più volte richiamato Considerando n. 4, GDPR, secondo il quale il diritto alla protezione dei dati personali «non è una prerogativa assoluta ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità». L'autorizzazione all'utilizzo di dati sanitari, normata dal Regolamento EHDS, si configura come un provvedimento che, verificate previamente tutte le condizioni tecniche e giuridiche, facoltizza il *data user* ad utilizzare i dati sanitari elettronici dell'interessato. Si contrappone, quindi, il diritto e/o il potere dell'utente dei dati di svolgere operazioni di trattamento (diritto radicato in alcuni articoli della Costituzione, in particolare, nell'art. 41, relativo all'iniziativa economica privata, nell'art. 33, che introduce il principio di libertà della scienza, e nell'articolo 9, che stabilisce « l'obbligo » della Repubblica di promuovere «lo sviluppo della cultura e della ricerca scientifica e tecnica»), nonché le implicazioni che il riconoscimento di tale diritto o potere ha, con il concorrente diritto dell'interessato a veder protetti i propri dati personali, con le conseguenti necessità di bilanciamento tra i relativi interessi giuridicamente rilevanti, che si confrontano però secondo logiche non (necessariamente) antagoniste [102]. Il *data user*, ottenuta l'autorizza-

[102] La natura delle posizioni giuridiche soggettive nascenti dalla disciplina europea sulla protezione dei dati personali è stata ampiamente dibattuta in dottrina, specie in campo privatistico, già alla luce della disciplina di cui alla Direttiva 95/46/CE, al punto che si è sostenuta la tesi dell'interesse legittimo anche nei rapporti tra soggetti privati (Cfr., a riguardo, G. Resta, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Rivista critica di diritto privato*, 2000, 329, il quale parla appunto di «interesse legittimo di diritto privato», rievocando istituti oggetto di studi meno recenti quali quelli di L. Bigliazzi Geri, *Contributo ad una teoria dell'interesse legittimo nel diritto privato*, Milano, Lefebvre Giuffrè, 1967). Nei rapporti con le pubbliche autorità, nei casi di trattamento dei dati personali, a favore della figura dell'interesse legittimo, cfr. G. Cirillo, *Trattamento pubblico dei dati personali e responsabilità civile della P.A.*, in *Foro amministrativo*, 1999, 3 ss., secondo cui «essendo l'attività di "trattamento" attività pubblicistica in senso stretto, la posizione dell'interessato, almeno secondo il sistema ricevuto, è di interesse legittimo, almeno che non vi

zione, acquisirà la facoltà propria del titolare di effettuare il trattamento per finalità legittime (attività di ricerca e per il perseguimento di interessi meritevoli di tutela), di gestire il trattamento e conformarlo alle proprie esigenze, nonché di trarre utilità anche economica dalle operazioni di trattamento sui dati, qualora ciò sia rispondente alla cornice delineata dalle condizioni di liceità del trattamento e dalle finalità con esso legittimamente perseguite. Ove l'Organismo si rifiuti di rilasciare un'autorizzazione ai dati, tale ente dovrà motivare il proprio diniego (vedi art. 68, par. 9, reg. EHDS) e la motivazione dovrà indicare i presupposti di fatto e le ragioni giuridiche che hanno determinato la decisione, anche in relazione alle risultanze dell'istruttoria, *ex* art.3, legge 241/1990.

In questo quadro, deve poter sempre essere risarcibile (sussistendone i presupposti concreti, naturalmente) il danno derivante dall'illegittimo diniego o dall'annullamento in autotutela dell'atto autorizzatorio da parte dell'Organismo di accesso ai dati sanitari, ovverosia la lesione consistente nell'illegittimo impedimento all'espansione del relativo diritto soggettivo [103]. Così dovrà essere pure ove si volesse addivenire alla configurazione di un rapporto "contrattuale" tra Organismo di accesso ai dati sanitari e *data user*, sulla base dell'individuazione

---

sia una espressa eccezione posta dal legislatore medesimo. Eccezione che non può essere rinvenuta semplicemente nel fatto che sia stata utilizzata la parola diritto». In tal senso, parrebbe propendere anche F. MIDIRI, *Il diritto alla protezione dei dati personali. Regolazione e tutela*, Napoli, Editoriale Scientifica, 2017, 126, che riconosce che «la situazione soggettiva (*de qua*) non è strutturalmente dissimile dall'interesse legittimo», salvo poi affermare che «il diritto alla protezione dei dati personali pare assimilabile alla categoria dei diritti nella quale parte della dottrina amministrativistica dissolve l'interesse legittimo». In argomento, vedi anche G. CARULLO, *Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato,* in *Rivista italiana di diritto pubblico comunitario*, 2020, 131, secondo cui si può ritenere che, quantomeno in tutti i casi in cui il potere di trattare dati personali coattivamente non sia interamente predeterminato dal legislatore, la posizione giuridica soggettiva rinvenibile in capo all'interessato sia qualificabile, nella prospettiva del nostro ordinamento, quale interesse legittimo.

[103] Fin da A.M. SANDULLI, *Lesione di interessi legittimi e obbligazione risarcitoria della pubblica amministrazione*, in *Rivista trimestrale di diritto e procedura civile*, 1963, 1293 ss.

di un "contatto sociale" o di un "contatto amministrativo qualificato" tra queste due parti, considerato l'elemento della fiducia che viene decantato dal regolamento EHDS in più occasioni e che pare confermare la nascita di una relazione molto stretta tra le parti dei rapporti che si instaurano ai sensi di questa normativa [104]. E del resto, anche la giu-

[104] Si veda, ad esempio, il Considerando 4 reg. EHDS, secondo cui, «vista la sensibilità dei dati sanitari elettronici personali, il presente regolamento intende fornire garanzie sufficienti sia a livello dell'Unione, sia a livello nazionale per assicurare un elevato livello di protezione, sicurezza, riservatezza e uso etico dei dati. Tali garanzie sono necessarie per promuovere la fiducia nella gestione sicura dei dati sanitari elettronici delle persone fisiche per l'uso primario e per l'uso secondario quali definiti nel presente regolamento.» In ordine all'impostazione "contrattuale" di cui al testo, non possono non menzionarsi gli scritti di Carlo Castronovo, il quale, dall'idea di un diritto amministrativo paritario, getta le premesse per una riconsiderazione della responsabilità della p.a. su basi relazionali. Lo spunto sul piano normativo è rappresentato dalla legge sul procedimento amministrativo, che impone una serie di precisi obblighi all'amministrazione; l'obiettivo, quello di una «civilizzazione», ove emerge una struttura nella quale i soggetti si fronteggiano con prerogative certo diverse e impari ma reciproche, onde al potere di uno corrisponde un dovere o una soggezione dell'altro, che pure però non è scevro di poteri». Accanto al rapporto di diritto pubblico, nel quale il cittadino è titolare di una situazione di interesse legittimo che si contrappone al potere, e che permane come situazione meramente strumentale di tipo processuale, si affiancherebbe, sin dal primo contatto con l'amministrazione, un rapporto obbligatorio, nel senso minimale, di relazione funzionale alla protezione delle sfere giuridiche coinvolte. La struttura teorica che dà forma a tale relazione, attribuendole la consistenza del rapporto obbligatorio, è quella dell'obbligazione senza prestazione che, a partire dall'ipotesi originaria della *culpa in contrahendo*, ha trovato un ambito di riferimento più ampio in tutte quelle ipotesi in cui «si rivelasse il sorgere di un affidamento in virtù del quale soggetti, sino ad allora estranei, diventano parti di un rapporto che, benché privo di una prestazione, può dirsi ugualmente obbligatorio per gli obblighi di conservazione della sfera giuridica altrui nei quali la buona fede innescata dall'affidamento si concretizza». Secondo tale teoria, l'obbligazione senza prestazione rappresenta, in altre parole, il vincolo di natura obbligatoria minimale che scaturisce dalla buona fede in senso oggettivo, in presenza di una relazione tra soggetti ancora non tradottasi in un rapporto giuridico di natura compiutamente obbligatoria, ma tale da ingenerare il legittimo affidamento in ordine al fatto che da tale relazione non scaturirà alcun pregiudizio per l'altra parte. Tale dottrina

risprudenza più recente della Suprema Corte accoglie questa impostazione, laddove vi sia una lesione del legittimo affidamento del privato in ordine ad un provvedimento della P.A. ampliativo della di lui posizione [105].

---

mette, infatti, in guardia dal riprodurre, per l'obbligazione senza prestazione, le stesse categorie dell'art. 1218 c.c., se non in via analogica, attraverso cioè un riadattamento di senso di quelle categorie che sono «esclusive dell'obbligo di prestazione e in tale limite vanno tenute». Addirittura non sarebbe neppure corretto parlare di inadempimento, né con riguardo agli obblighi di protezione, né tantomeno rispetto all'obbligazione senza prestazione, dal momento che adempimento e inadempimento sono categorie dell'azione riferibili solo all'obbligo di prestazione, sicché sarebbe più corretto parlare di violazione degli obblighi o dell'obbligazione (cfr. C. CASTRONOVO, *Responsabilità civile per la Pubblica Amministrazione*, in *Jus*, 1998, 647 ss.; ID., *La civilizzazione della p.a.*, in *Europa e diritto privato,* 2013, 637 ss.; ID, *L'obbligazione senza prestazione*, *ai confini tra contratto e torto*, in *Le ragioni del diritto*, *Scritti in onore di L. Mengoni*, Milano, Giuffrè, 1995, I, 148 ss.; ID., *La nuova responsabilità civile*, Milano, Giuffrè, 2006, 443 ss.; vedi pure A. IULIANI, *La responsabilità civile della pubblica amministrazione; alcune riflessioni intorno all'interesse legittimo dalla prospettiva dei rimedi*, in *Contratto e impresa*, 2016, 1196 ss. Sulla figura del contatto sociale, tra le opere monografiche, mi si consenta il rinvio a S. FAILLACE, *La responsabilità da contatto sociale*, Padova, 2004, Cedam, *passim*, e più di recente a F. VENOSTA, *Contatto sociale e affidamento*, Milano, Giuffrè, 2021).

[105] Cfr., in tal senso, la recentissima Cass. civ. 19 maggio 2025, n. 13289, in *Dejure*. Nel caso di specie, una società aveva presentato un'istanza per ottenere il certificato di compatibilità ambientale e l'autorizzazione per costruire e gestire un impianto microidroelettrico. Tuttavia, il provvedimento concessorio poi rilasciato fu, all'esito di vari gradi di giudizio, annullato, a seguito dell'impugnativa presentata da alcune associazioni ambientaliste. La società avviò, quindi, un'azione risarcitoria, sostenendo di aver fatto legittimo affidamento sulla validità dei provvedimenti poi annullati. Nel decidere la controversia, la Cassazione, pur respingendo il ricorso, affermando che la pendenza del giudizio impugnatorio esclude che il privato possa considerarsi in buona fede, con riguardo alle conseguenze derivategli per fatti verificatisi dopo l'avvio del giudizio dall'aver confidato nella legittimità dell'atto, ha confermato l'orientamento per cui la responsabilità della pubblica amministrazione per lesione dell'affidamento incolpevole del privato non è qualificabile né come extracontrattuale, né come contrattuale in senso proprio. Si configura, piuttosto, come una responsabilità di tipo relazionale o da «contatto sociale qualificato». In motivazione, si legge, in continuità con Cass. Sez. un., 19 gennaio 2023 n. 25324 (in *Dejure*),

Questione assai rilevante in ordine alla risarcibilità di tale posizione

che «il pregiudizio non deriva dalla violazione delle regole di diritto pubblico sull'esercizio della potestà amministrativa, bensì, in una più complessa fattispecie, dalla violazione dei principi di correttezza e buona fede, che devono governare il comportamento dell'amministrazione e si traducono in regole di responsabilità, non di validità dell'atto; pertanto, l'affidamento incolpevole, la cui lesione potrebbe determinare la responsabilità risarcitoria della P.A. è "una situazione autonoma, tutelata in sé, e non nel suo collegamento con l'interesse pubblico, come affidamento incolpevole di natura civilistica, che si sostanzia, secondo una felice sintesi dottrinale, nella fiducia, nella delusione della fiducia e nel danno subito a causa della condotta dettata dalla fiducia mal riposta: si tratta, in sostanza, di un'aspettativa di coerenza e non contraddittorietà del comportamento dell'amministrazione fondata sulla buona fede" (così, Cass., Sez. Un., n. 8236/2020, in motivazione)». Secondo la Suprema Corte (Cass. 19 maggio 2025 n. 13289, cit.), la prospettiva da cui muovere non è più quindi quella della responsabilità aquiliana, ex art. 2043 c.c., (l'orientamento favorevole a tale impostazione era stato inaugurato da Cass. Sez. Un. 23 marzo 2011 n. 6594, 6595 e 6596, in *Dejure*), poiché è ormai ampiamente consolidata l'impostazione secondo cui «la responsabilità della P.A. per lesione dell'affidamento incolpevole del privato non consista affatto nella c.d. "responsabilità del passante", essendo ravvisabile un *quid pluris* rispetto al generale precetto del *neminem laedere*; infatti, la responsabilità sorge tra soggetti che si conoscono reciprocamente già prima che si verifichi un danno; danno che consegue non alla violazione di un dovere di prestazione, ma alla violazione di un dovere di protezione, il quale sorge non da un contratto, ma dalla relazione che si instaura tra l'amministrazione ed il cittadino nel momento in cui quest'ultimo entra in contatto con la prima». Occorre, dunque, sempre secondo Cass. 19 maggio 2025 n.13289, cit., che il privato dimostri il contatto sociale qualificato, ossia il rapporto inerente al provvedimento autorizzatorio richiesto, nonché lo specifico comportamento – *lato sensu* inteso – della P.A., che si pretende reso in violazione dei doveri di correttezza e buona fede e tale da ingenerare, sotto il profilo eziologico, il proprio legittimo convincimento di poter confidare nella piena legittimità dell'atto amministrativo e di poter quindi determinarsi nelle conseguenti attività, quali gli esborsi occorrenti per l'esercizio delle relative facoltà; il privato, infine, deve dimostrare il danno in tesi subito (da rapportarsi, di regola, al c.d. interesse negativo), ed il nesso di causalità tra il comportamento illegittimo della P.A. e il danno stesso. La P.A. ha – per contro – l'onere di dimostrare o che il suddetto comportamento omissivo non vi è stato, o che esso (sia commissivo, che omissivo) non è rilevante sotto il profilo eziologico, oppure che l'evento di danno non è ad essa imputabile, per non esserle addebitabile la colpa, che com'è noto, ai sensi dell'art. 1218 c.c., si presume. Tale onere differenziale, a carico della P.A., se-

soggettiva appare peraltro quella dell'ampiezza della discrezionalità o delle valutazioni tecniche rimesse (sempre in base alla legge e ai limiti da essa posti) all'Autorità amministrativa in sede di esercizio del potere autorizzatorio. Quanto maggiore è tale ampiezza, tanto il diritto preesistente risulta nella sostanza incerto nella sua possibilità di esplicazione, condizionato ad apprezzamenti lati e opinabili, pur sempre soggetti, però, al principio di legalità, ai principi generali dell'azione amministrativa, al sindacato giurisdizionale di legittimità e risarcitorio [106].

Dal canto suo, il *data user*, oltre ad osservare un generale impegno a trattare il flusso di dati in conformità con il quadro etico-giuridico applicabile e a rendicontare – in termini di *accountability* – la conformità del riuso dei dati rispetto a quanto dichiarato in sede di richiesta di accesso, assume l'impegno specifico di rendere pubblici i risultati o gli esiti dell'uso secondario dei dati sanitari elettronici, comprese le informazioni pertinenti per la prestazione di assistenza sanitaria, entro 18 mesi dal completamento del trattamento dei dati sanitari elettronici. Il risultato, inoltre, deve essere reso pubblico nelle sintesi divulgative [107]. Una deviazione o un vero e proprio inadempimento da tali ob-

---

condo la Suprema Corte, vale dunque a caratterizzare il regime probatorio che discende dalla ripetuta qualificazione della responsabilità in parola quale responsabilità da «contatto sociale qualificato», rispetto alla mera responsabilità aquiliana, in cui l'intero onere probatorio sugli elementi caratterizzanti la fattispecie (compreso l'elemento psicologico) grava sul preteso danneggiato.

[106] Sotto questo profilo, è da evidenziare lo sforzo del legislatore Unionale che tenta di uniformare per quanto possibile il meccanismo autorizzativo. Cfr., infatti, il Considerando n. 73 reg. EHDS, secondo cui: «Al fine di garantire che tutti gli organismi responsabili dell'accesso ai dati sanitari rilascino autorizzazioni ai dati in modo simile, è necessario istituire un processo comune *standard* per il rilascio delle autorizzazioni ai dati, con richieste simili nei vari Stati membri. Il richiedente di dati sanitari dovrebbe fornire agli organismi responsabili dell'accesso ai dati sanitari diverse informazioni che li aiuterebbero a valutare la domanda di accesso ai dati sanitari e a decidere se il richiedente di dati sanitari può ricevere un'autorizzazione ai dati e si dovrebbe garantire la coerenza tra diversi organismi responsabili dell'accesso ai dati sanitari».

[107] Secondo l'art. 63 reg. EHDS, quando svolgono i compiti di monitoraggio e

blighi creerà, oltre all'irrogazione di sanzioni amministrative, una responsabilità da fatto illecito nei confronti dell'interessato.

Per quanto riguarda, infine, il concetto di danno risarcibile, esso dovrebbe essere interpretato in senso lato, alla luce della giurisprudenza della Corte di giustizia, in modo da rispecchiare pienamente gli obiettivi del regolamento EHDS (Cfr. Considerando 101 EHDS), sempre facendo salve le eventuali richieste di risarcimento danni derivanti dalla violazione di altre norme del diritto dell'Unione o nazionale [108]. Le persone fisiche dovrebbero, quindi, ottenere pieno ed ef-

---

controllo a norma dell'articolo 57, paragrafo 1, lettera a), punto ii), gli organismi responsabili dell'accesso ai dati sanitari hanno il diritto di chiedere e ricevere dagli utenti dei dati sanitari e dai titolari dei dati sanitari tutte le informazioni necessarie per verificare la conformità al presente capo. Qualora concludano che un utente dei dati sanitari o un titolare dei dati sanitari non rispetta le prescrizioni del presente capo, gli organismi responsabili dell'accesso ai dati sanitari ne informano immediatamente l'utente dei dati sanitari o il titolare dei dati sanitari e adottano misure appropriate. L'organismo responsabile dell'accesso ai dati sanitari interessato dà all'utente dei dati sanitari o al titolare dei dati sanitari interessato la possibilità di esprimere il proprio parere entro un termine ragionevole che non deve superare le quattro settimane. Qualora l'accertamento della non conformità riguardi una possibile violazione del regolamento (UE) 2016/679, l'organismo responsabile dell'accesso ai dati sanitari interessato informa immediatamente le autorità di controllo a norma dello stesso e fornisce loro tutte le informazioni pertinenti in merito a tale risultanza. Per quanto riguarda la non conformità da parte degli utenti dei dati sanitari, gli organismi responsabili dell'accesso ai dati sanitari hanno il potere di revocare l'autorizzazione ai dati rilasciata a norma dell'articolo 68 e di interrompere senza indebito ritardo il trattamento dei dati sanitari elettronici interessato da parte dell'utente dei dati sanitari, e adottano misure adeguate e proporzionate volte a garantire un trattamento conforme da parte degli utenti dei dati sanitari. Nel quadro di tali misure di esecuzione, se del caso, gli organismi responsabili dell'accesso ai dati sanitari possono anche escludere o avviare procedimenti per escludere, in conformità del diritto nazionale, l'utente dei dati sanitari interessato dall'accesso ai dati sanitari elettronici all'interno dello spazio europeo dei dati sanitari nel contesto dell'uso secondario per un periodo massimo di cinque anni.

[108] La Corte Ue con sentenza 4 maggio 2023 (causa C-300/21), in *Foro italiano*, 2023, IV, 268 ss., con note di A. Palmieri, R. Pardolesi, *Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)*; C. Scognamiglio, *Danno e risarcimen-*

fettivo risarcimento per il danno subito, ad esempio, in caso di fatti

---

to nel sistema del Rgpd: un primo nucleo di disciplina eurounitaria della responsabilità civile?, in *Nuova giurisprudenza civile commentata*, 2023, 1150 ss., in primo luogo ha smentito la tesi secondo la quale qualsiasi violazione del Regolamento implicherebbe un danno, facendo leva su due argomenti, l'uno di carattere letterale, l'altro sistematico. Nel primo senso, si è rilevato come dalla formulazione dell'art. 82 GDPR, emerga «chiaramente che l'esistenza di un "danno" che sia stato "subíto" costituisce una delle condizioni del diritto al risarcimento» e che «la menzione distinta di un "danno" e di una "violazione" [...] sarebbe superflua se il legislatore dell'Unione avesse ritenuto che una violazione delle disposizioni del regolamento in parola possa essere sufficiente, da sola e in ogni caso, a dare fondamento a un diritto al risarcimento»; inoltre, sul piano sistematico, si segnala come lo stesso Regolamento preveda, per il caso di una sua violazione, *altri rimedi,* diversi da quello risarcitorio di cui all'art. 82 GDPR., i quali, diversamente appunto da quest'ultima disposizione, non richiedono espressamente, per poter essere attivati, la causazione di un danno all'interessato. Nella stessa sede, la Corte tiene a rimarcare come l'art. 82 GDPR non subordini la risarcibilità del danno al superamento di una determinata soglia di gravità e che una tale subordinazione «(...) rischierebbe di nuocere alla coerenza del regime istituito dal GDPR, poiché la graduazione di una siffatta soglia, da cui dipenderebbe la possibilità o meno di ottenere detto risarcimento, potrebbe variare in funzione della valutazione dei giudici aditi(...)». La Corte Europea, quindi, stigmatizza quegli orientamenti nazionali, sino ad oggi seguiti anche dalla giurisprudenza italiana, secondo cui il risarcimento del danno in discorso dovrebbe essere bilanciato col principio di solidarietà che implica di verificare, ai fini della risarcibilità, il superamento di un non meglio identificato limite di tollerabilità della lesione. Infine, il Giudice Europeo, vista l'assenza di norme unionali sul punto del *quantum* risarcibile, ne rimanda all'ordinamento giuridico di ciascuno Stato membro l'individuazione, nel rispetto dei principi di equivalenza e di effettività del diritto dell'Unione. Dunque, in base all'art. 82, GDPR e al considerando 146, deve essere garantito un «(...) pieno ed effettivo risarcimento per il danno subito (...)» che, «tenuto conto della funzione compensativa del diritto al risarcimento previsto dall'art. 82 del GDPR (...)», valga a «(...)compensare integralmente il danno concretamente subito a causa della violazione di tale regolamento (...)». (Cfr., in argomento, B. PARENZO, *Note sparse in tema di responsabilità da illecito trattamento dei dati personali (a partire da due premesse)*, in *Rassegna di diritto civile*, 2024, 892 ss.) In senso critico rispetto all'orientamento della Cassazione (cfr., in tale filone giurisprudenziale stigmatizzato dalla Corte di Giustizia, ad esempio, Cass., 4 giugno 2018, n. 14242, in *Giurisprudenza italiana,* 2019, 43 ss.), che, ai fini della liquidazione di un danno non patrimoniale, adotta i filtri selettivi della «gravità della lesione» e della «serietà del danno», ed utilizza in maniera distorta il principio di

che abbiano come effetto quello della re-identificazione di persone fisiche, del trasferimento di dati sanitari personali al di fuori dell'ambiente di trattamento sicuro e in caso di trattamento dei dati per usi vietati o al di fuori di un'autorizzazione. Peraltro, qualora le autorità di sanità digitale, gli organismi responsabili dell'accesso ai dati sanitari, i titolari dei dati sanitari o gli utenti dei dati sanitari siano coinvolti nello stesso trattamento, ogni attore dovrebbe rispondere per la totalità del danno. Tuttavia, qualora essi siano riuniti negli stessi procedimenti giudiziari conformemente al diritto degli Stati membri, dovrà essere possibile ripartire il risarcimento in base alla responsabilità che ricade su ognuno di questi attori, a condizione che sia assicurato il pieno ed effettivo risarcimento della persona fisica che ha subito il danno. Dovrà pure considerarsi ammissibile, ex art. 2055 del codice civile, pur in assenza di indicazioni normative unionali in tal senso, un'azione di regresso in favore dei soggetti sopra individuati che abbiano corrisposto l'intero risarcimento del danno e nei confronti degli altri soggetti coinvolti nel medesimo trattamento, laddove vi siano responsabilità concorrenti.

7. *Riflessioni conclusive*

Il presente contributo ha tentato di approfondire quali gli strumenti di tutela per l'interessato proposti dall'ordinamento interno e da quello europeo, in caso di trattamenti di dati sanitari al fine di cura del singolo e per la tutela dei bisogni della collettività. La materia, come noto, è sempre più attuale, in quanto il progresso scientifico ri-

---

solidarietà, vedi F. Bravo, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contratto e impresa*, 2023, 426 ss. e Id., *Il principio di solidarietà*, in F. Bravo (a cura di), *Dati personali. Protezione, libera circolazione e Governance. 1. Principi*, Pisa, Pacini, 2023, 598 ss. In conformità con la sentenza del 4 maggio 2023 (causa C-300/21), può citarsi anche Corte Giust. UE 4 ottobre 2024, causa C-507/23, PTAC, che afferma possa trovare ristoro anche il cosiddetto danno bagatellare.

chiede che le autorità sanitarie procedano a raccogliere, conservare ed elaborare i dati sanitari dei singoli, per poter così fornire prestazioni di prevenzione, diagnostiche e di cura aggiornate ed efficaci, anche con l'ausilio di *software* caratterizzati da forme di intelligenza artificiale. Tale attività deve però mantenersi in equilibrio sul sottile filo che contempera il diritto all'autodeterminazione informativa con la libera circolazione dei dati per fini di ricerca scientifica.

A riguardo, si è convenuto, innanzitutto, che l'utilizzabilità universale delle numerose banche dati e biobanche, reti telematiche e piattaforme digitali esistenti è utile solo se i dati ivi presenti sono aggiornati, affidabili e interoperabili, nel rispetto del principio di minimizzazione. Peraltro, nel valutare le esperienze dei singoli Stati membri, si è appalesata una frammentazione di disciplina che, invero, ha reso problematico l'approccio europeo alla recente pandemia da Covid. In quel frangente, si è concepita l'idea della nascita di uno spazio europeo di condivisione di dati sanitari, visto non come un deposito centralizzato di dati, ma come un'architettura condivisa per stabilire regole comuni, procedure, *standard* tecnologici e infrastrutture. Come si è visto, tale nuova disciplina, appena entrata in vigore, ma con tempi per la sua reale applicabilità molto lunghi, è foriera di una diversa concezione di tutela del dato sanitario rispetto al GDPR e alla disciplina domestica di settore (che regola il fascicolo sanitario elettronico e il nuovo ecosistema di dati sanitari, banca dati che «acquisisce, memorizza e gestisce i dati», poi elaborati per offrire servizi agli esercenti le professioni sanitarie, al Ministero della salute, alle regioni/province autonome e allo stesso interessato). In particolar modo, un forte impatto lo creerà il rovesciamento delle priorità delle basi giuridiche (dalla prevalenza del consenso a quella dell'interesse pubblico, visto quasi come una clausola generale) e l'ampliamento prospettato dei diritti dell'interessato [109].

[109] Anche nella legge italiana sull'intelligenza artificiale, n. 132/2025, all'art. 8 (Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario), la base giuridica dell' «interesse pubblico» sovrasta

Eppure un percorso rilevante, seppur non decisivo, era stato già compiuto nel nostro ordinamento attraverso l'evoluzione del fascicolo sanitario elettronico, creato in origine prevalentemente come strumento che permettesse di costruire il processo di cura attorno al cittadino, proponendo il medesimo non come spettatore passivo di decisioni a lui in larga misura inintelligibili, ma con una rinnovata autodeterminazione decisionale, che si lega a doppio filo ai profili di protezione dei dati personali. Lo scenario è poi cambiato con gli ultimi indirizzi di politica legislativa e l'amplificazione di finalità quali lo studio e la ricerca scientifica in campo medico, biomedico ed epidemiologico, la programmazione sanitaria, la profilassi internazionale.

Nella formulazione originaria, il FSE prevedeva per la sua costruzione la raccolta di due consensi da parte dell'assistito: un consenso

---

e annichilisce quel che resta del «consenso», laddove stabilisce che «i trattamenti di dati, anche personali, eseguiti da soggetti pubblici e privati senza scopo di lucro, dagli Istituti di ricovero e cura a carattere scientifico (IRCCS), di cui al decreto legislativo 16 ottobre 2003, n. 288, nonché da soggetti privati operanti nel settore sanitario nell'ambito di progetti di ricerca a cui partecipano soggetti pubblici e privati senza scopo di lucro o IRCCS, per la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale per finalità di prevenzione, diagnosi e cura di malattie, sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicali, incluse protesi e interfacce fra il corpo e strumenti di sostegno alle condizioni del paziente, salute pubblica, incolumità della persona, salute e sicurezza sanitaria nonché studio della fisiologia, della biomeccanica e della biologia umana anche in ambito non sanitario, in quanto necessari ai fini della realizzazione e dell'utilizzazione di banche di dati e modelli di base, sono dichiarati di rilevante interesse pubblico in attuazione degli articoli 32 e 33 della Costituzione e nel rispetto di quanto previsto dall'articolo 9, paragrafo 2, lettera g), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016. Ai medesimi fini, fermo restando l'obbligo di informativa in favore dell'interessato, che può essere assolto anche mediante un'informativa generale messa a disposizione nel sito *web* del titolare del trattamento e senza ulteriore consenso dell'interessato ove inizialmente previsto dalla legge, è sempre autorizzato l'uso secondario di dati personali privi degli elementi identificativi diretti, anche appartenenti alle categorie indicate all'articolo 9 del regolamento (UE) 2016/679, da parte dei soggetti di cui al comma 1, salvi i casi nei quali la conoscenza dell'identità degli interessati sia inevitabile o necessaria al fine della tutela della loro salute».

«libero e informato» per l'alimentazione (comma 3-*bis*), potendo il cittadino decidere se e quali dati relativi alla propria salute far inserire nel fascicolo, ed un consenso alla consultazione dei dati e documenti da parte del curante. Il consenso all'alimentazione del fascicolo è stato poi eliminato, ed anzi l'alimentazione automatica del fascicolo sanitario è divenuta un diritto riconosciuto legislativamente in favore dell'interessato, prevedendosi, appunto, un obbligo in carico agli esercenti le professioni sanitarie che prendono in cura l'assistito di alimentare il FSE «in maniera continuativa e tempestiva». Un'obbligazione questa, detto per inciso, che, se inadempiuta, può causare una responsabilità dei suddetti operatori sanitari in caso di mancata, intempestiva o inesatta alimentazione. Si è pure visto come, in tale ipotesi, la violazione dell'obbligo di controllare la completezza e la correttezza del fascicolo sanitario elettronico possa configurare anche un inesatto adempimento della prestazione sanitaria, da parte della struttura ospedaliera, per mano del personale suo ausiliario, ex art. 1228 c.c. Si tratta di un inadempimento del contratto di «spedalità» tra paziente e struttura sanitaria, vale a dire quel contratto atipico, pacificamente riconosciuto dalla giurisprudenza, che pone a carico della struttura sanitaria, oltre alla prestazione principale di tipo diagnostico-terapeutico, una serie di altre prestazioni che, contribuendo a riempire di contenuto il concetto di «efficiente standard organizzativo», influiscono sulla delimitazione dei confini della responsabilità.

Rispetto alla consultazione del fascicolo da parte di terzi, l'utente può esprimere un consenso disgiunto per ogni finalità specifica nei confronti dei trattamenti effettuati per diagnosi, cura e riabilitazione, prevenzione e profilassi internazionale. Per le finalità di studio e ricerca scientifica, nonché di governo, l'accesso ai dati è limitato e sono previste specifiche misure tecniche a tutela degli utenti. Si potranno, infatti, estrarre esclusivamente dati anonimizzati e, per le finalità di governo, solo dati aggregati, privati degli elementi identificativi diretti e pseudonimizzati.

Gli interventi del legislatore, soprattutto i più recenti, sembrano, quindi, aver sancito il passaggio del FSE da strumento principalmente

per la persona e la tutela dei suoi diritti fondamentali, primo fra tutti quello alla sua salute, a strumento votato anche a perseguire una maggior efficienza nel contesto del funzionamento del Servizio sanitario nazionale, nelle politiche di governo della sanità e nella ricerca scientifica. L'interesse pubblico rilevante pare infatti fungere da valvola di apertura – attesa anche l'ampiezza dell'elenco delle materie di cui al comma 2, dell'art. 2-*sexies*, GDPR – o addirittura una clausola generale, che sostanzialmente elimina il divieto di trattamento, al ricorrere del generale elemento pubblicistico.

La protezione dei dati viene concepita secondo un paradigma circolatorio differente, informato al principio di solidarietà, oltre la dicotomia persona e mercato, doppia anima sottesa al GDPR.

Tuttavia, l'utilizzo del consenso come base giuridica, tuttora prevalente per l'utilizzo del fascicolo sanitario elettronico e per l'ecosistema dei dati sanitari, per i motivi che riepilogheremo nel prosieguo, rimane fonte di dubbi più che fondati.

E così può dirsi per la medesima tendenza consensocentrica che traspare pure nell'analisi della disciplina ad oggi vigente in merito all'utilizzo ulteriore dei dati sanitari (*secondary use*), desumibile dal GDPR e dal Codice Privacy, disciplina complessa e a tratti oscura, data anche la molteplicità di fonti che la regolano.

Si consideri che, a fronte di una normazione di cui al GDPR controversa in ordine all'uso secondario dei dati, tra svariate basi legittimanti e numerose possibili finalità, una norma nella pratica ha creato una notevole frammentazione a livello europeo. Si tratta dell'art. 9 par. 4 del GDPR, che stabilisce che «gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute». Vi sono, infatti, Stati membri la cui disciplina appare più elastica, ed altri in cui sussistono norme più restrittive. A fronte della facoltà concessa da tale norma, nel nostro ordinamento la regola è il consenso quale condizione di liceità.

Il legislatore italiano, infatti, sulla base dell'ampia delega più volte sopra citata, ha introdotto l'art. 110 del Codice *Privacy*, che stabilisce che i trattamenti dei dati sulla salute, per scopi primari e secondari,

nell'ambito delle sperimentazioni cliniche, sono ammessi solo previa acquisizione del consenso dell'interessato. Si tratta di una disposizione che si riferisce all'utilizzo ulteriore di dati sanitari da parte del titolare che ne ha acquisito la disponibilità per motivi di cura [110]. L'art. 110-*bis* del Codice in materia di protezione dei dati attribuisce, invece, al Garante la facoltà di autorizzare il trattamento ulteriore (quindi per scopo diverso da quello per il quale il dato era stato primariamente raccolto) di dati personali, compresi quelli ex art. 9 GDPR, a scopo di ricerca scientifica o statistica, da parte di soggetti terzi che svolgano principalmente tali attività se, a causa di particolari ragioni, informare gli interessati ai fini della manifestazione del consenso risulta impossibile o implica uno sforzo sproporzionato o, ancora, rischia di rendere irrealizzabile o pregiudicare gravemente il conseguimento delle finalità di ricerca. Al Garante è attribuita anche la possibilità di emanare provvedimenti generali rivolti a determinate categorie di titolari e di trattamenti. In definitiva, quindi, qualunque progetto di riutilizzo dei dati, per essere sottoposto al vaglio del Garante, dovrà dimostrare preventivamente di aver predisposto tutte le misure di protezione dei dati [111].

---

[110] La necessità del consenso come condizione di liceità del trattamento, come visto, conosce solo due eccezioni. La prima deroga trova applicazione quando la ricerca viene svolta in base a disposizioni normative o regolamentari, quali i programmi di ricerca biomedica o sanitaria di cui all'art. 12-*bis* del d.lgs. 30 dicembre 1992, n. 502 oppure quelli previsti dal diritto dell'Unione europea, ai sensi del citato art. 9, par. 2, lett. j) GDPR. In tal caso, il trattamento dovrà essere anticipato dalla redazione di una valutazione di impatto ai sensi degli artt. 35 e 36, GDPR. La seconda deroga rileva ogniqualvolta «a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale. In tali casi, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del presente codice».

[111] Resta escluso dalla nozione di riutilizzo e, pertanto, dall'applicazione dell'art.

È il consenso la base giuridica appropriata anche in base a quanto definito dall'art. 5, commi 2 e 3, delle «Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica», il cui rispetto «costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali» (ex art. 2-*quater*, comma 4, del D. Lgs. 196/2003, Codice *privacy*), con riferimento al trattamento ulteriore di dati sanitari da parte dei soggetti privati che partecipano al Sistema statistico nazionale ai sensi della legge 28 aprile 1998, n. 125.

Ebbene, il consenso non sembra garantire sufficientemente la libertà di scelta dell'interessato, essendo chiara l'asimmetria informativa tra il paziente e il promotore della ricerca clinica. Vi è di più. Il considerando 33 del GDPR sembra non negare o non vietare possibili forme di utilizzo nella ricerca scientifica di un (pur discutibile) consenso ampio, pur apparendo preferibile un consenso a più livelli che fornisca ai partecipanti una gamma di preferenze di consenso ed il consenso dinamico, che utilizza la tecnologia dell'informazione per facilitare, modificare e aggiornare le preferenze di consenso ai progetti. Suscita perplessità, peraltro, anche il repentino cambio di impostazione del Legislatore italiano, che, con la nuova legge sull'intelligenza artificiale, come già ricordato, per finalità connesse al campo della ricerca scientifica e sperimentazione, da un lato, non prevede il consenso dell'interessato per l'uso secondario dei dati sanitari (ma solo un'informativa sul sito *web* del titolare dei dati), dall'altro, a differen-

---

110-*bis*, il trattamento dei dati raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca (ma i soggetti menzionati, a rigore, sarebbero nient'altro che titolari del trattamento, e non terzi). Il motivo di tale eccezione risiede nel fatto che tali enti perseguono finalità di ricerca, prevalentemente clinica e traslazionale, nel campo biomedico e in quello dell'organizzazione e gestione dei servizi sanitari ed effettuano prestazioni di ricovero e cura di alta specialità (art. 1 d.lgs. 16/10/2003, n. 288) e hanno la missione istituzionale di effettuare ricerca nell'interesse della collettività con una diretta ricaduta sull'assistenza del malato, sull'organizzazione e sulla gestione dei servizi sanitari, effettuando prestazioni di ricovero e cura di alta specializzazione.

za di quanto stabilito dal regolamento EHDS, nemmeno introduce una procedura autorizzativa pubblicistica che tuteli l'interessato e/o un diritto di *opt out*.

Tenta di fornire meccanismi di tutela diversi per l'interessato un'altra fondamentale regolamentazione di derivazione europea, spinta anche dall'esigenza pubblicistica di condividere, per fini di prevenzione e ricerca, una quantità maggiore di dati sanitari. Si tratta del cosiddetto *Data Governance Act*, che propone di dare impulso alla costituzione di uno spazio unico europeo dei dati, attraverso la loro condivisione, cui possano accedere, a parità di condizioni, tutti gli operatori economici, comprese le piccole imprese, scardinando in tal modo l'oligopolio delle maggiori. Tale regolamento intende favorire pure la destinazione altruistica dei dati, assecondando un'esigenza sociale emersa prepotentemente con l'esperienza pandemica, che ha posto in luce la necessità del reimpiego dei dati nell'interesse generale, per la promozione, ad esempio, della ricerca scientifica ed il supporto alle politiche sanitarie, nell'acquisita consapevolezza della funzione sociale che la protezione dei dati è chiamata a realizzare. Più in generale, il riutilizzo dei dati protetti detenuti da enti pubblici ed i servizi di intermediazione dei dati, punti focali di tale nuova normativa, sono immaginati dal legislatore europeo anche al servizio del perseguimento di finalità sociali. A rientrare nell'ambito di applicazione oggettivo di tale Regolamento, in particolare, sono le categorie di dati detenuti da enti pubblici e tutelati per ragioni anche di protezione dei dati personali. Ogni soggetto pubblico è libero di decidere se consentire o negare l'accesso per il riutilizzo. Il riutilizzo dei dati personali, inoltre, ai sensi dell'art. 5, comma 3, DGA, è possibile solo qualora l'ente pubblico che concede l'accesso garantisca, tra le altre cose, che i dati siano stati previamente anonimizzati, ossia privati della loro natura di informazione riguardante una persona fisica identificata o identificabile. In tale Regolamento viene anche cristallizzato un modello già registrato nella prassi, basato sul ruolo dell'intermediario di dati che, nel fornire il servizio di *data sharing*, agisce come una sorta di *broker* "*sui generis*" tra «titolare dei dati» e «utente dei dati». L'art. 10, comma 1, contempla tre tipologie di servizi di intermediazione tra loro molto diversi. Le nuove norme ri-

mediano, quindi, alla constatata debolezza dell'interessato nell'esercizio del suo diritto al controllo, che abbisogna di essere supportato (o anche sostituito in questa attività) da soggetti che perseguano finalità non egoistiche. Si presume, infatti, che gli intermediari dei dati aumentino la fiducia nella condivisione dei dati ed eliminino le asimmetrie esistenti di potere e di informazione nell'interporsi in modo neutrale tra i titolari dei dati e gli utenti. In tali servizi di intermediazione, si affacciano una molteplicità di rapporti disegnati dal legislatore europeo – che vanno dalla messa in servizio e gestione di infrastrutture e piattaforme (anche per *data spaces* comuni), ai servizi di elaborazione di dati, alla conservazione temporanea e custodia di dati, all'esercizio su delega di diritti, alla consulenza, a varie attività di controllo sull'operato di terzi (presenti anche nelle attività di riuso e dovute in caso di processazione di dati in ambienti sicuri) – rapporti riconducibili a specifici tipi contrattuali, suscettibili di convergere in contratti a causa complessa o collegati: contratti di somministrazione, appalti di servizi, contratti di mandato od opera professionale, deposito (relativamente alle ipotesi in cui sia prevista la conservazione e custodia, anche solo temporanea, di dati).

Tra le tipologie di intermediari descritti dal *Data Governance Act*, in questo lavoro è stata oggetto di approfondimento la figura nuova, almeno per la nostra esperienza giuridica, della cooperativa di dati, quale strumento atto a rafforzare l'influenza effettiva di un gruppo di interessati sui propri dati personali nei confronti di terzi e, allo stesso tempo, ad assoggettare tale risorsa a regole comuni di utilizzo, in vista di un obiettivo collettivo [112]. La cooperativa di dati, insomma, dovrebbe avere la capacità di fornire agli individui e alle comunità le risorse e le conoscenze per valutare i termini del consenso. I membri della cooperativa, dopo essersi giovati della consulenza dalla struttura, saranno più propensi ad accettare condizioni favorevoli e, dopo il consenso, potranno avvalersi delle competenze della cooperativa per valutare

[112] Cfr., per ulteriori approfondimenti, F. Bravo (a cura di), *EU Data Cooperatives: l'ingresso delle cooperative di dati nell'ordinamento europeo,* Torino, Giappichelli, 2024.

il trattamento dei dati da parte di terzi. Essa dovrebbe avere anche la possibilità di avviare unilateralmente negoziati contrattuali con le organizzazioni di utenti dei dati nell'interesse dei loro membri e di adoperarsi per ottenere condizioni contrattuali che meglio si adattino ai loro interessi.

Le cooperative di dati dovrebbero poi valutare le conseguenze sociali prodotte dall'implementazione di sistemi di IA da parte di terzi o aiutare a distribuire i dati in *pool* per fornire valore ai propri membri eseguendo algoritmi in modo autonomo. Ovviamente, l'apporto del socio-interessato alla formazione della volontà della cooperativa non può tradursi nell'automatico trasferimento alla cooperativa del potere di autodeterminazione facente capo all'interessato medesimo. È infatti ribadito il principio di irrinunciabilità dei diritti dell'interessato, incluso il diritto di revoca del consenso al trattamento dei dati personali, che non può ritenersi abdicato neanche qualora l'esercizio dei diritti fosse delegato alla cooperativa di dati. Si è poi rimarcato come tale differenza di struttura e funzioni tra questo intermediario e gli altri previsti dal *Data governance act* si riverberi sull'eventuale natura della responsabilità civilistica degli uni e degli altri, in caso di illegittimo trattamento dei dati personali degli interessati, rispondendo gli intermediari di cui alle lett. a) e b) dell'art. 10, DGA, come soggetti autonomi, sulla base di una responsabilità precontrattuale o contrattuale, a seconda dell'inquadramento del rapporto preesistente, in linea con la discussa posizione degli intermediari finanziari, e le cooperative di dati, invece, sulla base del rapporto societario.

Il vantaggio mutualistico per i soci della cooperativa di dati sanitari senza fine di lucro pare derivare, anche in assenza di un ristorno in senso tecnico, dai servizi forniti dalla cooperativa senza un corrispettivo e collegati al trasferimento dei dati tra gli interessati e la cooperativa. Si può quindi enucleare da tali rapporti tra cooperativa e socio un rapporto contrattuale ulteriore di consulenza ed eventualmente di mandato. L'accordo, poi, stabilisce il diritto degli interessati-soci ad ottenere dati meglio strutturati rispetto ai dati iniziali forniti, eventualmente anonimizzandoli e/o rendendoli più sicuri.

Per la sua impronta prettamente pubblicistica, si contraddistingue,

invece, il Regolamento per la creazione di un *European Health Data Space,* che intende fornire regole, *standard* e pratiche comuni, infrastrutture e un quadro di *governance* sia per l'uso primario (l'utilizzo di dati sanitari elettronici personali per fornire servizi all'individuo), che per l'uso secondario (l'utilizzo di dati sanitari elettronici per esigenze più ampie come la ricerca sanitaria o le politiche pubbliche) dei dati sanitari. Nell'ottica del potenziamento dell'uso primario dei dati sanitari, tale regolamento stabilisce disposizioni specifiche relative ai diritti delle persone fisiche in relazione al trattamento dei loro dati personali. L'applicazione di tali diritti è indipendente dallo Stato membro in cui sono trattati i dati sanitari elettronici personali, dal tipo di prestatore di assistenza sanitaria, dalle fonti di tali dati o dallo Stato membro di affiliazione della persona fisica. Ai sensi dell'art. 3, reg. EHDS, e con disciplina migliorativa rispetto a quella di cui al GDPR, l'interessato ha il diritto di accedere immediatamente, gratuitamente e in un formato facilmente leggibile, consolidato e accessibile, ai propri dati sanitari elettronici personali che siano trattati per la prestazione di assistenza sanitaria attraverso i servizi di accesso ai dati sanitari elettronici nel formato europeo di scambio delle cartelle cliniche elettroniche. Ai sensi dell'art. 5, reg. EHDS, inoltre, le persone fisiche o i loro rappresentanti hanno il diritto di inserire informazioni nella propria cartella clinica elettronica attraverso servizi o applicazioni di accesso ai dati sanitari elettronici collegati a tali servizi. Tale diritto di inserimento è un diritto nuovo e si affianca ai diritti di rettifica e portabilità, che si basano sulla loro precedente concettualizzazione nel GDPR. Secondo l'art. 7, reg. EHDS, che disciplina il diritto alla portabilità poi, le persone fisiche hanno il diritto di concedere l'accesso ai loro dati sanitari elettronici personali a un altro prestatore di assistenza sanitaria di loro scelta, gratuitamente e senza ostacoli da parte del prestatore di assistenza sanitaria o dei fabbricanti dei sistemi utilizzati dal prestatore di assistenza sanitaria. Qualora i prestatori di assistenza sanitaria si trovino in Stati membri diversi, le persone fisiche hanno il diritto di chiedere la trasmissione dei loro dati sanitari elettronici personali nel formato europeo di scambio delle cartelle cliniche elettroniche. In questa nuova versione, poi, vi è l'inclusione esplicita della

portabilità dei dati desunti, integrazione necessaria anche alla luce della loro utilizzabilità nei *set* di dati necessari per il "*training*" e l'utilizzo dell'intelligenza artificiale. Inoltre, il diritto alla portabilità è esteso ad ogni base giuridica e il trattamento dei dati non è limitato più quindi solo a fattispecie cui sia sotteso un atto negoziale o un atto giuridico di carattere autorizzatorio.

Con riferimento all'uso secondario dei dati, si assiste alla perdita della centralità del consenso come base giuridica, essendo prevista l'istituzione di uno o più organismi per l'accesso ai dati sanitari ai quali gli utenti dei dati sanitari dovranno rivolgersi appunto per accedere e trattare i dati sanitari sulla base di un'autorizzazione o di una richiesta di dati sanitari rilasciata, sempre che siano soddisfatti alcuni criteri esiziali, quali l'aderenza della finalità descritta nella domanda con quelle considerate lecite dalla norma; l'adeguatezza e necessarietà dei dati; la competenza del richiedente rispetto alle finalità previste per l'uso dei dati. Insomma, il nuovo Regolamento EHDS permette, seppur a determinate condizioni ed entro certi limiti, ad organi terzi, a titolari dei dati, agli utenti dei dati, di avere la base normativa necessaria (permeata dell'interesse pubblico) a far sì che tali dati, fonte inestimabile di attività di ricerca, possano effettivamente essere utilizzati senza il consenso dell'interessato. Si stabilisce, infatti, nel Considerando n. 52 reg. EHDS che gli Stati membri non dovrebbero più poter mantenere o introdurre, ulteriori condizioni, comprese limitazioni e disposizioni specifiche che richiedano il consenso delle persone fisiche, per quanto riguarda il trattamento per l'uso secondario dei dati sanitari elettronici personali, ad eccezione dell'introduzione di misure più rigorose e garanzie supplementari a livello nazionale intese a tutelare la sensibilità e il valore di taluni dati come previsto dal presente regolamento. Ciò è giustificato sulla base del fatto che il consenso è sostituito «con una *governance* affidabile e a costi inferiori rispetto all'affidamento sul consenso». L'EHDS sembra proporre quindi un nuovo paradigma per l'uso secondario dei dati sanitari per la ricerca scientifica, non più basato sul consenso come regola generale, ma sulle nozioni di interesse generale della società e di interesse pubblico. L'assenza del consenso tra le basi giuridiche è in parte controbilanciata però dalla possibilità

per l'interessato di procedere all'*opt-out*. Si tratta di un meccanismo che ha precedenti nell'esperienza di alcuni stati membri, con risultati contrastanti. Analizzando la disciplina di tale istituto, la medesima pare in linea con le esigenze di bilanciamento tra le contrapposte situazioni giuridiche, in cui si incanala la libera circolazione dei dati, funzionale sia alla piena realizzazione del mercato interno, sia al processo di coesione sociale e istituzionale dell'UE. Dopo essere stato debitamente reso edotto circa i propri diritti, l'interessato, consapevole degli effetti del proprio silenzio, può decidere di rimanere inerte ovvero di assolvere l'onere che la legge gli impone al fine di impedire l'uso secondario, esplicitando il suo rifiuto a che ciò avvenga. In ciascun caso, il soggetto considerato dovrebbe esprimere una volontà – informata e consapevole dei propri effetti che è espressione dell'autonomia individuale di determinare il destino dei propri dati sanitari.

È da segnalare, però, che la possibilità per gli Stati membri di introdurre eccezioni all'*opt-out* per motivi di interesse pubblico (considerando 54) può determinare notevoli divergenze nel modo in cui tale limitazione è applicata da uno Stato membro all'altro, soprattutto in considerazione della mancanza di un'interpretazione comune di ciò che possa considerarsi nell' «interesse pubblico».

Nel fornire accesso a una serie di dati, l'organismo responsabile dovrà utilizzare una tecnologia di pseudonimizzazione o anonimizzazione all'avanguardia, garantendo nella misura massima possibile che una persona fisica non possa essere reidentificata dagli utenti dei dati sanitari. Senonché, ciò presuppone che vi sia uno *standard* europeo condiviso sulla definizione di dato anonimo. Le definizioni giuridiche e i requisiti per l'anonimizzazione e la pseudonimizzazione variano, infatti, notevolmente da un paese all'altro. Sono necessari quindi orientamenti più precisi a livello dell'UE su come soddisfare i requisiti del GDPR in questo settore, in modo da conseguire un ragionevole equilibrio tra rischi e benefici, per eliminare l'incertezza giuridica e il conseguente timore di controversie per gli utenti secondari dei dati. Peraltro, l'anonimizzazione, soprattutto se particolarmente rigorosa, può ridurre l'utilità dei dati per la ricerca scientifica. Inoltre, non è del tutto chiaro chi dovrà anonimizzare i dati, cioè se debba adoperar-

si in tal senso il titolare dei dati prima di condividerli con l'organismo responsabile dell'accesso ai dati sanitari, ovvero questo stesso organismo (cfr. Considerando n. 49 EHDS).

Altro problema rilevato concerne il fatto che il Regolamento EHDS definisca, all'art. 51, come «dati sanitari elettronici a disposizione per l'uso secondario» un'ampia gamma di categorie di dati che vanno ben oltre ciò che sono le informazioni sulla salute o sulle cure mediche dei pazienti, comprendendo, ad esempio dei determinanti socioeconomici, ambientali e comportamentali della salute, dati amministrativi relativi all'assistenza sanitaria, anche in relazione alle dispensazioni, alle domande di rimborso, dati sui fattori ambientali, quali l'inquinamento, le radiazioni o l'uso di determinate sostanze chimiche. Le finalità per le quali i dati sanitari possono essere trattati per usi secondari (cfr. art. 53 del Regolamento EHDS) sono poi numerose e forse sovrabbondanti. Si tratta in linea generale di compiti svolti da organismi pubblici, quali l'esercizio di funzioni pubbliche, compresi la sorveglianza sanitaria pubblica, i compiti di pianificazione e comunicazione, l'elaborazione delle politiche sanitarie, la garanzia della sicurezza dei pazienti, la qualità dell'assistenza e la sostenibilità dei sistemi sanitari, la ricerca scientifica.

Si è infine approfondita la disciplina che regola la responsabilità civilistica, l'art. 100 Regolamento EHDS, che risulta ancor più laconico nella sua formulazione rispetto a quanto previsto dall'art. 82 del GDPR, non aiutando di certo l'idea della creazione di una responsabilità civile europea (così come non è stato di aiuto il recente ritiro della direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale). Vista la parziale similitudine tra le suddette disposizioni, si sono riproposti in tale sede alcuni interrogativi sulla natura della responsabilità che deriva in caso di violazione delle norme di questo regolamento. In linea generale, e soprattutto in mancanza di chiari riferimenti testuali in un senso o nell'altro, è coerente l'adozione della disciplina della responsabilità contrattuale o di quella extracontrattuale, distinguendo i casi a seconda dell'inquadramento che si dà del rapporto tra le parti. Si tratta di una valutazione ermeneutica necessaria e doverosa, considerando

che, anche in questa fattispecie, manca una puntuale regolamentazione di aspetti rilevanti in materia di responsabilità, e quindi non può che sopperire la disciplina domestica.

Ebbene, il regolamento EHDS disegna il formarsi di un rapporto che prevede la presenza di quattro parti: chi genera i dati (l'interessato), chi li detiene per fini di cura (titolare dei dati), chi ne gestisce l'accesso (l'autorità per l'accesso ai dati) e chi ne chiede e poi ne ottiene la disponibilità per fini di riutilizzo (utente dei dati). Profili di responsabilità si possono verificare nelle deviazioni rispetto ai termini e alle condizioni di accesso e riuso del flusso di dati ovvero laddove si verifichi una violazione nel trattamento dei dati personali (accesso non autorizzato, perdita o alterazione delle informazioni). In questo contesto, si è proposta la configurazione di un rapporto *lato sensu* contrattuale sia tra l'interessato e il titolare dei dati, che tra l'interessato e l'Organismo per l'accesso ai dati sanitari. Anche al di fuori di una vera relazione contrattuale, si appalesa una relazione di fiducia tra le parti sopramenzionate, fiducia che è uno dei principali obiettivi dichiarati di questa normativa, così come del *Data Governance Act*. Tale fiducia è puntellata e rafforzata da una serie di obblighi indicati dalla normativa europea a carico sia del titolare dei dati sanitari, che dell'Organismo per l'accesso ai dati sanitari. In queste ipotesi, quindi, la responsabilità sarà disciplinata dall'art. 1218 c.c., che disciplina l'inadempimento di obblighi di natura contrattuale. Profili di responsabilità di natura extracontrattuale, invece, non rinvenendosi un previo rapporto tra le parti, sono attribuibili al *data user* nei confronti dell'interessato, se si verifichi una sua violazione volontaria o colposa nel trattamento dei dati da cui derivi una fuga di dati potenzialmente o concretamente capace di re-identificare l'interessato medesimo, condotta esplicitamente vietata dal Regolamento, in coerenza con la tutela dei diritti fondamentali tutelati dal GDPR, e ad essa potrà affiancarsi, in concorso, una responsabilità dell'Organismo per l'accesso ai dati sanitari, che male abbia valutato le capacità dell'utente dei dati, anche dal punto di vista della sicurezza dell'ambiente proposto, in fase di richiesta di autorizzazione.

Ove l'Organismo di accesso ai dati sanitari si rifiuti di rilasciare

un'autorizzazione ai dati, tale ente dovrà motivare il proprio diniego (vedi art. 68, par. 9, reg. EHDS) e la motivazione dovrà indicare i presupposti di fatto e le ragioni giuridiche che hanno determinato la decisione, anche in relazione alle risultanze dell'istruttoria *ex* art.3 legge 241/1990. In questo quadro, dovrà poter sempre essere risarcibile (sussistendone i presupposti concreti, naturalmente) il danno derivante dall'illegittimo diniego o dall'annullamento in autotutela dell'atto autorizzatorio da parte dell'Organismo di accesso ai dati sanitari, ovverosia la lesione consistente nell'illegittimo impedimento all'espansione del diritto soggettivo. Così dovrà essere pure ove si volesse addivenire ad una configurazione di un rapporto "contrattuale" tra Organismo di accesso ai dati sanitari e *data user*, sulla base dell'individuazione di un «contatto sociale» o di un «contatto amministrativo qualificato» tra queste due parti, considerato l'elemento della «fiducia» che viene decantato dal regolamento EHDS in più occasioni e che pare confermare la nascita di una stretta relazione tra le parti dei rapporti che si instaurano ai sensi di questa normativa.

Nel concludere, va ricordato come il regolamento EHDS, che mira a istituire un meccanismo comune per l'accesso ai dati sanitari elettronici per uso secondario in tutta l'Unione europea, proponga un meccanismo comune, ma non esclusivo, considerato che l'art. 1, par. 8, del Regolamento stabilisce, in parte vanificandone la portata generale, che tale disciplina «lascia impregiudicato l'accesso ai dati sanitari elettronici per l'uso secondario concordato nel quadro di accordi contrattuali o amministrativi tra soggetti pubblici o privati.» E questo doppio binario può creare non poche perplessità nell'ottica della tutela dei diritti dell'interessato. Sembra infatti che tale disposizione configuri una sorta di clausola di salvezza per le aziende farmaceutiche e per gli enti privati (vista anche la definizione molto ampia dell'«utente dei dati»), per svicolare da tale ultima regolamentazione piuttosto rigida, e ritornare nei meandri più confusi e complessi, e per ciò stesso in realtà non sempre più comodi, del GDPR.

BIBLIOGRAFIA

Alpa G., *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in Cuffaro V., Ricciuto V., Zeno Zencovich V. (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffrè, 1999, 26;

Alpa G. (a cura di), *La responsabilità sanitaria. Commento alla L. 8 marzo 2017*, n. 24, Pisa, Pacini, 2017;

Alpa G., *Solidarietà. Un principio normativo*, Bologna, Il Mulino, 2022;

Amram D., *La transizione digitale delle vulnerabilità e il sistema delle responsabilità – The digital transition of vulnerabilities and the system of liabilities*, in *Rivista italiana di medicina legale*, 2023, 1 ss.;

Astone A., *Responsabilità sanitaria ed emergenza pandemica*, in *Diritto di famiglia e delle persone*, 2022, 731;

Bachelet V., *Il contratto di scambio di "servizi contro dati" (o contro prezzo)*, in *Rivista di diritto civile*, 2024, 1130;

Balducci Romano F., in Sciaudone R., Caravà E. (a cura di), *Il codice della privacy: commento al d.lgs. 196/2003 e al d.lgs. 101/2018 alla luce del Regolamento (UE) 2016/679 (GDPR)*, Pisa, Pacini, 2019, 732;

Bani E., Macchiavello E., *Il diritto alla portabilità dei dati nell'ambito della nuova economia dei dati*, in Falce V., *Financial Innovation tra disintermediazione e mercato*, Torino, Giappichelli, 2021, 137 ss.;

Barbierato D., *Trattamento dei dati personali e «nuova» responsabilità civile*, in *Responsabilità civile e previdenza*, 2019, 2157;

Bassi A., *Delle imprese cooperative e delle mutue assicuratrici (artt. 2511-2548)*, in *Il codice civile commentato*, diretto da Schlesinger P., Milano, Giuffrè, 1988, 1 ss.;

Bassi A., *Le società cooperative*, Torino, Utet, 1995, 192;

Basunti C., *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contratto e impresa*, 2020, 882;

BATTELLI E., D'IPPOLITO G., *Il diritto alla portabilità dei dati personali*, in TOSI E. (a cura di), *Privacy digitale. riservatezza e protezione dei dati personali tra GDPR e nuovo codice privacy*, Milano, 2019, 185 ss.;

BECKERS A., TEUBNER G., *Three Liability Regimes for Artificial Intelligence*, Londra, Hart, 2022;

BELLISARIO E., *Il pacchetto europeo sulla responsabilità per danni da prodotti e da intelligenza artificiale. Prime riflessioni sulle Proposte della Commissione*, in *Danno e responsabilità*, 2023, 153 ss.;

BERTOLINI A., *Intelligenza artificiale e responsabilità civile*, Bologna, Il Mulino, 2025;

BIANCA M.C., *Diritto civile*, 5, *La responsabilità*, 2a ed., Milano, Giuffrè, 2012, 1;

BIANCHI L.R., *Il diritto alla portabilità dei dati, in circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (codice privacy),* in PANETTA R. (a cura di), *Scritti in memoria di Stefano Rodotà*, Milano, Giuffrè, 2019, 223 ss.;

BIASIN E., *EHDS, un anno dopo: i temi caldi del dibattito sullo Spazio europeo dei dati sanitari*, consultabile al link *https://www.agendadigitale.eu*;

BIASIOTTO R., PRAMSTALLER P., MASCALZONI D., *The dynamic consent of the Cooperative Health Research in South Tyrol (CHRIS) study: broad aim within specific oversight and communication*, in *BioLaw journal* 2021, 277 ss.;

BIGLIAZZI GERI L., *Contributo ad una teoria dell'interesse legittimo nel diritto privato*, Milano, Giuffrè, 1967;

BILANCETTI M., *La responsabilità penale e civile del medico*, Padova, Cedam, 1996, 312 ss.

BINCOLETTO G., *A Data Protection by Design Model for Privacy Management in Electronic Health Records,* 161 ss. in NALDI M., ITALIANO G.F., RANNENBERG K., MEDINA M., BOURKA A., *Privacy Technologies and Policy,* Berlino, Springer, 2019;

BIONDI M., *Contratto di spedalità e responsabilità della struttura sanitaria*, in *Contratti*, 2022, 447;

BLASIMME A., VAYENA E., HAFEN E., *Democratizing health research through data cooperatives*, in *Philosophy and technology*, 2018, 31(3), 473–79;

Bocchini F., *Le cartelle cliniche. Funzioni, documento, prova*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2018, 35 ss.;

Bolognini L., Zipponi S., *Prospettive future in sanità: spazio europeo dei dati sanitari e regolazione dei dati scientifici*, in Bolognini L., Zipponi S. (a cura di), *Privacy e diritto dei dati sanitari*, Milano, Lefebvre Giuffrè, 2024, 261 ss.;

Bonavera E., *Recesso parziale del socio di cooperativa tra rapporto societario e rapporto mutualistico*, in *Società*, 2022, 549 ss.;

Bonfante G., *La legislazione cooperativa. Evoluzione e problemi*, Milano, Giuffrè, 1984, 9 ss.;

Bonfante G., *La "morte" del contratto di scambio nelle cooperative secondo una sentenza del Supremo Collegio*, in *Società*, 2024, 24 ss.;

Bonfante G., *La società cooperativa, Itinerari di giurisprudenza*, in *Società*, 2023, 102 ss.;

Bonfante G., *sub* art. 2545 *sexies*, in Cottino G., Bonfante G. Cagnasso O., Montalenti P., *Il nuovo diritto societario. Commentario*, Bologna, Zanichelli, 2004;

Borkin S., *Platform co-operatives – solving the capital conundrum*, 2019, consultabile in https://platform.coop/blog/nesta-foundation-proposes-gbp-1-million-investment-fund-for-platform-co-ops/;

Bortolotti N., Verzeletti A., Antonietti A., *Il concorso di colpa del paziente in ipotesi di responsabilità professionale medica*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2018, 1343 ss.

Bragazzi N.L., Haijiang D., Damiani G., Behzadifar M., Martini M., Wu J., *How Big Data and Artificial Intelligence Can Help Better Manage the COVID-19 Pandemic*, in *International Journal of Environmental Research and Public Health*, 2020, 1 ss.;

Bravo F., *Cooperative di dati*, in *Contratto e impresa*, 2023, 757 ss.;

Bravo F. (a cura di), *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, Torino, Giappichelli, 2024;

Bravo F., *Il commercio elettronico dei dati personali*, in *Questioni attuali in tema di commercio elettronico*, a cura di Pasquino T., Rizzo A., Tescaro M., Napoli, ESI, 2020, 83-130;

Bravo F., *Il consenso e le altre condizioni di liceità del trattamento dei dati personali, in* Finocchiaro G. (a cura di), *Il nuovo Regolamento europeo sulla*

privacy e sulla protezione dei dati personali, Bologna, Zanichelli, 2017,152-157;

BRAVO F., *Il principio di solidarietà*, in BRAVO F. (a cura di), *Dati personali. Protezione, libera circolazione e Governance. 1. Principi*, Pisa, Pacini, 2023, 598 ss.;

BRAVO F., *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contratto e impresa,* 2023, 426 ss.;

BRAVO F., Il *principio di solidarietà tra data protection e data governance,* in *Diritto dell'informazione e dell'informatica*, 2023, 481 ss.;

BRAVO F., *Intermediazione di dati personali e servizi di data sharing dal GDPR al data governance act*, in *Contratto e impresa/Europa*, 2021, 199 ss.;

BRAVO F., *L' «architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 775-854 ss.;

BRAVO F., *Le condizioni di liceità del trattamento di dati personali*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia*, Bologna, Zanichelli, 2019, 140 ss.;

BRAVO F., *Lo "scambio di dati personali" nella fornitura di servizi digitali ed il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, 34 ss.;

BRAVO F., *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e impresa*, 2018, 6;

BRAVO F., *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in ZORZI GALGANO N. (a cura di) *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, Wolters Kluwer, 2019, 384 ss.;

BUONOCORE V., *Diritto della cooperazione*, Bologna, Il Mulino, 1997, 35 ss.;

BUONOCORE V., *Rapporto mutualistico e parità di trattamento*, in *Il nuovo diritto delle società, Liber amicorum Gianfranco Campobasso*, diretto da ABBADESSA P., PORTALE G.B., 4, Torino, Utet, 2007, 579 ss.;

BUSCA N., *Chiarimenti sull'applicazione della disciplina di protezione dei dati in ambito sanitario*, in *www.rivistaresponsabilitamedica.it*, 8 aprile 2019;

Busnelli F.D., P*er uno statuto del corpo umano inanimato, in* Canestrari S., Ferrando G., Mazzoni C.M., Rodotà S., Zatti P. (a cura di*), Il governo del corpo, II, in Trattato di biodiritto* Rodotà S., Zatti P.*,* II, Milano, Lefebvre Giuffrè, 2011, 2137 ss.;

Calabretta N., *Consumer-driven, patient-centered health care in the age of electronic information*, in *Journal of the Medical Library Association*, vol. 90, 1, 2002, 32;

Calisai F., *I diritti dell'interessato*, in Cuffaro V., D'Orazio R., Ricciuto V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 327;

Camardi C., *Enti collettivi e formazioni sociali, dal Libro I al Libro V attraverso il Terzo settore*, in *Contratto e impresa*, 2023, 470 ss.;

Camardi C., *Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea*, in *Nuova giurisprudenza civile commentata*, 2023, 1145 ss.;

Campagna M., *Il regolamento europeo 679/2016 e l'utilizzo delle banche dati in sanità*, in Monica A., Balduzzi G. (a cura di), *Governare il cambiamento istituzionale e organizzativo nelle amministrazioni europee*, Pavia, Pavia University Press, 2019, 59 ss.;

Candini A., *Gli strumenti di tutela*, in Finocchiaro G. (diretto da), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Giuffrè, 2017, 569 ss.;

Capilli G., *Diritto privato sanitario. Fondamenti*, Pisa, Pacini, 2022, 5 ss.;

Capo G., *Le cooperative di comunità*, in *Giurisprudenza commerciale,* 2021, 616;

Carapezza Figlia G., *Decisioni algoritmiche tra diritto alla spiegazione e divieto di discriminare*, in Orlando S. (a cura di), *Libertà e liceità del consenso nel trattamento dei dati personali*, Firenze, Persona e mercato ed., 2024, 64 ss.

Cardarelli F., *Le banche dati pubbliche: una definizione*, in *Il diritto dell'informazione e dell'informatica*, 2002, 321;

Caredda V., *Concorso del fatto colposo del creditore, art. 1227, Il codice civile commentario*, già diretto da Schlesinger P. e continuato da Busnelli F.D. e Ponzanelli G., Milano, Giuffrè Lefebvre, 2020;

Caredda V., *La questione dell'onere*, Torino, Giappichelli, 2024;

CAREDDA V., *L'onere e la norma: prove di accesso al diritto*, in *Giustizia civile*, 2019, 51 ss.;

CAROVANO G., FINCK M., *Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy*, in *Computer Law and Security Review*, Vol. 50, 2023;

CARULLO G., *Dati sanitari, sistemi sanitari nazionali e riuso dei dati*, in *Sanità pubblica e privata*, 2023, 19 ss.;

CARULLO G., *Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato,* in *Rivista italiana di diritto pubblico comunitario*, 2020, 131;

CASALE F., *Scambio e mutualità nella società cooperativa*, Milano, Lefebvre Giuffrè, 2005, 86;

CASAROSA F., GENNARI F., *Data Sharing in the Internet of Medical Things: Between the Data Act and the EHDS*, in *Giornale europeo della regolamentazione dei rischi*, 2025, 1–23;

CASCINI F., ARCURI M.A., *Uso secondario dei dati personali relativi alla salute: panoramica della normativa europea e nazionale, in Diritto dell'informazione e dell'informatica,* 2024, 837 ss.;

CASTRONOVO C., *Il negozio giuridico dal patrimonio alla persona*, in *Europa e diritto privato*, 2009, 87 s.;

CASTRONOVO C., *La civilizzazione della p.a.*, in *Europa e diritto privato,* 2013, 637 ss.;

CASTRONOVO C., *La nuova responsabilità civile*, Milano, Giuffrè, 2006, 443 ss.;

CASTRONOVO C., *L'obbligazione senza prestazione*, *ai confini tra contratto e torto*, in *Le ragioni del diritto*, *Scritti in onore di L. Mengoni*, Milano, Giuffrè, 1995, I, 148 ss.;

CASTRONOVO C., *Responsabilità civile per la Pubblica Amministrazione*, in *Jus*, 1998, 647 ss.;

CATELANI E., *La digitalizzazione dei dati sanitari: un percorso ad ostacoli*, in *Corti supreme e salute*, 2023, 423 ss.;

CATERINA R., THOBANI S., *Il diritto al risarcimento dei danni*, in *Giurisprudenza italiana*, 2019, 2807 ss.;

CECCHERINI A., *La società cooperativa europea (Regolamento CE, n. 1435/03 del Consiglio)*, in *Le nuove leggi civili commentate*, 2003, 1295;

P. Cervera De La Cruz, Shabani M., in *Fair enough? Exploring the role of fairness in secondary uses of health data in the European Health Data Space*, in Slokenberga S., Ó Cathaoir K., Shabani M., *The European Health Data Space; Examining A New Era in Data Protection*, London, Routledge, 2025, 136 ss.;

Cesqui S.M., *La funzione sociale della cooperazione nel progetto costituzionale*, in *Rivista delle società*, 1995, 1153;

Chen J., Dove E.S., Bhakuni H., *Explicit Consent and Alternative Data Protection Processing Grounds for Health Research,* in Kosta E., Leenes R., Kamara I. (eds), *Research Handbook on EU Data Protection Law* (Elgar, 2022);

Ciancimino M., *AI-Based Decision-Making Process in Healthcare*, in *Journal of European Consumer and Market Law*, vol. 11, n. 5, 2022, 173 ss.;

Ciancimino M., *Circolazione "secondaria" di dati sanitari e biobanche. Nuovi paradigmi contrattuali e istanze personalistiche*, in *Diritto di famiglia e delle persone*, 2022, 68;

Ciancimino M., *Protezione e controllo dei dati in àmbito sanitario e intelligenza artificiale. I dati relativi alla salute tra novità normative e innovazioni tecnologiche*, Napoli, ESI, 2020;

Cirillo G., *Trattamento pubblico dei dati personali e responsabilità civile della P.A.*, in *Foro amministrativo*, 1999, 3 ss.;

Colangelo R.M., *App mediche e protezione dei dati personali. Alcuni spunti giuridici tra GDPR, codice privacy novellato e chiarimenti del Garante*, in *Autonomie locali e servizi sociali*, 2019, 275 ss.;

Comandé G., *Ricerca in sanità e data protection un puzzle... risolvibile*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2019, 187 ss.;

Comandè G., *sub* art. 21, in D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, Milano, Giuffrè, 2021, 366 ss.;

Comandé G., Nocco L., Peigné V., *Il fascicolo sanitario elettronico: uno studio multidisciplinare*, in *Rivista italiana di medicina legale e del diritto in campo sanitario,* 2012, 105 s.;

Corso S., *Alla frontiera del diritto privato. Nuove tecnologie e persona anziana*, in *Nuova giurisprudenza civile commentata*, 2024, II, 1253 ss.;

CORSO S., *European Health Data Space. La Commissione europea presenta la proposta di Regolamento sullo spazio europeo dei dati sanitari*, in *www.rivistaresponsabilitamedica.it*, 13 giugno 2022;

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

CORSO S., *Il fascicolo sanitario elettronico 2.0. Spunti per una lettura critica*, in *Le nuove leggi civili commentate*, 2024, 334;

CORSO S., *Il fascicolo sanitario elettronico fra e-Health, privacy ed emergenza sanitaria*, in *Responsabilità medica*, 2020, 393 ss.;

CORSO S., *Il parere congiunto del Comitato europeo per la protezione dei dati e del Garante europeo della protezione dei dati in merito alla proposta di Regolamento sullo spazio europeo dei dati sanitari*, in *www.rivistaresponsabilitamedica.it*, 5 settembre 2022;

CORSO S., *L'intelligenza artificiale e il trattamento dei dati relativi alla salute*, in *Responsabilità medica*, 2023, 317 ss.;

CORSO S., *Lo spazio europeo dei dati sanitari: la Commissione Europea presenta la proposta di regolamento*, in *federalismi.it*, *Osservatorio di diritto sanitario*, 10 agosto 2022, 2 ss.;

CORSO S., *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, in *Le nuove leggi civili commentate*, 2025, 577;

CORSO S., *Salute e riserbo del paziente: questioni aperte in tema di cartella clinica*, in *Rivista responsabilità medica*, 2017, 395 ss.;

CUFFARO V., voce *Risarcimento del danno e trattamento dei dati personali*, in *Enc. dir.*, *I tematici*, VII, *Responsabilità civile*, diretto da C. Scognamiglio, Milano, 2024, 1360 ss.;

CUSA E., *I ristorni nelle società cooperative*, Milano, Giuffrè Lefebvre, 2000, 163;

CUSA E., *La nozione unionale di organizzazione non lucrativa tra contratti pubblici, terzo settore e trasporti sanitari di urgenza*, in *Società*, 2023, 21;

CUSA E., *La vigilanza sulla gestione delle cooperative nella legge n. 142 del 2001*, in *Rivista della cooperazione*, 2002, 33;

CUTTAIA F. G., *The impact of EU Regulation 2016/679 on the Italian health system*, in FARES G.M. (a cura di), *The Protection of Personal Data Con-*

cerning Health at the European Level. A Comparative Analysis, Torino, 2021, 200 s.;

Dabormida R., *La cooperativa europea finalmente in porto*, in *Rivista della cooperazione*, 2003, 123;

Dabormida R., *Mutualità e ristorni nei consorzi con attività esterna*, in *Società,* 2015, 670;

D'Agostino Panebianco M., *Il trattamento dei dati nel Sistema Sanitario Nazionale italiano alla luce del Provvedimento del Garante del 7 marzo 2019*, in *Ciberspazio e diritto*, 2019, 241 ss.;

D'Alfonso G., *I nuovi scenari dannosi correlati all'impiego delle tecnologie digitali emergenti. L'intervento del legislatore europeo di modernizzazione della disciplina sulla responsabilità del produttore*, in Grasso B. (a cura di), *Scritti in memoria di Ubaldo La Porta*, Napoli, ESI, 2023, 217 ss.;

Dawande M., Mehta S., Mu L., *Robin Hood to the rescue: sustainable revenue-allocation schemes for data cooperatives*, in *Production and operation management*, 2022, vol. 32, 8;

De Cristofaro G., *Die datenschutzrechtliche Einwilligung als Gegenstand des Leistungsversprechens*, in Padovini F., Pertot T., Schmidt Kessel M. (a cura di), *Rechte an Daten*, Tübingen, Mohr Siebrek, 2020, 151 ss.;

De Ferra G., *Principi costituzionali in materia di cooperazione a carattere di mutualità*, in *Rivista delle società*, 1964, 776;

De Franceschi A., *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, 59;

De Hert P., Papakonstantinou V., Malgieri G., Beslay L., Sanchez I., *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, in *Computer Law & Security Review*, 2018, 193;

Delacroix, S. Lawrence N.D., *Bottom-up data trusts: disturbing the 'one size fits all' approach to data governance. International Data Privacy Law*, 2019;

De Marsico A., *Natura giuridica del verbale di ricovero d'urgenza in ospedale e cartella clinica. I controlli e la loro influenza in atti*, in *Giust. pen.*, 1971, 97 ss.;

De Matteis R., *La responsabilità medica tra prospettive comunitarie e nuove tendenze giurisprudenziali*, in *Contratto e impresa,* 1995, 488;

DE MIGUEL ASENSIO P.A., *Los servicios de intermediación de datos en el nuevo Reglamento de Gobernanza de Datos*, in *La Ley Unión Europea*, n. 105, 2022;

DE MINICO G., *Electronic health record: political issues and privacy*, in *www.a-pertacontrada.it*, 18 dicembre 2015;

DE PIETRO O., D'ANCORA L., *La cartella clinica. Problemi procedurali e aspetti medico-legali*, Napoli, Martinucci, 1985, 39;

DI CIOMMO F., *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, in CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2018, 367 ss.;

DI CIOMMO F., *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e responsabilità,* 2022, 121 ss.;

DI DONNA L., *Intelligenza artificiale e rimedi risarcitori*, Milano, Wolters Kluwer, 2022;

DI GREGORIO V., *Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie?*, in *Danno e responsabilità*, 2022, 51 ss.;

DI LUCA N.M., LAROCCA D., CAVALLI A., *Profili medico-legali e giuridici della cartella clinica nell'evoluzione legislativa e giurisprudenziale*, in *Jura Medica* 1-3, 81, 1990;

DI MAJO A., *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela,* in CUFFARO V., RICCIUTO V., ZENO ZENCOVICH V., *Trattamento dei dati personali e tutela della persona*, Milano, Giuffrè, 1999, 230;

DUCATO R., *Commento all'art. 89*, in D'ORAZIO R., FINOCCHIARO G., POLLICINO O., RESTA G., *Codice della privacy e data protection* (a cura di), Milano, Lefevbre Giuffrè, 2021, 970;

DUCATO R., IZZO U., *Diritto all'autodeterminazione informativa del minore e gestione dei dati "supersensibili" nel contesto del Fascicolo Sanitario Elettronico*, in *Diritto dell'informazione e dell'informatica*, 2013, 703 ss.;

DURANTE V., voce "*Onere*", in *Enc. giur. Treccani*, vol. XXI, Roma, 1990, 3;

EMILIOZZI E.A., *Esiste la responsabilità per l'incompleta compilazione della cartella clinica?*, in *giustiziacivile.com,* 2020;

EVANS R.S., *Electronic Health Records: Then, Now, and in the Future*, in *Yearbook of Medical Informatics*, 2016, *Special 25 Anniversary Edition*, 48 ss.;

Faccioli M., (a cura di), *Profili giuridici dell'utilizzo della robotica e dell'intelligenza artificiale in medicina*, Napoli, ESI, 2022;

Faccioli M., *La responsabilità civile per difetto di organizzazione delle strutture sanitarie*, Pisa, Pacini, 2018;

Faillace S., *La controversa categoria delle obbligazioni ex lege*, Milano-Padova, Wolters Kluwer, 2023, *passim*;

Faillace S., *La natura e la disciplina delle obbligazioni di cui all'art. 25 del GDPR, espressione dei principi di privacy by design e di privacy by default*, in *Contratto e impresa*, 2022, 1123 ss.;

Faillace S., *La responsabilità da contatto sociale*, Padova, Cedam, 2004;

Falcone G., *Commento* sub *art. 2545-sexies*, in Sandulli M., Santoro V. (a cura di), *Le riforma delle società. Società cooperative. Artt. 2511-2548 cod. civ.*, Torino, Giappichelli, 2003, 179-180;

Fappiano G., *Gli obblighi informativi degli intermediari finanziari al vaglio della giurisprudenza*, in *Contratti*, 2019, 424 ss.;

Ferraris A.F., *European data strategy e intermediario di dati: nuove prospettive per il mercato della condivisione*, in *Il Quotidiano Giuridico*, 2022;

Ferraro L., *Il Regolamento UE 2016/679 tra Fascicolo Sanitario Elettronico e Cartella Clinica Elettronica: il trattamento dei dati di salute e l'autodeterminazione informativa della persona*, in *BioLaw Journal – Rivista di BioDiritto*, 2021, 91 ss.;

Ferraro L., *La telemedicina quale nuova (e problematica) frontiera del diritto alla salute*, in *Diritto dell'informazione e dell'informatica*, 2022, 837;

Fici A., *Tipo e status nella nuova disciplina dell'impresa sociale*, in *Contratto e impresa*, 2023, 112 ss.;

Fici A., Pellecchia E., *Il consenso al trattamento*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di R. Pardolesi, Milano, Giuffrè, 2003, 502;

Fidanza F., *Sulla distinzione tra intelligenza artificiale e algoritmi*, in *Rivista di diritto dell'impresa*, 2022, 389;

Filauro F., *Telemedicina, cartella clinica elettronica e tutela della privacy*, in *Danno e responsabilità*, 2011, 472;

Finocchiaro G., *Diritto dell'intelligenza artificiale*, Bologna, Zanichelli, 2024;

Finocchiaro G., *Identità personale su Internet: il diritto alla contestualizza-*

zione dell'informazione, *Diritto dell'informazione e dell'informatica*, 2012, 389;

FINOCCHIARO G., *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, in FERRARI G.F. (a cura di), *La legge sulla privacy dieci anni dopo*, Milano, Egea, 2008, 213;

FINOCCHIARO G., *Intelligenza artificiale e responsabilità*, in *Contratto e impresa*, 2020, 713 ss.;

FINOCCHIARO G., *Intelligenza artificiale. Quali regole?*, Bologna, Il Mulino, 2024, 67 ss.;

FINOCCHIARO G., *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove leggi civili commentate*, 2017, 1 ss.;

FINOCCHIARO G., *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, Zanichelli, 2012, 305;

FIORIGLIO G., *La protezione dei dati sanitari nella Società algoritmica. Profili informatico-giuridici*, in *Journal of Ethics and Legal Technologies*, vol. 3, n. 2, 2021, 79 ss.;

FOGLIA M., *Patients and privacy: GDPR compliance for healthcare organizations*, in *European Journal of Privacy Law & Technologies*, 2020, Special Issue, 43 ss.;

FORNASARI M., ZAMAGNI V., *Il movimento cooperativo in Italia. Un profilo storico-economico (1854-1992)*, Firenze, Vallecchi, 1997;

FRACCHIA F., *Autorizzazioni amministrative*, in CASSESE S. (a cura di), *Dizionario di diritto pubblico*, Milano, Giuffrè, 2006, I, 598 ss.;

FRACCHIA F., *Autorizzazione amministrativa e situazioni giuridiche soggettive*, Napoli, Jovene, 1996;

FRANCHINI F., *Le autorizzazioni amministrative costitutive di rapporti giuridici fra l'amministrazione e i privati*, Milano, Giuffrè, 1957;

FUSARO A., *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo,* in *Nuova giurisprudenza civile commentata*, 2020*,* II*,* 1344 ss.;

GADONI CANAAN R., *Data cooperatives in Brazil: applicability and property rights*, in *Revista de Direito e as Novas Tecnologias*, n.11, 2021;

GALGANO F., *Contratto e responsabilità contrattuale nell'attività sanitaria* in *Rivista trimestrale di diritto e procedura civile*, 1984, 710;

Galgano F., *La cooperazione nel sistema costituzionale*, in *Nuovo diritto agrario*, 1977, 412 ss.;

Galgano F., *Mutualità e scambio nelle società cooperative*, in *Rivista di diritto civile,* 1985, 1031 ss.;

Gallo P., *Il consenso al trattamento dei dati personali come prestazione*, in *Rivista di diritto civile*, 2022, 1079 ss.;

Gallone G., *II Consiglio di Stato marca distinzione tra algoritmo, automazione ed intelligenza artificiale*, in *Diritto di internet*, 2022, 1;

Gambini M., *Responsabilità e risarcimento nel trattamento dei dati personali*, in Cuffaro V., D'Orazio R., Ricciuto V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1048 ss.;

Gambino A., Maggio V., Occorsio E., *La riforma del fascicolo sanitario elettronico*, in *Diritto Mercato Tecnologia*, 22 luglio 2020, 10 ss.;

Garofalo A.M., *Regolare l'irregolabile: il consenso al trattamento dei dati nel GDPR*, in S. Orlando, G. Capaldo (a cura di), *Annuario 2021, Osservatorio Giuridico sulla innovazione Digitale*, Roma, Sapienza Università editrice, 2021, 122 ss.;

Garofalo G., *Trattamento e protezione dei dati personali, spunti rimediali in ambito sanitario*, in *Diritto di famiglia e delle persone*, 2021, 1392 ss.;

Gellert R., Jansenn A., *The impact of artificial intelligence on european tort law: taking stock of an ongoing process*, in Janssen A., Lehmann M., Schulze R. (eds), *The future of European Private Law*, Hart Nomos, 2023, 185 ss.;

Genco R., *La struttura finanziaria*, in Genco R. (a cura di) *La riforma delle società cooperative*, Milano, Ipsoa, 2003, 92;

Genco R., *Scopo mutualistico e gestione dell'impresa*, in Schiano Di Pepe G. (a cura di), *Cooperative, consorzi, raggruppamenti*, Milano, Ipsoa, 1996, 30;

Giaimo G., *Natura e caratteristiche del consenso al prelievo di organi e tessuti da cadavere. un raffronto tra Italia ed Inghilterra*, in *Europa e diritto privato*, 2018, 215 ss.;

Giannone Codiglione G., *La tutela della riservatezza*, in *Manuale di diritto dell'informazione e della comunicazione*, a cura di Sica S., Zeno Zencovich V., Padova-Milano, Cedam-Wolter Kluwer, 2019, 281-310;

GIARDINA C., *Il fascicolo sanitario elettronico tra norme e prassi*, in *Azienditalia*, 2021, 12, 2043 ss.;

GILBERT S., BACA-MOTES K., QUER C., WIEDERMANN M., BROCKMANNAND D., *Citizen Data Sovereignty Is Key to Wearables and Wellness Data Reuse for the Common Good (2024) 7 npj Digital Medicine;*

GILLE F., VAYENA E., *How private individuals maintain privacy and govern their own health data cooperative: MIDATA in Switzerland*, in SANFILIPPO M., STRANDBURG K., FRISCHMANN B., *Governing privacy in knowledge Commons*, Cambridge, Cambridge University Press, 2021, 53-69;

GIORDANO R., *La tutela amministrativa e giurisdizionale dei dati personali*, in CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1001 ss.;

GIORGIANNI M., *Il «nuovo» diritto alla portabilità dei dati personali. Profili di diritto comparato*, in *Contratto e impresa*, 2019, 1387 ss.;

GIRISH S., AVERY M., *Data Cooperative: Enabling Meaningful Collective Negotiation of Data Rights for Communities,* 2022, consultabile in https://ssrn.com/abstract=4414473;

GLENNIE H., *Electronic Health Records: Where They Are Now and Where They Need to Be*, in R. MA (a cura di), *Clinical Costing Techniques and Analysis in Modern Healthcare Systems*, Hershey, 2019, 87 ss.;

GLIATTA G., *Il diritto alla privacy in ambito medico: trattamento dei dati sensibili e fascicolo sanitario elettronico*, in *La responsabilità civile*, 2010, 682;

GLIATTA G., *Il trattamento dei dati sensibili e la responsabilità per la tenuta del fascicolo elettronico*, in M. FRANZONI (diretto da), *Le responsabilità nei servizi sanitari: responsabilità civile, responsabilità penale, diritto processuale, amministrativo e del lavoro, profili medico-legali e comparatistici, analisi economica*, Bologna, Zanichelli, 2011, 289 ss.;

GRAEF I., *Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union*, in *Telecommunications Policy*, 2015, 39, 6, 502;

GRAEF I., VERSHAKELEN J., VALCKE P., *Putting the right to data portability into a competition law perspective*, in *Law: The Journal of the Higher School of Economics*, in *Annual Review*, 2013, 53;

GRONDONA M., *Intelligenza artificiale e responsabilità da attività pericolose. Una prospettiva ideologicamente orientata e un inventario di problemi*, in

Cuocci V.V., Lops F.P., Motti C. (a cura di), *La responsabilità civile nell'era digitale. Atti della Summer school 2021*, Bari, Cacucci, 2022, 181 ss.;

Guarda P., *Civile – Fascicolo sanitario elettronico*, in *Digesto online*, 2011;

Guarda P., *Fascicolo sanitario elettronico e protezione dei dati personali*, Trento, Università degli studi di Trento, 2011, 65 ss.;

Guarda P., *I dati sanitari*, in Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 591;

Guidi M., *L'interazione tra la normativa dell'UE in materia di protezione dei dati personali e il Regolamento UE 536/2014 sulle sperimentazioni cliniche*, in *Diritto dell'informazione e dell'informatica,* 2024, 157;

Hardjono T., Pentland T., *Data Cooperatives: towards a foundation for decentralized personal data management* in *arXiv.org*;

Harman L.B., Flite C.A., Bond K., *Electronic Health Records: Privacy, Confidentiality, and Security*, in *Virtual Mentor. American Medical Association Journal of Ethics*, 2012, vol. 14, n.9, 712 ss.;

Hartl A., Ludin A., *Recht der Datenzugänge*, in MMR, 2021, 534 ss.;

Hoffman S., *Electronic Health Records and Medical Big Data. Law and policy*, Cambridge, 2016;

Hussein R., Scherdel L., Nicolet F., Martin-Sanchez F., *Towards the European Health Data Space (EHDS) Ecosystem: A Survey Research on Future Health Data Scenarios*, in *International Journal of Medical Informatics*, Shannon, Ireland, 170 (2023), in doi: 10.1016/j.ijmedinf.2022.104949;

Iaselli M., *Le nuove regole per l'uso primario e secondario dei dati sanitari. Reg. UE 11 febbraio 2025, n. 327 (EHDS)*, Santarcangelo di Romagna, Maggioli, 2025;

Iengo M., sub art.2545-*quaterdecies*, in Bonfante G., Corapi D., Marziale G., Rordorf R., Salafia V. (a cura di), *Codice delle società commentato*, Milano, Giuffrè, 2011, 1851;

Ingenito C., *La rete di assistenza sanitaria on-line: la cartella clinica elettronica*, in *www.federalismi.it*., n.5, 2021, 80-82;

Iorio C., *Intelligenza artificiale e responsabilità: spunti ricostruttivi*, in *Tecnologie e diritto*, 2021, 51 ss.;

IRTI C., *Consenso "negoziato" e circolazione dei dati personali*, Torino, Giappichelli, 2021, 96;

IRTI C., *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano*, in *Persona e mercato*, 2023, 32;

IUDICA G. (a cura di), *La tutela della persona nella nuova responsabilità sanitaria*, Milano, Lefebvre Giuffrè, 2019;

IULIANI A., *La responsabilità civile della pubblica amministrazione; alcune riflessioni intorno all'interesse legittimo dalla prospettiva dei rimedi*, in *Contratto e impresa*, 2016, 1196 ss.;

KENKEL P., *Economic justification for a cooperative*, 2020, in *https://cooperatives.extension.org/economic-justification-for-a-cooperative/*;

KNAPP J., KOBLER J., RICHTER F., *Data cooperatives – collective action as an opportunity for the European data economy and a European data private Law* in *InTe*R 1/23;

KRUUS M., *The Public Interest Requirement In the Secondary Use of Health Data In Scientific Research: The Examples of Estonia and Finland* (2023), 32, *Juridica International,* 64;

KÜHLING J., SACKMANN F., SCHNEIDER H., *Datenschutzrechtliche Dimension Datentreuhänder: Kurzexpertise' (Bundesministerium für Arbeit und Soziales*, 2020), 20, in *https://nbn-resolving.org/urn:nbn:de:0168-ssoar-70086-9*;

LAGIOIA F., *L'intelligenza artificiale in sanità: un'analisi giuridica*, Torino, Giappichelli, 2020;

LAWRENCE N., MONTGOMERY J., OH S., *Enabling data sharing for social benefit through data trusts at the Global Partnership on AI, GPAI*, in *OECD AI Policy Observatory*, 2021, 18;

LEANZA C., *Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio*, in *Responsabilità civile e previdenza*, 2021, 1011 ss.;

LEINO A., *Planning patient-centered care*, in *American Journal of Nursing*, vol. 52, no. 3, 1952, 324;

LI W., *A tale of two rights: exploring the potential conflict between right to data portability and right to be forgotten under the General Data Protection Regulation*, in *International Data Privacy Law*, 2018, 8, 4, 309;

LI W., QUINN P., *The European Health Data Space: An expanded right to*

data portability?, in Computer Law & Security Review, V. 52, 2024, 105913;

Liotta M., *Il favor per la ricerca scientifica e la sua effettiva applicazione nella normativa europea, nazionale e da parte dell'autorità garante*, in *Diritto dell'informazione e dell'informatica* 2024, 363 ss.;

Locatello D. M., *Adeguata gestione del rischio e presunzione di colpa nell'imputazione del danno da illecito trattamento di dati personali*, in *Contratto e impresa*, 2024, 1215 ss.;

Locatello D. M., *Osservazioni sulla costruzione di un regime europeo di responsabilità civile per l'Intelligenza artificiale*, in *Jus civile*, 2022,130 ss.;

Lucchini Guastalla E., *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e imp*resa, 2018, 113;

Maestri E., *Il feticcio della privacy nella sanità. Cura del paziente e biobanking genetico prima e dopo l'entrata in vigore del GDPR*, in Thiene A., Corso S. (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza*, Napoli, Jovene, 2023, 23 ss.;

Maietta A., *La prova del danno da illecito trattamento dei dati personali*, Bari, Cacucci, 2023, 86;

Malgieri G., *Il diritto alla portabilità dei dati personali,* in Comandé G., Malgieri G. (a cura di) *Manuale per il trattamento dei dati personali*, Milano, Il sole 24 ore, 2019, 54;

Malgieri G., *Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data, Privacy, in Germany* – PinG, 2016, 4, 133, 143;

Malgieri G., *User-provided personal content' in the EU: digital currency between data protection and intellectual property* in IRLCT 2018, 32, 1, 118, 130;

Mantelero A., *Big Data And Data Protection*, in G. González-Fuster, R. Van Brakel, P. De Hert (a cura di) *Research Handbook on Privacy and Data Protection Law*, Cheltenham, Edward Elgard Publishing, 2022, 335;

Marano P., *La società cooperativa europea e le politiche comunitarie per reti e gruppi di imprese*, in *Rivista della cooperazione*, 2006, 9;

Marasà G., *Imprese sociali, altri enti del terzo settore, società* benefit, Torino, Giappichelli, 2019;

MARASÀ G., *Problemi attuali della società cooperativa e soluzioni della riforma*, in G. MARASÀ, *La riforma di società, cooperative, associazioni e fondazioni*, Padova, Cedam, 2005, 156;

MARCHESE A., *Profili civilistici dell'information technology in ambito sanitario*, Napoli, ESI, 2021;

MARRA E.*, La società cooperativa europea*, in *Notariato*, 2005, 108;

MARTONE M., *Algoritmi e diritto: appunti in tema di responsabilità civile*, in *Tecnologie e diritto*, 2020, 128 ss.;

MAZZAMUTO S., *Il principio del consenso e il problema della revoca,* in PANETTA R.*, Libera circolazione e protezione dei dati personali*, I, Milano, Giuffrè, 2006, 993 ss.;

MAZZUCA M., *Note minime sulla responsabilità per i danni scaturenti dall'uso dei sistemi di IA*, in *Teoria e prassi del diritto*, 2022, 399 ss.;

MELCHIONNA S., *Commento all'art. 110-bis*, in SCIAUDONE R., *Commentario al codice della privacy,* Pisa, Pacini, 2023, 340 ss.;

MELCHIONNA S., *Sanità digitale e innovazione*, in BOLOGNINI L., ZIPPONI S. (a cura di), *Privacy e diritto dei dati sanitari*, Milano, Lefebvre Giuffrè, 2024, 103 ss.;

MEOLI B., SICA S., STANZIONE P. (a cura di), *Commentario alla legge 8 marzo 2017*, n.24, Napoli, ESI, 2018;

MESSINETTI D., *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali,* in *Rivista critica di diritto privato,* 1998, 351;

MICHELI M., FARELL E., CARBALLA-SMICHOWSKI B., POSADA-SÁNCHEZ M., SIGNORELLI S., VESPE M., *Mapping the landscape of data intermediaries: Emerging models for more inclusive data governance*, 2023 [Report], *Publications Office of the European Union*, in *https://data.europa.eu/doi/10.2760/8943*;

MICKLITZ H. W., *Il fascino del diritto privato europeo*, in *Contratto e impresa/Europa*, 2021, 103 ss.;

MIDIRI F., *Il diritto alla protezione dei dati personali. Regolazione e tutela*, Napoli, Editoriale Scientifica, 2017, 126;

MILLER K., *Radical proposal: data cooperatives could give us more power over our data,* 2021, consultabile in *https://hai.stanford.edu/news/radical-proposal-data-cooperatives-could-give-us-more-power-over-our-data;*

MILNE R., SORBIE A., DIXON-WOODS M., *What can data trusts for health*

research learn from participatory governance in biobanks? in *Journal of Medical Ethics*, 2022; 48:323–8;

Miron-Shatz T., Elwyn G., *To serve and protect? Electronic health records pose challenges for privacy, autonomy and person-centered medicine*, in *The International Journal of Person Centered Medicine*, 2011, vol. 1,405 ss.;

Moerel L., *Big data protection, How to Make the Draft EU Regulation on Data Protection Future Proof*, 2014, 9, in *www.debrauw.com/wpcontent/uploads/NEWS-PUBLICATIONS/Moerel_oratie.pdf*, 24;

Morace Pinelli A., *Dalla Data Protection alla Data Governance: il regolamento (UE) 2022/868. Commentario al Data Governance Act*, Pisa, Pacini, 2024, 1 ss.;

Morace Pinelli A., *Data Act (reg. UE 2023/2854): la circolazione dei dati nell'interesse privato e generale*, in *Nuova giurisprudenza civile commentata*, 2025,1, 218;

Morace Pinelli A., *La circolazione dei dati personali tra tutela della persona, contratto e mercato*, in *Nuova giurisprudenza civile commentata*, 2022, 1322 ss.;

Morana D., Balduzzi T., Morganti F., *La salute "intelligente":* eHealth*, consenso informato e principio di non-discriminazione*, in *federalismi.it*, 28 dicembre 2022, n. 34, 127 ss.;

Morara P., *Il sistema dei controlli*, in Genco R. (a cura di), *La riforma delle società cooperative*, Milano, Ipsoa, 2003, 211;

Naeem I., Nurul A., Vaska M., Goopy S., Rashid R., Kassan A., Aghajafari F., Ferrer I., Kazi I., Sadi I., O' Bierne M., Leduc C., Turin C.T., *Community-based health data cooperatives towards improving the immigrant community health: a scoping review to inform policy and practice*, 2020, in https://ijpds.org/article/view/1158/3214;

Navone G., *Ieri, oggi e domani della responsabilità civile da illecito trattamento dei dati personali*, in *Nuove leggi civili commentate*, 2022, 132 ss.;

Nazzaro A.C., *L'utilizzo dei Big data e i problemi di tutela della persona*, in *Rassegna di diritto civile*, 2018, 1239 ss.;

Nicolussi A., *Autonomia privata e diritti della persona*, in *Enc. dir.*, Annali, IV, Milano, Giuffrè, 2011, 133 s.

Nicolussi A., *Lo sviluppo della persona umana come valore costituzionale e il cosiddetto biodiritto*, in *Europa e diritto privato*, 2009, 1 s.;

NIGRO A., *Art. 45*, in G. Branca (a cura di) *Commentario della costituzione italiana*, III, Bologna-Roma, Zanichelli, 1980, 4 ss.;

NIVARRA L., *Il disordine delle fonti e l'ordine del diritto*, in *Rivista critica di diritto privato*, 2021, 158 s.;

NORDFALK F., HOEYER K., *The Rise and Fall of an Opt-out System* (2020) 48, in *Scandinavian Journal of Public Health,* 400;

NUCCIO M.R., *Digitalizzazione e circolazione dei dati sanitari*, in *Tecnologie e diritto*, 2023, 357 ss.;

OPPO G., *Sul consenso dell'interessato, Trattamento dei dati e tutela della persona*, in CUFFARO V., RICCIUTO V., ZENO ZENCOVICH V. (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffrè, 1993, 123 s.;

ORSI BATTAGLINI A., *Autorizzazione amministrativa*, in *Digesto delle discipline pubblicistiche*, II, Torino, Utet, 1987, 1 ss.;

OTTOLIA A., *Big Data e innovazione computazionale*, in *Quaderni AIDA* n. 28, Torino, Giappichelli, 2017;

PAGALLO U., *The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection*, in *European Data Protection Law Review,* 2017, 36;

PALMERINI E., *sub art. 82*, GDPR, in *Codice della responsabilità civile*, a cura di NAVARRETTA E., Milano, Lefebvre Giuffrè, 2021, 2497 ss.;

PALMIERI A., PARDOLESI R., *Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)*, in *Foro it.*, 2023, IV, 268 ss.;

PAOLUCCI L. F., *I ristorni nelle cooperative*, in *Società*, 2000, 43;

PARENZO B., *Note sparse in tema di responsabilità da illecito trattamento dei dati personali (a partire da due premesse)*, in *Rassegna di diritto civile*, 2024, 870 ss.;

PASCHKE A., RÜCKER D., *Data governance act, Kommentar*, München, C. H. Beck, 2024;

PATANÈ S., *La revisione cooperativa*, in CUSA E. (a cura di), *La cooperativa s.r.l. fra legge e autonomia statutaria*, Padova, Cedam, 2008, 489;

PATTI S., *Il consenso dell'interessato al trattamento dei dati personali*, in *Rivista di diritto civile*, 1999, II, 455 s.;

PEIGNÉ V., *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2011, 1519 ss.;

Peignè V., *Verso il Fascicolo Sanitario Elettronico: presentazione della riforma francese*, in *Diritto dell'internet*, 2007, 296;

Pelino E., *Commento all'art.110*, in Bistolfi C., Bolognini L., Pelino E., *Il regolamento privacy europeo*, Milano, Giuffrè Lefebvre, 2016, 123;

Pelino E., *I diritti dell'interessato*, in Bolognini L., Pelino E., Bistolfi C. (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Lefebvre Giuffrè, 2016, 225-235;

Pelino E., Bolognini L. (a cura di) *Codice della disciplina privacy*, Milano, Lefevbre Giuffrè, 2024;

Peloquin D., DiMaio M., Bierer B., Barnes M., *Disruptive and avoidable: GDPR challenges to secondary research uses of data, in European Journal of Human Genetics,* 2020, 697 ss., consultabile *on line* all'indirizzo: http://www.nature.com/articles/s41431-020-0596-x;

Perlingieri C., *Intelligenza artificiale in àmbito medico-sanitario: profili di ricostruzione normativa a séguito dell'*AI Act, in Perlingieri C., *Innovazione tecnologica e diritto civile. Saggi*, Napoli, ESI, 2025, 131 ss.;

Perlingieri C., *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici*, in Perlingieri C., *Innovazione tecnologica e diritto civile. Saggi*, Napoli, ESI, 2025, 131 ss.;

Petrone L., *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, 800 ss.;

Pezza F., *Diritto alla portabilità dei dati*, in G.M. Riccio, G. Scorza, E. Belisario, (a cura di) *GDPR e normativa privacy. commentario*, Milano, Lefebvre Giuffrè, 2022, 201 ss.;

Phillips A.M., *The right to insert and add information to my health record – does my doctor need to know this? A critical discussion of the right to insert information in an EHR using the example of data from direct-to-consumer genetic testing*, in Slokenberga S., Ó Cathaoir K., Shabani M. (eds), *The European Health Data Space. Examining A New Era in Data Protection*, London, Routledge, 2025, 44 ss.;

Pioggia A., *Il decreto "rilancio", sanità e sicurezza*, in *Giornale di diritto amministrativo*, 2020, 560;

Pioggia A., *Il Fascicolo sanitario elettronico: opportunità e rischi dell'interope-*

rabilità dei dati sanitari, in CAVALLO PERIN R. (a cura di), *L'amministrazione pubblica con i* big data*: da Torino un dibattito sull'intelligenza artificiale*, Torino, 2021, Università degli studi di Torino, 215 ss.;

PIRAINO F., *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Le nuove leggi civili commentate*, 2017, 390;

PIRAS A., *Profili mutualistici della* governance *delle società cooperative*, in CAMPOBASSO M., CARIELLO V., DI CATALDO V., GUERRERA F., SCIARRONE ALIBRANDI A. (a cura di), *Società, banche e crisi di impresa, Liber amicorum Pietro Abbadessa*, Torino, Utet, 2, 2014, 2023 ss.;

PISCOPO M., ZIPPONI S., *European Health Data Space e uso secondario dei dati: le molte domande ancora senza risposta*, in *www.agendadigitale.eu*;

PIZZETTI G., *Privacy e il diritto europeo alla protezione dei dati personali – Il Regolamento europeo 2016/679*, in PIZZETTI G. (a cura di), *I diritti nella "rete" della rete*, Torino, Giappichelli, 2016;

POLETTI D., *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, 46 ss.;

POSTERARO N., *Danni da responsabilità medica*, in G. CASSANO (a cura di), *Il danno alla persona*, Milano, Lefebvre Giuffrè, 2021, 831 ss.;

POSTERARO N., *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *Federalismi.it* N. 26/2022, 189 ss.;

PRAINSACK B., FORGÓ N., *Why paying individual people for their data is a bad idea,* in *Nature Medicine*, 2022, 28, 1989 ss.;

PROCIDA MIRABELLI DI LAURO A., *La riparazione dei danni alla persona*, Napoli, ESI, 1993, 47;

RACUGNO G., *La società cooperativa*, in *Tratt. dir. comm.*, diretto da BUONOCORE V., IV, 9, Torino, Giappichelli, 2006, 15 ss.;

RANELLETTI O., *Scritti giuridici scelti*, a cura di FERRARI E., SORDI B., Napoli, Jovene, 1992, III, 77 ss.;

RAPISARDA C., *La* privacy *sanitaria alla prova del* mobile ecosystem. *Il caso delle* app *mediche*, in *Le nuove leggi civili commentate*, 2023, 184 ss.;

RAPISARDA C., *Ricerca scientifica e circolazione dei dati personali. Verso il definitivo superamento del paradigma privatistico?*, in *Europa e diritto privato*, 2021, 335 ss.;

Rapisarda C., *Sul costituendo spazio europeo dei dati sanitari*, in *Responsabilità medica*, 2023, 413 ss.;

Reichel J., *Administrative tools for balancing societal and individual interests – data protection safeguards and administrative procedural guarantees in secondary use in the European Health Data Space*, in Slokenberga S., Ó Cathaoir K., Shabani M. (eds), *The European Health Data Space. Examining A New Era in Data Protection*, London, Routledge, 2025, 207 ss.;

Resta G., *La regolazione digitale nell'Unione Europea – Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, 2022, 971 ss.;

Resta G., *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Rivista critica di diritto privato*, 2000, 299 s.;

Resta G., Riccio G.M., *Il DDL AI è legge: primi spunti di riflessione*, pubblicato il 18 settembre 2025 in *www.altalex.com*.

Ricci A., *I diritti dell'interessato*, in Finocchiaro G. (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 183;

Ricci A., *Introduzione al Regolamento europeo sull'accesso equo ai dati e sul loro utilizzo*, in *Le Nuove Leggi Civili Commentate*, 2024, 799;

Ricci A., *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2017, 586 ss.;

Riccio G.M., *Portabilità dei dati personali e interoperabilità,* in Cuffaro V., R. D'Orazio R., Ricciuto V. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 397 ss.;

Ricciuto V., *Base giuridica del trattamento del dato sanitario nell'ottica dell'EHDS*, relazione al Convegno: *Sanità digitale. Regolamento sullo spazio europeo dei dati sanitarie fonti interne*, tenutosi in Roma 21-22 marzo 2025;

Ricciuto V., *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali,* in *Rivista critica di diritto privato,* 2020, 642;

Ricciuto V., *L'equivoco della* privacy. *Persona vs dato personale,* Napoli, ESI, 2022, 137 ss.;

Ricciuto V., *La patrimonializzazione dei dati personali. Contratto e mercato*

nella ricostruzione del fenomeno, in CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *I dati personali nel diritto europeo,* 2019, 40 ss.;

RICHTER H., *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, in *GRUR International*, 72, 5, May 2023, 458-470;

ROCCHI E., *sub* artt. 2512-2514 c.c., in PRESTI G. (a cura di), *Società cooperative*, Milano, Egea, 2006, 28 ss.;

RODON MÒDOL J., *Citizens Cooperation in the Reuse of Their Personal Data: The Case of Data Cooperatives in Healthcare,* in K. RIEMER, S. SCHELLHAMMER, M. MEINERT (eds), *Collaboration in the Digital Age: how technology enables individuals, teams and businesses*, in *Progress in IS,* Berlin, 2018, 159 ss., consultabile in *https://doi.org/10.1007/978-3-319-94487-6_8; I*;

RODOTÀ S., *Conclusioni,* in V. CUFFARO, V. RICCIUTO, V. ZENO ZENCOVICH (a cura di), *Trattamento dei dati* e *tutela della persona,* Milano, 1998, 308;

RODOTÀ S., *Elaboratori elettronici e controllo sociale,* Bologna, Il Mulino, 1973, 47 ss.;

ROLLI R., *Antiche e nuove questioni sul silenzio come tacita manifestazione di volontà*, in *Contratto e Impresa*, 2000, 206;

ROMBOLI R., *Problemi costituzionali della cooperazione*, in *Rivista trimestrale di diritto pubblico*, 1977, 105;

ROSA F., *The use of IT tools and artificial intelligence in the health sector: the patient as a vulnerable subject*, in *European Journal of Privacy Law & Technologies*, 2020, 224 ss.;

ROSSI-MORI A., MACERATINI R., *La cartella clinica elettronica (Electronic Patient Record)*, in *Manuale di informatica medica*, 2000;

RUFFOLO U. (a cura di), *La nuova responsabilità medica*, Milano, Giuffrè, 2018;

RUFO L., *Il dossier sanitario elettronico, Un approccio traslazionale alla disciplina del trattamento dei dati sanitari in ambito clinico*, Bologna, Il Mulino, 2018;

SALANITRO U., *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di giustizia*, in *Rivista di diritto civile*, 2023, 426 ss.;

Salanitro U., *Intelligenza artificiale e responsabilità: la strategia della commissione europea*, in *Rivista di diritto civile*, 2020, 1246 ss.;

Salvatore V. (a cura di), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Torino, Giappichelli, 2023;

Sandulli A., *Abilitazioni, autorizzazioni, licenze*, in *Rassegna di diritto pubblico*, 1958, 3 ss.;

Sandulli A., *Lesione di interessi legittimi e obbligazione risarcitoria della pubblica amministrazione*, in *Rivista trimestrale di dirtto civile*, 1963, 1293 ss.;

Sandulli A., *Notazioni in tema di provvedimenti autorizzativi*, in *Rivista trimestrale di diritto pubblico*, 1957, 784 ss.;

Sborlini D., *Il broad consent come mezzo per la valorizzazione dei dati personali nell'ambito della ricerca scientifica e il suo rilievo negli spazi di condivisione dei dati*, in *Contratto e impresa*, 2024, 223;

Sborlini D., *Proporzionalità dei trattamenti di dati personali svolti mediante dispositivi di geolocalizzazione in ambito lavorativo*, in *Diritto di internet*, 2023, 163;

Schildbach R., *Access to public data and data altruism under the draft Data Governance Act*, in ZD 2022, 148 ss.;

Schreiber K., Pommerening P., Schoel P., *Das neue Recht der Daten-Governance*, 2023 § 4, Rn. 3;

Schmitt T., Cosgrove S., Pajic V., Papadopoulos K., Gille F., *What does it take to create a European Health Data Space? International commitments and national realities*, in *Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen,* 2023, 179, 1 ss.;

Scognamiglio C., *Danno e risarcimento nel sistema del Rgpd: un primo nucleo di disciplina eurounitaria della responsabilità civile?*, in *Nuova giurisprudenza civile commentata*, 2023, 1110 ss.;

Scozzafava T.O., voce *Onere (nozione)*, in *Enc. dir.*, XXX, Milano, Giuffrè, 1980, 99 s.;

Senigaglia R., *Reg. UE 2016/679 e diritto all'oblio nella comunicazione telematica. identità informazione e trasparenza nell'ordine della dignità personale*, in *Nuove leggi civili commentate,* 2017, 1060;

Shekelle P.G., Morton S. C., Keeler E. B., *Costs and benefits of health information technology*, in *Evidence report/technology assessment,* (Full Rep), n. 132, 2006, 1;

SICA S., *Verso l'unificazione del diritto europeo alla tutela dei dati personali*, in SICA S., D'ANTONIO V., RICCIO G.M. (a cura di), *La nuova disciplina europea della privacy*, Milano, Wolters Kluwer, 2016, 893;

SILVANO C., *La digitalizzazione dei servizi sanitari alla luce del riparto di competenze tra Stato e Regioni. Il caso del Fascicolo Sanitario Elettronico*, in *federalismi.it*, 1 novembre 2023, n. 26, 228 ss.;

SLOKENBERGA S., SHABANI M., CATHAOIR K. Ó, *The European Health Data Space: Examining A New Era in Data Protection,* Londra, Routledge, 2025;

SLOKENBERGA S., TZORTZATOU O., REICHEL J., *GDPR and biobanking - individual rights, public interest and research regulation across Europe [Internet*], Springer, 2020, in *https://www.springer.com/gp/book/9783030493875*;

SOKOL T., *European health data space, use of data and data subject's control over their own health data: can an opt-out restore the balance?*, in *European journal of health law*, vol. 31, n. 4, 2024, 365 ss.;

SORRENTINO E., GUAGLIANONE M.T., CARDILLO E., CHIARAVALLOTI M.T., SPAGNUOLO A.F., CAVARRETTA G.A., *La conservazione dei documenti che alimentano il Fascicolo Sanitario Elettronico*, in *Rivista italiana di informatica e diritto*, 2020, 35;

SPECHT L., HENNEMANN M., *Data governance act*, Baden-Baden, C.H. Beck, 2023, 103 ss.;

SPECHT L., RIEMENSCHNEIDER L., BLANKERTZ A., SIEREK P., SCHNEIDER R., KNAPP J., HENNE T., *Die Datentreuhand,* in MMR-Beil. 2021, 25;

SPEZIALE I., *L'ingresso dei dati personali nella prospettiva causale dello scambio: i modelli contrattuali di circolazione*, in *Contratto e impresa*, 2021, 602 ss.;

SPINA A., *La medicina degli algoritmi: Intelligenza Artificiale, medicina digitale e regolazione dei dati personali*, in PIZZETTI G. (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018, 319 ss.;

STAUNTON C., SHABANI M., MASCALZONI D., MEZINSKA S., SLOKENBERGA S., *Ethical and social reflections on the proposed European Health Data Space*, in *European Journal of Human Genetics,* 32, 498–505 (2024);

STEFANELLI S., *Ecosistema Dati Sanitari, c'è la norma: cos'è e come funziona la*

banca dati per la Salute in Italia, in *www.agendadigitale.eu* del 7 marzo 2025;

Stefanelli S., *Thin, perché il Garante sbaglia e blocca la ricerca in Sanità*, in in *www.agendadigitale.eu* del 2 agosto 2023;

Stoykovar R., *The Right to Data Portability. Data protection scope and technical feasibility*, in *Computer Law Review International*, 2018, 3, 65 ss.;

Tacconelli E., Gorskaa A., Carrara E., Davisa R.J., Bontenb M., Friedrichc A.W., Glasnerc C., Goossense H., Hasenauerf J., Haro Abadh M., Peñalvoj J.L., Sanchez-Niuboh A., Sialml A., Scipionem G., Sorianoj G., Yazdanpanahn Y, Vorstenboschh E., Jaenisch T., *Challenges of data sharing in European Covid-19 projects: A learning opportunity for advancing pandemic preparedness and response*, in *The Lancet Regional Health - Europe*, 2022, 1;

Tampieri M., *L'identità personale: il nostro documento esistenziale*, in *Europa e diritto privato*, 2019, 1198 ss.;

Tanwar A.S., Evangelatos N., Venne G., Ogilvie L., Satyamoorthy K., Brand A., *Global Open Health Data Cooperatives Cloud in an Era of COVID-19 and Planetary Health*, in *OMICS: A Journal of Integrative Biology*, 2021, in *https://doi.org/10.1089/omi.2020.01*;

Tarte J.P., Bogiages C.C., *Patient-centered care delivery and the role of information systems*, in *Computer Health*, vol. 13, n. 2, 1992, 44;

Tatarano M. C., *La nuova impresa cooperativa*, Milano, Giuffrè, 2011, 91 ss.;

Tazare J., Henderson A.D., Morley J., Blake H.A., McDonald H.I., Williamson E.J., Strongman H., *NHS National Data Opt-Outs: Trends and Potential Consequences for Health Data Research* (2024) *BJGP Open;*

Teare H.J.A., Prictor M., Kaye J., *Reflections on dynamic consent in biomedical research: the story so far*, in *European Journal of Human Genetics,* 2021, 649–56;

Tedeschi C., *I controlli*, in Marasà G. (a cura di), *Le cooperative prima e dopo la riforma societaria,* Padova, Cedam, 2004, 717;

Terzis P., *Compromises and Asymmetries in the European Health Data Space*, in *European Journal of Health Law*, in *brill.com*, 27 ottobre 2022;

Terzis P., Santamaria Echeverria E., *Interoperability and governance in*

the European Health Data Space regulation, in *Medical Law International*, in *journals.sagepub.com*, 24 aprile 2023;

THIENE A., *Commento all'art. 9*, in D'ORAZIO R., FINOCCHIARO G., POLLICINO O., RESTA G., *Codice della privacy e data protection*, Milano, Giuffrè, 2021, 245;

THIENE A., *La regola e l'eccezione. Il ruolo del consenso in relazione al trattamento dei dati sanitari alla luce dell'art. 9 GDPR* , in THIENE A., CORSO S., *La protezione dei dati sanitari privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, Napoli, Jovene, 2023, 7 ss.;

THIENE A., *Salute, riserbo e rimedio risarcitorio*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2015, 1421;

THIENE A., CORSO S. (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, Napoli, Jovene, 2023, 1 ss.;

THOBANI S., *Consenso al trattamento e delibere assembleari*, in *Giurisprudenza italiana*, 2022, 12, 2599 ss.;

THOBANI S., *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali,* Milano, Ledizioni, 2018;

THOBANI S., *I requisiti del consenso al trattamento dei dati personali*, Rimini, Maggioli, 2016, 2 ss.;

THOMPSON T. J., BRAILER D.G., *The decade of health information technology: delivering consumer-centric and information-rich health care*, Washington, DC: US Department of Health and Human Services, 2004;

TONELLI E., *Scambio mutualistico e rapporto sociale: interferenze e connessioni*, in SANDULLI M., VALENSISE P. (a cura di), *Le cooperative dopo la riforma del diritto societario*, Milano, Franco Angeli, 2005, 29;

TOSI E., *Circolazione dei dati personali tra contratto e responsabilità,* Milano, Lefebvre Giuffrè, 2023, 78 ss.;

TOSI E., *Diritto privato delle nuove tecnologie digitali*, Milano, Lefebvre Giuffrè, 2021, 599;

TOSI E., *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del* nuovo *Codice Privacy*, in TOSI E. (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Lefebvre Giuffrè, 2019, 1;

TOSI E., *Trattamento illecito dei dati personali, responsabilità oggettiva e danno*

non patrimoniale alla luce dell'art. 82 del GDPR UE, in *Danno e responsabilità civile*, 2020, 444 ss.;

Troiano S., *Il diritto alla portabilità dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR* (a cura di Zorzi Galgano), Milano, Wolters Kluwer, 2019, 199;

Troiano V., Motroni R. (a cura di), *La Mifid II. Rapporti con la clientela – regole di governance – mercati*, Milano, Wolters Kluwer, 2016;

Turk M., *Electronic Health Records: How to Suture the Gap Between Privacy and Efficient Delivery of Healthcare*, in *Brooklyn Law review*, vol.80, n. 3, 2015, 565 ss.;

Van Der Auwermeulen B., *How to attribute the right to data portability in Europe: A comparative analysis of legislations*, in *Computer Law & Security Review* 2017, 33, 57, 61;

Van Roessel I., Reumann M., Brand A., *Potentials and Challenges of the Health Data Cooperative Model,* in *Public health genomics* 20, n. 6 (2018): 321–331, consultabile in *https://doi.org/10.1159/000489994*;

Vella F., Genco R., Morara P., *Diritto delle società cooperative*, Bologna, Il Mulino, 2018, 235 ss.;

Venosta F., *Contatto sociale e affidamento*, Milano, Giuffrè, 2021;

Venturi P., Zandonai F., *Neomutualismo. Ridisegnare dal basso competitività e* welfare, Milano, Egea, 2022;

Verrucoli P., voce *Cooperative (Imprese)*, in *Enciclopedia del diritto*, Milano, Giuffrè, 1962, 568;

Versaci G., *La contrattualizzazione dei dati personali dei consumatori,* Napoli, ESI, 2020, *passim*;

Vicarelli G., Bronzini M., *La sanità digitale: dimensioni di analisi e prospettive di ricerca*, in *Politiche sociali*, 2018, 150;

Viciani S., *Strategie contrattuali del consenso al trattamento dei dati personali*, in *Rivista critica di diritto privato*, 1999, 159 s.;

Villata R., *Autorizzazioni amministrative e iniziativa economica privata*, Milano, Giuffrè, 1974, 34;

Visintini G., Cabella Pisu L., *L'inadempimento delle obbligazioni*, in *Tratt. dir. priv.*, diretto da Rescigno P., vol. 9, *Obbligazioni e contratti*, tomo I, Torino, Utet, 1984, 155;

Vivarelli B., *Profilazione dei dati e aziende sanitarie*, in Adinolfi A., Si-

MONCINI A. (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, ESI, 2022, 363 ss.;

VOLPE F. (a cura di), *La nuova responsabilità sanitaria dopo la riforma Gelli-Bianco (legge n.24/2017)*, Bologna, Zanichelli, 2018;

VON DITFURTH L., *Datenmärkte, Datenintermediäre Und Der Data Governance Act: Eine Analyse Der Europäischen Regulierung Von B2b-datenvermittlungsdiensten*, Berlin, De Gruyter, 2023, 265 ss.;

VON HAGEN P., VÖLZMANN L., *Datenaltruismus aus datenschutzrechtlicher Perspektive*, in MMR, 2022, 176 ss.

WANG C.K., *Security and privacy of personal health record, electronic medical record and health information*, in *Problems and Perspectives in Management*, 2015, vol.13, n.4, 19 ss.;

WARREN S., BRANDEIS L., *The right to privacy*, in *Harvard Law Review*, 1890, 5, 193 ss.;

WEBER R.H., *Data portability and big data analytics. New competition policy challenges*, in *Concorrenza e mercato*, 2016, 59;

WILBANKS J., TOPOL E., *Stop the privatization of health data*, in *Nature*, 2016, 345 ss.;

ZAMAGNI S., ZAMAGNI V., *La cooperazione*, Bologna, Il Mulino, 2008.

ZAMBRANO V., *Dati sanitari e tutela della sfera privata*, in *Diritto dell'informazione e dell'informatica*, 1999, 27;

ZANGHERI R., GALASSO G., CASTRONOVO V., *Storia del movimento cooperativo in Italia. La Lega Nazionale delle Cooperative e Mutue (1886-1986)*, Torino, Einaudi,1987;

ZANOBINI G., *Corso di diritto amministrativo*, Milano, 1958, I, 262;

ZENO ZENCOVICH V., *Una lettura comparatistica della l. 675/96 sul trattamento dei dati personali*, 169 s., in CUFFARO V., RICCIUTO V., ZENO ZENCOVICH V. (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffrè, 1993, 123 s.;

ZICCARDI M., *La rivelazione non autorizzata dei "dati relativi alla salute" tra tutela dell'interessato e adeguatezza del rimedio sanzionatorio,* in *Tecnologia e diritto*, 2024, 603 ss.;

ZIPPONI S., MARMORATO G., *Tutela dei dati personali nel settore della ricerca scientifica e delle sperimentazioni cliniche: la normativa comunitaria*, in BO-

lognini L., Zipponi S., *Privacy e diritto dei dati sanitari*, Milano, Lefebvre Giuffrè, 2024, 191 ss.;

Zorzi Galgano N., *Le due anime del GDPR e la tutela del diritto alla* privacy, in Zorzi Galgano N. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, Wolters Kluwer, 2019, 35 ss.

INFORMATION TECHNOLOGY LAW
Series Editors Fabio Bravo *and* Angelo Giuseppe Orofino

1. Stefano Faillace, *Prospettive civilistiche in ordine agli spazi di condivisione dei dati sanitari alla luce del Regolamento EHDS* (2025)

The subject of this monographic work is an in-depth analysis of the rights and legal remedies available to data subjects, as provided under national and European legal frameworks, in cases involving the processing of health data for the purposes of individual care as well as for the pursuit of collective needs. This analysis rests upon the precarious balance between the right to informational self-determination and the free movement of data for scientific research purposes. In examining the experiences of individual Member States of the European Union, a fragmentation and lack of clarity in the regulatory framework have emerged. This situation has led to the most recent Union legislation proposing a partial reconsideration of the approach adopted by the GDPR regarding the primary and secondary use of health data. New regulatory directions have been outlined, such as the strengthening of data subject rights (notably the rights of access, portability, and rectification in the EHDS Regulation); the intermediation of entities capable of inspiring trust in data subjects and supporting them in managing their personal data (Data Governance Act); and the introduction of the requirement for administrative authorisation issued by a public body for the secondary use of health data (EHDS Regulation). Moreover, the EHDS proposes a reversal in the hierarchy of legal bases for the processing of health data, shifting from the primacy of consent to that of public interest, counterbalanced by the possibility for data subjects to exercise an opt-out. This work also undertakes a detailed examination of the contractual and non-contractual liability profiles that may arise when there are deviations from the established terms and conditions governing access to and reuse of health data flows.

5 000002 689963
9 788813 388218
€ 35,00 I.V.A. INCLUSA