

MARCO GUIDI

L'INTERAZIONE TRA LA NORMATIVA DELL'UE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E IL REGOLAMENTO UE 536/2014 SULLE SPERIMENTAZIONI CLINICHE

SOMMARIO: 1. Introduzione. — 2. Ricerca clinica e pseudonimizzazione dei dati personali. — 2.1. Il provvedimento “Thin” del Garante per la protezione dei dati personali in materia di anonimizzazione dei dati personali. — 2.2. La sentenza “CRU” del Tribunale dell’UE e l’approccio “pragmatico” in materia di anonimizzazione dei dati personali. — 3. Le basi giuridiche dei trattamenti dei dati personali nell’ambito delle sperimentazioni cliniche nel diritto dell’UE. — 3.1. L’uso primario dei dati nel diritto dell’UE. — 3.1.1. Le basi giuridiche dei “trattamenti correlati esclusivamente ad attività di ricerca”. — 3.1.2. Le basi giuridiche dei “trattamenti correlati a finalità di tutela della salute”. — 3.2. L’uso secondario dei dati nel diritto dell’UE. — 4. Il consenso quale base giuridica per l’uso primario e secondario dei dati personali: gli articoli 110 e 110-bis del Codice Privacy. — 5. Conclusione.

I. INTRODUZIONE.

L'utilizzo dei dati rappresenta sempre più di frequente un elemento cruciale per l'innovazione in ambito sanitario. Esemplificativo, in tal senso, è il ruolo fondamentale ricoperto dai cd. *big data*¹ durante l'epidemia da COVID-19, con riguardo tanto alle strategie di contenimento del contagio quanto alla verifica in merito all'efficacia e alla sicurezza delle soluzioni terapeutiche, non solo vaccinali, adottate per fronteggiare le sintomatologie associate al virus SARS-CoV-2². Questa tendenza, posta in rilievo

* Un sentito ringraziamento al Prof. M. Carta per i preziosi suggerimenti ai fini della stesura del presente articolo.

¹ V. A. MANTELEIRO, *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, 2022, p. 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, p. 36; A. OTTOLEA, *Big Data e innovazione computazionale*, in *Quaderni AIDA* n. 28, Torino, 2017.

² In tal senso può leggersi il lancio da parte della Commissione europea, nel-

anche dalla recente proposta di regolamento sullo spazio europeo dei dati sanitari³, si è ulteriormente consolidata con l'impiego massivo dell'intelligenza artificiale, che consente di testare rapidamente ed economicamente la potenziale efficacia delle molecole più promettenti in differenti ambiti terapeutici, di svolgere esami diagnostici predittivi oppure, ancora, di apprestare soluzioni di telemedicina, medicina personalizzata e di precisione⁴.

Non stupisce, dunque, che proprio attorno ai dati si sviluppino la conduzione delle sperimentazioni cliniche — *species* del più ampio *genus* dei cd. “studi clinici” — disciplinate dal regolamento 536/2014 (anche solo “Regolamento”)⁵.

Le sperimentazioni cliniche sono indagini svolte su soggetti umani al fine di scoprire o testare la sicurezza e/o l'efficacia dei medicinali e si caratterizzano, rispetto agli studi osservazionali, per il verificarsi di una tra le seguenti condizioni: “a) l'assegnazione del soggetto a una determinata strategia terapeutica è decisa anticipatamente e non rientra nella normale pratica clinica dello Stato membro interessato; b) la decisione di prescrivere i medicinali sperimentali e la decisione di includere il soggetto nello studio clinico sono prese nello stesso momento; c) sono applicate ai

l'aprile del 2020, della cd. *European COVID-19 Data Platform*, ossia la piattaforma europea di dati sul COVID-19 che ha lo scopo, 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. Sul tema v. E. TACCONELLI ET AL., *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, p. 1; N.L. BRACCAZZA ET AL., *How Big Data and Artificial Intelligence Can Help Better Manage the COVID-19 Pandemic*, in *International Journal of Environmental Research and Public Health*, 2020, p. 1.

³ Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari, COM(2022) 197 def.

⁴ V. Agenzia europea per i medicinali, *The use of Artificial Intelligence (AI) in the medicinal product lifecycle*, 19 luglio 2023, EMA/CHMP/CVMP/83833/2023; L. FERRARO, *La telemedicina quale nuova (e problematica) frontiera del diritto alla salute*, in questa *Rivista*, 2022, p. 837; 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, 2018, p. 319.

⁵ Regolamento (UE) 2014/536 del Parlamento europeo e del Consiglio del 16 aprile 2014 sulla sperimentazione clinica di medicinali per uso umano che abroga la direttiva 2001/20/CE, in *GUUE* L 158 del 27 maggio 2014, p. 1. Per una prima introduzione al rapporto tra il GDPR e il regolamento 536/2014 si rimanda a A.W. FOX, *Where is European Regulation 536/2014 Taking Us?*, in *Pharmaceutical Medicine*, 2023, p. 343; E. ARNOLD, *Medical Research and Data Protection in Europe. The Emergence of General Legal Principles*, in V. Colcelli, R. Cipitani, C. Brochhausen-Delius, R. Arnold (a cura di), *GDPR Requirements for Biobanking Activities Across Europe*, Cham, 2023, p. 11; F. DI TANO, *Protezione dei dati personali e ricerca scientifica: un rapporto controverso ma necessario*, in *Rivista di BioDiritto*, n. 1/2022, p. 71; T. MINNSEN, N. RAJAM, M. ROGERS, *Clinical trial data transparency and GDPR compliance: Implications for data sharing and open innovation*, in *Science and Public Policy*, 2020, p. 616; E. TENTI, G. SIMONETTI, M.T. BOCHICCHIO, G. MARTINELLI, *Main changes in European Clinical Trials Regulation (No 536/2014)*, in *Contemporary Clinical Trials Communications*, 2018, p. 99.

soggetti procedure diagnostiche o di monitoraggio aggiuntive rispetto alla normale pratica clinica;”⁶.

La conduzione di sperimentazioni cliniche comporta la raccolta di diversi dati dei soggetti partecipanti allo studio. La prestazione dei consensi informati, la redazione delle cartelle e dei registri clinici, lo svolgimento di visite mediche, gli accertamenti diagnostici e i test di laboratorio, formano quell’insieme di dati e di evidenze scientifiche inclusi nei *dossier* che le industrie farmaceutiche e gli enti di ricerca sottopongono alle Agenzie regolatorie di settore al fine di vedersi riconoscere la cd. autorizzazione all’immissione in commercio dei farmaci *ex art.* 6, par. 1 della direttiva 83/2001⁷.

Il loro utilizzo riveste, quindi, un ruolo primario per la buona riuscita della sperimentazione stessa che, tuttavia, espone a seri rischi la tutela della privacy dei soggetti coinvolti, soprattutto considerata la natura (sensibile) dei dati in questione: i dati personali relativi alla salute⁸.

Ciononostante, il corretto bilanciamento tra il diritto all’accesso a farmaci innovativi e sicuri, corollario del diritto alla salute, e il diritto alla protezione dei dati personali, previsti rispettivamente agli artt. 35 e 8 della Carta dei diritti fondamentali dell’Unione europea, non risulta adeguatamente assicurato né dal regolamento generale sulla protezione dei dati 2016/679 (“GDPR”)⁹ né dal regolamento 536/2014¹⁰.

⁶ Cfr. art. 2, n. 2, Regolamento.

⁷ Direttiva 2001/83/CE del Parlamento europeo e del Consiglio, del 6 novembre 2001, recante un codice comunitario relativo ai medicinali per uso umano, in *GUCE* L 311 del 28 novembre 2001, p. 67. Giova rilevare che nel caso di conflitti tra la direttiva 2001/83/CE e il regolamento 536/2014, trovano applicazioni le disposizioni di quest’ultimo, in quanto norma speciale. Nello specifico, tale ipotesi si verifica tra l’art. 58 del regolamento, che dispone che i dati raccolti nell’ambito della conduzione dello studio devono essere conservati dal promotore per 25 anni, e l’Allegato I della direttiva, che non dispone alcun termine di conservazione dei dati da presentare alle autorità regolatorie per la concessione dell’autorizzazione all’immissione in commercio di un farmaco. Per una introduzione al settore farmaceutico, si rimanda a M. COLANGELO, *Regulation, Innovation and Competition in Pharmaceutical Markets. A Comparative Study*, Oxford, 2023.

⁸ Sulla natura sensibile dei dati sulla salute v. A. THIENE, *Art. 9 Trattamento di categorie particolari di dati personali*, in R. D’Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della privacy e data protection*, cit., p. 240; G. FARES, *I dati relativi alla salute e i trattamenti in ambito sanitario*, in L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica*

e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679, Napoli, 2017, pp. 444 e ss.

⁹ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in *GUUE* L 119 del 4 maggio 2016, p. 1. Per una prima introduzione alla normativa in materia di protezione dei dati personali v. G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *Commentario GDPR e Normativa Privacy*, Milano, 2022; F. ROSSI DAL POZZO, *Il mercato unico digitale europeo e il regolamento UE sulla privacy*, in R. Cavallo Perin, D.U. Galetta (a cura di), *Il Diritto dell’Amministrazione Pubblica digitale*, Torino, 2022, pp. 43 e ss.; R. D’Orazio, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, 2021; V. CUFFARO, R. D’Orazio, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017.

¹⁰ Sul tema della protezione dei dati nell’ambito delle sperimentazioni cliniche v.

Il GDPR, infatti, ad esclusione dei richiami operati dai *consideranda* nn. 156 e 161 — utili ai soli fini ermeneutici — è privo di disposizioni specifiche sul trattamento dei dati nell'ambito delle sperimentazioni cliniche. Se difficilmente si può imputare ad una disciplina a carattere “generale” la mancata previsione di un *corpus* normativo esauriente con riguardo ad un ambito così specifico, cionondimeno occorre rilevare che i numerosi richiami nel GDPR alla conduzione della ricerca scientifica (questo sì, ambito più generale) non sono in grado di sopperire del tutto a tale carenza, in quanto eccessivamente “schiacciati”, a livello testuale e applicativo, sulle differenti fattispecie dell'archiviazione nel pubblico interesse e della ricerca storica o a fini statistici.

A tali lacune non pone rimedio il Regolamento che, seppur norma di carattere speciale rispetto al GDPR, in materia di protezione dei dati personali si limita a richiamare, all'art. 93, il rispetto della direttiva 1995/46¹¹, a quel tempo ancora in vigore.

Anche i numerosi interventi interpretativi di *soft law* della Commissione europea, del Gruppo di lavoro “Articolo 29” (oggi Comitato europeo per la protezione dei dati o cd. “EDPB”), delle Autorità Garanti degli Stati membri e dell'Agenzia europea per i medicinali, sebbene si pongano quali coordinate utili per orientarsi nel complesso contesto dell'utilizzo dei dati sulla salute ai fini delle sperimentazioni cliniche, non sono tuttavia dirimenti. In particolare, come si avrà modo di osservare, le maggiori problematiche afferiscono alla pseudonimizzazione dei dati sulla salute e al loro utilizzo per scopi di ulteriori ricerche cliniche rispetto a quelli originariamente prestabiliti.

2. RICERCA CLINICA E PSEUDONIMIZZAZIONE DEI DATI PERSONALI.

I dati personali sono definiti dall'art. 4, n. 1 GDPR come qualsiasi informazione che identifica, o permette di identificare una persona fisica, definita “interessato”. La norma fornisce un elenco esemplificativo delle informazioni che possono condurre a tale identificazione — diretta o indiretta — dell'interessato, ossia: il suo nome, i dati relativi all'ubicazione, l'indirizzo IP da questi utilizzato durante la navigazione online, gli elementi caratteristici

P. AURUGGI, *Legal Issues in Regulating Observational Studies: The impact of the GDPR on Italian Biomedical Research*, in *European Data Protection Law Review*, 2019, p. 197; C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 2018, pp. 16 e ss.; J.M.M. RUMBOLD, B. PIERSCIONEK, *The Effect of the Ge-*

neral Data Protection Regulation on Medical Research, in *Journal of Medical Internet Research*, 2017, p. 1.

¹¹ Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in *GUCE* L 281 del 23 novembre 1995, p. 31.

della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Come facilmente intuibile, in tale definizione non possono che rientrarvi anche i “dati relativi alla salute”, un insieme estremamente variegato composto da dati connessi “allo stato di salute fisica o mentale passata, presente o futura dello stesso”. Si tratta, infatti, di: (i) informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria; (ii) numeri o simboli attribuiti all’interessato per identificarlo in modo univoco a fini sanitari; (iii) esiti di esami e controlli anatomici o relativi ad una sostanza organica, compresi i dati genetici e i campioni biologici; (iv) informazioni relative a degenza ospedaliera, malattie, disabilità, il rischio di contrarre malattie, indagini anamnestiche, trattamenti clinici o lo stato fisiologico o biomedico dell’interessato, indipendentemente che siano raccolti dagli operatori sanitari, oppure attraverso l’uso di *wearable device*, dispositivi medici o *test* diagnostici in vitro ¹².

Ai fini dell’applicazione del GDPR, questi dati devono essere oggetto di “trattamento”, definito come quell’insieme di operazioni, anche automatizzate, quali “la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione”; la persona fisica o giuridica che svolge tali trattamenti è denominato “titolare” ¹³.

Di converso, è escluso dalla disciplina del GDPR il trattamento dei dati anonimi come, ad esempio, quelli di natura meteorologica, statistica o economico-sociale, e dei dati che, sebbene inizialmente personali, sono stati successivamente sottoposti a processi di anonimizzazione che ne hanno cancellato definitivamente qualsiasi riferimento ad un determinato individuo rendendolo, in tal modo, non più identificabile ¹⁴.

Il discrimine tra dati personali e anonimi, sebbene tracciato a livello formale, risulta di difficile individuazione pratica, anche a causa dell’implementazione di moderne tecniche di “re-identificazione”, in grado di estrarre informazioni di natura

¹² Crf. art. 4, n. 15 e considerando n. 35, GDPR. Inoltre, il considerando 51 GDPR specifica che: “(m)eritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali.”. Sul punto si è espressa anche la Corte di Giustizia dell’Unione europea, sentenza del 5

giugno 2023, *Commissione c. Polonia*, causa C-204/21, ECLI:EU:C:2023:442, par. 345.

¹³ Per le definizioni di “trattamento” e “titolare” cfr. art. 4, nn. 2 e 7, GDPR.

¹⁴ Relativamente ai dati non personali trova applicazione il regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell’Unione europea, in *GUUE* L 303 del 28 novembre 2018.

personale dall'analisi incrociata di *database* di dati anonimi ¹⁵. A tal proposito, il GDPR specifica che identificativi online quali indirizzi *IP* o *cookies* possono lasciare tracce (c.d. *footprint*) che, “se combinate con identificativi univoci e altre informazioni ricevute dai *server*, possono essere utilizzate per creare profili delle persone fisiche e identificarle” ¹⁶. Non deve pertanto stupire che, allo scopo di stabilire se ci si trovi in presenza di dati personali o anonimizzati, il GDPR preveda di tenere in considerazioni molteplici fattori oggettivi e fattuali quali, non solo “i costi e il tempo necessario per l'identificazione”, ma anche le tecnologie attuali e in fase di sviluppo e i *set* di dati servibili dal soggetto che svolge il trattamento ¹⁷. In altre parole, più evolute sono le tecnologie a disposizione del titolare del trattamento, e più ricchi sono i *database* a cui ha accesso, maggiori sono le possibilità di identificare specifici interessati.

In quest'ottica deve, dunque, leggersi l'art. 4, par. 5 del GDPR sulle cd. tecniche di pseudonimizzazione del dato, ossia la sostituzione di dati personali con codici univoci — gli pseudonimi — che, una volta decifrati tramite l'impiego di un'apposita “chiave”, consentono l'identificazione di un individuo. Per via della loro attitudine a re-identificare un determinato individuo essi sono paragonati ai dati personali, con conseguente sottoposizione alla disciplina del GDPR. Tuttavia, il trattamento di dati pseudonimi espone l'interessato a minor rischi rispetto al trattamento di dati personali in chiaro, data la necessità di disporre della chiave di decifrazione per risalire alla sua identità. Per questa ragione, le tecniche di pseudonimizzazione sono considerate misura di sicurezza del trattamento dei dati personali che concorrono ad assicurare un livello adeguato di tutela degli interessati ¹⁸.

In base a tali caratteristiche meglio si comprende il motivo per cui, nell'ambito delle sperimentazioni cliniche, vige l'obbligo di pseudonimizzazione dei dati del paziente. Infatti, l'articolo 1.58 delle cd. *Good Clinical Practice* ¹⁹ specifica che il paziente dovrà essere indicato attraverso un codice identificativo univoco, formato da 9 cifre (3 cifre rispettivamente per il codice del paese in

¹⁵ Gruppo di lavoro “Articolo 29”, Parere 4/2007 del 20 giugno 2007 - WP 136 sul concetto di dati personali; Parere 05/2014 del 10 aprile 2014 - WP 216 sulle tecniche di anonimizzazione. 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.

¹⁶ Considerando n. 30, GDPR.

¹⁷ *Ivi*, considerando n. 26.

¹⁸ Comitato europeo per la protezione dei dati, Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research - Final Report, EDPS/2019/02-08; Garante per la protezione dei dati personali, Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali - 24 luglio 2008, in *GURI* n. 190 del 14 agosto 2008.

¹⁹ Agenzia europea per i medicinali, Guideline for good clinical practice E6(R2), 1° dicembre 2016, EMA/CHMP/ICH/135/1995.

cui si svolge la sperimentazione, per il centro di sperimentazione e per il soggetto arruolato), la cui chiave di decodificazione è nella sola disponibilità dello “sperimentatore principale del Centro”, ossia il medico che conduce le attività di somministrazione del medicinale oggetto di sperimentazione²⁰. Questa impostazione riduce il rischio che l'identità del paziente arruolato possa essere rilevata erroneamente o carpita in maniera fraudolenta.

La riduzione del rischio non è, tuttavia, l'unica ragione per l'utilizzo degli pseudonimi. La pseudonimizzazione consente, infatti, al promotore di riportare il dato al suo stato “in chiaro” in caso di specifiche esigenze. Tramite la decodifica del codice univoco il promotore dello studio può salvaguardare propri diritti, quali quelli di difesa in sede giurisdizionale oppure adempiere ad obblighi di legge come, ad esempio, in ambito di monitoraggio sull'andamento dello studio in osservanza al protocollo, di cui all'art. 48 o, ancora, in materia di farmacovigilanza ex art. 42.

Ne consegue che l'utilizzo di tale pseudonimo caratterizza tutti i principali trattamenti svolti durante la sperimentazione clinica, dalla registrazione dei pazienti fino alle segnalazioni sugli eventi avversi seri (*serious adverse events*), passando dalla redazione del cd. *Case Report Form* contenenti i dati richiesti dal protocollo di studio o all'uso del cd. *Clinical Trials Information System* (CTIS), ossia lo strumento elettronico che supporta il flusso di informazioni tra i promotori delle sperimentazioni cliniche, gli Stati membri, i paesi dello Spazio economico europeo e la Commissione europea²¹.

2.1. Il provvedimento “Thin” del Garante per la protezione dei dati personali in materia di anonimizzazione dei dati personali.

I trattamenti svolti nell'ambito delle sperimentazioni cliniche non sono limitati alla sola sfera dei dati pseudonimi. Non sono rare le ipotesi di impiego di dati anonimi, per irrobustire o verificare le evidenze scientifiche ottenute a conclusione dello studio oppure per effettuare analisi statistiche.

Il perimetro dei dati clinici impiegati, quindi, oscilla tra i dati pseudonimizzati, con conseguente applicabilità del GDPR, e i dati anonimi che, esulando da tale normativa, comportano modalità di utilizzo più ampie e meno gravose. Una valutazione che, come si

²⁰ Cfr. Art. 2, n. 15, Regolamento.

²¹ V. Agenzia europea per i medicinali, Guidance document on how to approach the protection of personal data and commercially confidential information while using the Clinical Trials Information System (CTIS), 10 luglio 2023, EMA/212507/

2021; Z. ZEMŁA-PACUD, G. LENARCZYK, *Clinical Trial Data Transparency in the EU: Is the New Clinical Trials Regulation a Game-Changer?*, in *IIC - International Review of Intellectual Property and Competition Law*, 2023, p. 732.

avrà modo di osservare, può equivalere alla possibilità, o meno, di condurre proficuamente la ricerca stessa.

In tale contesto si inserisce il provvedimento n. 226 del 1° giugno 2023²², con cui il Garante per la protezione dei dati personali (anche solo “Garante”) ha negato la natura anonima ai 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 sul software gestionale “Medico 2000”, 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, quindi, trasferiti a Thin per la conduzione del proprio progetto.

Il provvedimento mette in luce che la società Thin avesse 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 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 locali 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; per tale ragione, l’Autorità ha ordinato a Thin di pagare la somma di € 15.000 a titolo di sanzione amministrativa pecuniaria e di conformare i trattamenti a quanto indicato nel provvedimento stesso, disponendo altresì la sua pubblicazione sul sito *web* del Garante, con contestuale trasmissione alla Federazione Nazionale degli Ordini dei Medici Chirurghi e degli Odontoiatri (FNOMCeO) e agli Ordini Provinciali dei Medici Chirurghi e degli Odontoiatri.

Difatti, a giudizio del Garante, la società sanzionata ha 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.

Tralasciando gli aspetti maggiormente tecnici della vicenda, l’approccio adottato dal Garante nella fattispecie pare eccessiva-

²² Garante per la protezione dei dati personali, provvedimento n. 226 del 1° giugno 2023, doc. web 9913795.

mente formalistico, data l'assenza di una dimostrazione fattuale degli effetti delle tecniche di anonimizzazione oggetto di contestazione, con la conseguenza che la mera possibilità di re-identificare i pazienti interessati, seppur prevedibile a livello teorico, è sufficiente a rendere i dati in questione pseudonimi.

Il provvedimento del Garante sembra, pertanto, 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”²³. Diversamente, questi elementi paiono essere stati presi in considerazione dal giudice di merito che ha disposto la sospensione — seppur parziale — del provvedimento *de quo*, laddove ha previsto la necessità, per la risoluzione della controversia, di accertare se il *software* utilizzato “renda impossibile” la re-identificazione dell'interessato e, “nel caso in cui tale impossibilità non sia totale, quale sia il concreto rischio di re-identificazione, nonché il suo costo (quantomeno in termini di tempo);”²⁴.

2.2. La sentenza “CRU” del Tribunale dell'UE e l'approccio “pragmatico” in materia di anonimizzazione dei dati personali.

Sotto il profilo dell'anonimizzazione dei dati personali si è di recente espresso il Tribunale dell'Unione europea con la sentenza *CRU* che, seppur afferente al settore creditizio, offre interessanti spunti di analisi²⁵. Il caso di specie origina da una decisione del Garante europeo della protezione dei dati (“GEPD”) nei confronti del Comitato di Risoluzione Unico (“CRU”)²⁶, relativamente al programma da questi adottato nei riguardi del Banco Popolar

²³ Considerando n. 26, GDPR.

²⁴ Tribunale di Milano, Ordinanza del 4 dicembre 2023, n. 29521.

²⁵ Tribunale UE, sentenza del 26 aprile 2023, causa T-557/20, *Comitato di risoluzione unico (CRU)*, ECLI:EU:T:2023:219.

²⁶ Il Comitato di risoluzione unico (CRU) o *Single Resolution Board* (SRB) è l'autorità di risoluzione delle crisi dell'Unione bancaria europea istituita dall'art. 42 del Regolamento (UE) n. 806/2014 (v.

infra), al quale è devoluta la gestione del “Meccanismo di Risoluzione Unico”, cardine insieme al “Fondo di risoluzione unico” della cd. Unione bancaria. V. L. DONATO, Z. ROTONDI, A. SCOGNAMIGLIO, *La disciplina europea sulle crisi bancarie: dal modello normativo all'impatto per il sistema bancario italiano*, in *Banca Impresa Società*, 2018, pp. 79 e ss.; D. ROSSANO, *La nuova regolazione delle crisi bancarie*, Milano, 2017.

Español SA, sulla base del regolamento (UE) n. 806/2014²⁷. In tale contesto, CRU ha richiesto alla società Deloitte di valutare, ai sensi dell'art. 20, para. da 16 a 18 del suddetto Regolamento, se gli azionisti e i creditori avrebbero potuto ricevere un trattamento migliore nel caso in cui il Banco Popular fosse stato sottoposto a una procedura ordinaria di insolvenza. A tal fine, CRU ha condiviso con Deloitte una serie di osservazioni generate dall'analisi di un questionario compilato, anche con l'inserimento dei propri dati personali, dagli azionisti e creditori coinvolti. Tali osservazioni erano state precedentemente oggetto di un processo di pseudonimizzazione volto a sostituire i riferimenti individuali con un codice alfanumerico, mediante cui solo CRU avrebbe potuto risalire all'identità del soggetto compilante; ciò al solo fine di consentire la verifica, e la relativa prova, che ogni osservazione fosse stata trattata e debitamente presa in considerazione, mentre a Deloitte non era consentito l'accesso alla chiave di decifrazione di tali codici alfanumerici. Peraltro, le osservazioni controverse erano state filtrate, classificate e aggregate da CRU prima della condivisione, cosicché delle 23.822 osservazioni complessive, Deloitte ne aveva ricevute solamente 1.104.

A seguito dei reclami esperiti dagli azionisti e creditori che lamentavano la carenza, nella informativa sulla protezione dei dati personali loro fornita da CRU, della menzione di Deloitte quale potenziale destinatario dei propri dati personali, il GEPD ha aperto un'indagine formale conclusasi con l'accertamento della violazione dell'obbligo di informazione previsto all'art. 15, par. 1, lett. d) del regolamento 2018/1725²⁸, sulla base del fatto che le osservazioni trasmesse riportavano dati pseudonimizzati, ossia il citato codice alfanumerico.

Il Tribunale è stato, quindi, chiamato da CRU ad esprimersi sulla vicenda al fine di annullare il provvedimento del GEPD, ai sensi dell'art. 263 TFUE. I Giudici del Lussemburgo, richiamandosi alla precedente sentenza *Breyer*²⁹, relativa alla possibilità che un indirizzo IP dinamico costituisca un dato personale, ha rimarcato l'importanza della valutazione degli elementi fattuali per lo svolgimento della verifica sulla natura anonima, o meno, dei dati. Infatti, se da un lato, come sostenuto dal GEPD,

²⁷ Regolamento (UE) n. 806/2014 del Parlamento europeo e del Consiglio, del 15 luglio 2014, che fissa norme e una procedura uniformi per la risoluzione degli enti creditizi e di talune imprese di investimento nel quadro del meccanismo di risoluzione unico e del Fondo di risoluzione unico e che modifica il regolamento (UE) n. 1093/2010, in *GUUE* L 225 del 30 luglio 2014, p. 1.

²⁸ Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23

ottobre 2018, 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, in *GUUE* L 295 del 21 novembre 2018, p. 39.

²⁹ Corte di giustizia dell'Unione europea, sentenza *Breyer*, cit.

l'indisponibilità in capo a Deloitte delle informazioni aggiuntive necessarie per identificare gli autori delle osservazioni non consente di escludere a priori il trattamento dei dati personali, dall'altro lato, una siffatta verifica deve svolgersi "dal punto di vista" di Deloitte stessa ³⁰. Pertanto, precisa il Tribunale, incombeva al CEPD esaminare se le osservazioni inviate a Deloitte costituissero dati personali, tenendo in conto "se Deloitte disponeva di mezzi legali e realizzabili in pratica" che le consentissero di accedere alle informazioni aggiuntive necessarie per la re-identificazione degli autori delle osservazioni ³¹.

In conclusione, l'approccio adottato dal Tribunale pare discostarsi dall'interpretazione del Garante nel suddetto caso *Thin*, in aderenza, invece, a quanto precisato nelle linee guida dell'EPBD ³² e delle autorità garanti nazionali per la protezione dei dati ³³, che hanno delineato alcuni approdi interpretativi in materia di anonimizzazione dei dati. 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 ³⁴. Tale verifica sulla riduzione del rischio, specifica l'EPBD, deve svolgersi "caso per caso" ³⁵.

Sulla stessa scorta si pongono anche le c.d. Regole deontologiche

³⁰ Tribunale UE, sentenza *CRU*, cit., par. 97.

³¹ *Ivi*, par. 105.

³² Gruppo di lavoro "Articolo 29", Parere 5/2014 sulle tecniche di anonimizzazione, cit.

³³ Sul punto si vedano le linee guida in materia di pseudonimizzazione dell'Agencia Espanola Protección 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-anonimi-dad-en.pdf> e quelle, in materia di anonimizzazione, redatte dall'Information Commissioner's Office, Privacy-enhancing technologies (PETs), 2023, disponibili all'indirizzo online <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf>.

³⁴ Tra le tecniche 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, Gruppo di lavoro "Articolo 29", Parere 5/2014 sulle tecniche di anonimizzazione, cit., para. 3.1 e ss.

³⁵ *Ivi*, par. 5. Sul punto v. anche Commissione europea, Comunicazione del 29 maggio 2019 - Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, COM(2019) 250 def., par. 2.1, ove si precisa che: "(l)a valutazione se i dati siano stati adeguatamente resi anonimi dipende dalle condizioni specifiche ed uniche di ogni singolo caso".

per trattamenti a fini statistici o di ricerca scientifica³⁶, all. 4 del d.lgs. 196/2003 (“Codice Privacy”)³⁷, novellato dal d.lgs. 101/2018³⁸, 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 citato caso Thin.

3. LE BASI GIURIDICHE DEI TRATTAMENTI DEI DATI PERSONALI NELL’AMBITO DELLE SPERIMENTAZIONI CLINICHE AI SENSI DEL DIRITTO DELL’UE.

3.1. *L’uso primario dei dati nel diritto dell’UE.*

Se la pseudonimizzazione e anonimizzazione dei dati costituiscono, quindi, un utile strumento di riduzione del rischio di

³⁶ 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, in *GURI* n. 11 del 14 gennaio 2019.

³⁷ D. Lgs. n. 196/2003, recante il « Codice in materia di protezione dei dati personali » (« Codice Privacy »), in *GURI* n. 174 del 29 luglio 2003.

³⁸ D. Lgs. n. 101/2018, recante « Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del

Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) », in *GURI* n. 205 del 4 settembre 2018. V. con particolare riferimento alla disciplina di adeguamento dettata dal d.lgs. 101/2018 e agli effetti in ambito sanitario L. DURST, *Il trattamento di categorie di dati in ambito sanitario*, in R. Panetta (a cura di) *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, 2019, pp. 75 e ss.

violazioni alla privacy dei soggetti partecipanti ad una sperimentazione clinica, la loro adozione non esaurisce i requisiti normativi per la liceità del trattamento dei dati personali ³⁹.

A tal fine, infatti, il trattamento deve fondarsi su di una tra le sei “basi giuridiche” previste dall’art. 6 GDPR, la cui individuazione spetta al titolare, in ossequio ai principi di liceità e di responsabilizzazione *ex art. 5*, para. 1 e 2 GDPR, e in previsione della finalità e natura del trattamento che questi intenda svolgere. La finalità del trattamento e la sua base giuridica sono, quindi, strettamente correlate: la preventiva individuazione della finalità del trattamento guida il titolare a stabilire quale sia la specifica base giuridica più adatta a conseguirla.

Dietro indicazione della Commissione europea *ex art. 70*, par. 1, lett. b) GDPR, su tale rapporto si è di recente espresso l’EPBD che ha discriminato, innanzitutto, tra uso primario e secondario dei dati ⁴⁰.

L’uso primario include tutti i trattamenti svolti per la conduzione della sperimentazione clinica, in aderenza al suo protocollo ⁴¹. Tale uso va a coprire, dunque, tutti i trattamenti svolti durante l’intero ciclo di vita della sperimentazione, dall’arruolamento dei pazienti fino alla cancellazione dei dati alla scadenza del periodo di archiviazione, passando per le necessarie attività di farmacovigilanza previste dal Regolamento. Questa ampia definizione include i “trattamenti correlati esclusivamente ad attività di ricerca” e i “trattamenti correlati a finalità di tutela della salute”.

3.1.1. Le basi giuridiche dei “trattamenti correlati esclusivamente ad attività di ricerca”.

A seconda dell’inquadramento giuridico del titolare, quale ente pubblico o privato, e dell’attività di sperimentazione da questi svolta, il trattamento dei dati personali correlati esclusivamente alle attività di ricerca può prevedere tre basi giuridiche.

Queste basi giuridiche, insieme alle disposizioni di cui all’art. 9 GDPR inerenti ai dati particolari, costituiscono le condizioni di liceità del trattamento. A tal proposito, infatti, l’art. 9 dispone, al paragrafo 1, un divieto al trattamento dei dati particolari, a meno

³⁹ Sulla liceità del trattamento v. D. POLETTI, *Art. 6 - Liceità del trattamento*, in R. D’Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice Della Privacy E Data Protection*, cit., p. 191.

⁴⁰ Comitato europeo per la protezione dei dati, *Parere 3/2019 relativo alle domande e risposte sull’interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati (articolo 70, paragrafo 1, lettera b))*, 23

gennaio 2019. Sul concetto di finalità nell’ambito della ricerca scientifica v. R. BECKER ET AL., *Purpose definition as a crucial step for determining the legal basis under the GDPR: implications for scientific research*, in *Journal of Law and the Biosciences*, 2024, p. 1.

⁴¹ L’Allegato I del Regolamento specifica che “il protocollo descrive l’obiettivo, il disegno, la metodologia, gli aspetti statistici, lo scopo e l’organizzazione della sperimentazione clinica.”.

che non ricorra una delle esenzioni previste al seguente paragrafo 2. Pertanto, qualsiasi trattamento dei dati personali particolari per superare il vaglio di legittimità previsto dal GDPR deve fondarsi su una delle basi giuridiche di cui all'art. 6, e allo stesso tempo prevedere il ricorrere di una delle esenzioni di cui al citato paragrafo 2 dell'art. 9.

Fatta questa doverosa premessa, si osserva che la prima base giuridica adottabile per fondare un trattamento di dati personali ai fini di ricerca clinica è "l'esecuzione di un compito di interesse pubblico" di cui all'art. 6, par. 1, lett. e). Il GDPR chiarisce, infatti, che nella definizione di "pubblico interesse" sono ricompresi anche finalità inerenti alla salute, quali la sanità pubblica, la protezione sociale e la gestione dei servizi di assistenza sanitaria. L'utilizzo di questa base giuridica, però, è condizionato da un duplice requisito: la conduzione delle sperimentazioni cliniche deve, da un lato, rientrare direttamente nel mandato conferito al titolare e, dall'altro lato, derivare da una norma del diritto dell'Unione o di uno Stato membro. In questo ambito, un singolo atto giuridico può essere sufficiente come base per più trattamenti. Tuttavia, tale atto dovrà stabilire la finalità del trattamento, le caratteristiche in base a cui designare il titolare, il tipo di dati personali in oggetto, gli interessati, i soggetti cui possono essere comunicati i dati personali, le limitazioni della finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto⁴². L'applicabilità di tale base giuridica non è limitata alle sole pubbliche autorità, comprendendo anche i soggetti privati⁴³.

Anche il cd. "legittimo interesse" del titolare del trattamento di cui all'art. 6, par. 1, lett. f) può fondare la liceità del trattamento, ma in tal caso sarà necessario svolgere un bilanciamento tra gli interessi del titolare e le "ragionevoli aspettative" dei diritti dei partecipanti alla sperimentazione⁴⁴.

Entrambe le suddette basi giuridiche devono accompagnarsi all'applicazione di una delle esenzioni elencate al citato art. 9, par. 2.

Si tratta, innanzitutto, dell'ipotesi di cui alla lett. i), secondo cui il trattamento dei dati particolari è lecito se "necessario per motivi

⁴² Art. 6, par. 3 e considerando n. 45, GDPR.

⁴³ Gruppo di lavoro "Articolo 29", Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE del 9 aprile 2014 - WP 217, p. 25.

⁴⁴ Considerando n. 47, GDPR. Sul concetto di legittimo interesse si rimanda a Gruppo di lavoro "Articolo 29", Parere 6/2014 sul concetto di interesse legittimo,

cit.; I. KAMARA, P. DE HERT, *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach*, in *Brussels Privacy Hub - Working Paper*, 2018, p. 4; C. D'ACATA, *Il legittimo interesse del titolare o di un terzo nel quadro dei diversi presupposti di legittimità del trattamento*, in R. Panetta (a cura di) *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, cit., p. 81.

di interesse pubblico nel settore della sanità pubblica, sulla base del diritto dell'Unione o degli Stati membri".

In tal caso, il concetto di sanità pubblica è da interpretarsi, per via del riferimento esplicito al regolamento (CE) n. 1338/2008⁴⁵, in maniera estesa, ricomprendendosi: "tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale ad essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità."⁴⁶ Alla luce di ciò, rientrano in questa esenzione di cui all'art. 9, par. 2, lett. i) i trattamenti svolti per la "protezione da gravi minacce per la salute a carattere transfrontaliero" oppure per "la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici (...)".

Si potrà altrimenti optare per l'esenzione dettata dall'art. 9, par. 2, lett. j), secondo cui il trattamento dei dati particolari è lecito qualora "necessario a fini (...) di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale (...)". Il GDPR precisa che il concetto di "ricerca scientifica" è da intendersi in senso lato ricomprendendo, ad esempio, "sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati", nonché "gli studi svolti nell'interesse pubblico nel settore della sanità pubblica."⁴⁷

Le previsioni di cui alle lettere i) e j) sono accomunate, quindi, dalla "necessarietà" del trattamento in base all'interesse pubblico sotteso, dal rispetto dei principi di proporzionalità e di finalità, nonché dalla previsione di "*misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*".

● Quale terza base giuridica disponibile al titolare per i tratta-

⁴⁵ Regolamento (CE) n. 1338/2008 del Parlamento europeo e del Consiglio, del 16 dicembre 2008, relativo alle statistiche comunitarie in materia di sanità pubblica e di salute e sicurezza sul luogo di lavoro, in GUUE L 354 del 31 dicembre 2008, p. 70.

⁴⁶ Considerando n. 54, GDPR, che riprende quanto previsto dall'art. 3, lett. c) del citato regolamento (CE) n. 1338/2008.

⁴⁷ Ai sensi del considerando 159 GDPR. Sul punto, il Gruppo di lavoro "Articolo 29" ha precisato, tuttavia, che "tale nozione non possa essere estesa oltre il suo significato comune e che per "ricerca scientifica", in questo contesto, si intenda un progetto di ricerca istituito in conformità con le pertinenti norme metodologiche e

deontologiche settoriali, in linea con le buone prassi.", Gruppo di lavoro "Articolo 29", Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, 28 novembre 2017, WP 259 rev.01. In materia di ricerca scientifica e protezione dei dati si rimanda a G.M. UDA, *Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., p. 557. Sul tema v. anche Garante europeo della protezione dei dati, *A Preliminary Opinion on data protection and scientific research*, 2020, disponibile all'indirizzo online https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

menti in questione figura il consenso *ex art. 6, par. 1, lett. a)*⁴⁸. Con specifico riferimento alle categorie di dati particolari, tenuto conto della loro natura sensibile sotto il profilo dei diritti e delle libertà fondamentali, tale consenso deve essere manifestato “esplicitamente”, ossia per iscritto, come stabilito dall’art. 9, par. 2, lett. a) GDPR⁴⁹. Attraverso la prestazione di un siffatto consenso esplicito, il paziente acconsente quindi che il titolare svolga un trattamento dei suoi dati personali, anche di natura particolare e tale trattamento può considerarsi lecito *ex artt. 6 e 9 GDPR*.

Tuttavia, il consenso, quale la base giuridica del trattamento nell’ambito delle sperimentazioni cliniche, comporta alcune criticità. Ai sensi del combinato disposto dagli artt. 5, 6, par. 1, lett. a) e 7 GDPR, il consenso deve essere prestato attraverso un atto positivo con cui l’interessato manifesta una volontà libera, specifica, informata e — novità introdotta dal GDPR — “inequivocabile”, relativa al trattamento dei dati personali che lo riguardano, con ciò prevedendosi che l’interessato abbia una scelta effettiva e il controllo sui propri dati⁵⁰. Il GDPR stabilisce che, qualora l’interessato non disponga di una scelta effettiva, sentendosi invece obbligato ad acconsentire oppure rischi di subire conseguenze negative per il diniego al trattamento dei propri dati, il consenso non potrà considerarsi come validamente acquisito⁵¹. In buona sostanza il consenso non è considerato libero se l’interessato non può rifiutarlo, senza che dal rifiuto espresso possa derivarne un qualche pregiudizio. Sul punto, come messo in rilievo anche dall’EDPB⁵², il consenso non parrebbe la condizione di liceità più adatta ad un contesto dove, spesso, l’interessato non ha reali alternative alla sua prestazione, a costo altrimenti di rischiare di non vedersi arruolato in una sperimentazione clinica che può rappresentare l’unica reale soluzione e risposta ai propri bisogni terapeutici inevasi.

Pertanto, tale orientamento è conforme a quanto previsto dall’art. 28 del Regolamento 536/2014 con riferimento al (differente) consenso informato, requisito essenziale delle sperimentazioni cliniche che coinvolgono gli esseri umani. Tale norma specifica che: “ai fini della certificazione della libertà del consenso infor-

⁴⁸ 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*, Torino, 2017, pp. 127 e ss.

⁴⁹ Comitato europeo per la protezione dei dati, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 13 maggio 2020, par. 4.

⁵⁰ Considerando nn. 32, 42 e 43, GDPR.

⁵¹ Art. 7 e considerando nn. 42 e 43, GDPR.

⁵² Comitato europeo per la protezione dei dati, *Linee guida 5/2020 sul consenso*, cit., para. 13 e ss.; v. E. S. DOVE, J. CHEN, *Should Consent for Data Processing Be Privileged in Health Research? A Comparative Legal Analysis*, in *International Data Privacy Law*, 2020, p. 117; M. DONNELLY, M. McDONACH, *Health Research, Consent and the GDPR Exemption*, in *European Journal of Health Law*, 2019, p. 97.

mato, lo sperimentatore dovrebbe tenere conto di tutte le pertinenti circostanze che possono influenzare la decisione di un potenziale soggetto di partecipare a una sperimentazione clinica, in particolare l'eventuale appartenenza del soggetto a un gruppo economicamente o socialmente svantaggiato o magari una sua situazione di dipendenza istituzionale o gerarchica potenzialmente in grado di influire in maniera non appropriata sulla decisione di partecipare.”⁵³.

Dunque, la prestazione di tali forme di consenso risponde a differenti necessità: da una parte, la tutela del diritto alla protezione dei dati di carattere personale, con riferimento al consenso previsto dal GDPR; dall'altra parte, la tutela del diritto alla dignità umana e all'integrità dell'individuo di cui agli articoli 1 e 3 della Carta dei diritti fondamentali dell'Unione europea, per quanto attiene invece all'obbligo di raccolta del consenso informato dei partecipanti a una sperimentazione clinica. Ciononostante, rispetto ad entrambi i suddetti consensi, soprattutto nell'ambito di sperimentazioni cliniche particolarmente delicate quali, ad esempio, quelle relative ai farmaci salvavita, possono sorgere seri interrogativi sul pieno rispetto del principio della libertà della prestazione del consenso. Ne consegue la necessità di prevedere, in merito al consenso informato di carattere medico, una verifica rafforzata sulle intenzioni e condizioni del singolo che sottendono la sua decisione di sottoporsi alla sperimentazione clinica, adottando specifiche salvaguardie quali lo “scambio comunicativo continuo e interattivo” con i ricercatori e l'adeguamento agli “effettivi rischi e benefici di ciascun protocollo”⁵⁴; in merito al consenso sulla privacy, l'adozione di altre basi giuridiche, quali l'esecuzione di un compito di interesse pubblico o, in via residuale, il legittimo interesse.

3.1.2. *Le basi giuridiche dei “trattamenti correlati a finalità di tutela della salute”.*

Come anticipato, l'uso primario dei dati include altresì i trattamenti correlati a finalità di tutela della salute, i quali sono espressamente previsti dal Regolamento e sono correlati al moni-

⁵³ Il consenso informato deriva dai requisiti etici fondamentali consolidati dalla World Medical Association, Declaration of Helsinki: ethical principles for medical research involving human subjects, vers. 2008. Sul tema si rimanda a F. FORNI, *Consenso informato e sperimentazione clinica nella normativa dell'Unione europea*, in *Dir. com. sc. int.*, 2012, pp. 215 e ss.

⁵⁴ Crf. Centro di Coordinamento Nazionale dei Comitati Etici, *Linee di indirizzo per la raccolta del consenso informato alla partecipazione a sperimentazioni cliniche*, 2020, disponibile all'indirizzo online https://www.aifa.gov.it/documents/20142/1619583/linee_indirizzo_centro_coordinamento_20_05_2022.pdf.

toraggio delle condizioni di salute del paziente arruolato nello studio.

Derivando da previsioni normative, questi trattamenti possono considerarsi come necessari “per adempiere un obbligo legale al quale è soggetto il titolare del trattamento”, base giuridica disposta dall’art. 6, par. 1, lett. c) GDPR. Si tratta dei trattamenti dei dati relativi agli obblighi imposti dal Regolamento in tema di: (i) reportistica della sintesi dei risultati della sperimentazione che, ai sensi dell’art. 37, para. 4 e 8, il promotore deve pubblicare sulla banca dati UE; (ii) comunicazione degli eventi avversi e di eventi avversi gravi, da parte dello sperimentatore al promotore, ex art. 41; (iii) comunicazione delle sospette reazioni avverse che, ex art. 42, devono essere riportate dal promotore all’Agenzia regolatoria nazionale, tramite la banca dati elettronica per le comunicazioni in materia di sicurezza di cui all’art. 40; (iv) monitoraggio obbligatorio, da parte del promotore, sull’affidabilità dei dati comunicati e sulla conduzione della sperimentazione, ai sensi dell’art. 48; (v) obblighi di registrazione, elaborazione, gestione e conservazione, in capo al promotore o allo sperimentatore, di tutte le informazioni sulla sperimentazione clinica, assicurando al contempo la riservatezza dei dati personali degli interessati, anche attraverso la previsione di misure tecniche e organizzative idonee a limitare il rischio di “*data breach*”, ai sensi dell’art. 56; (vi) archiviazione del fascicolo permanente, inclusivo di tutti i documenti essenziali e i dati clinici generati durante la conduzione dello studio, per venticinque anni, come prescritto dall’art. 58; e, infine, (vii) sottoposizione ad attività ispettive condotte dall’autorità di uno Stato membro e relative anche ai dati clinici dei soggetti arruolati, ex art. 78.

Anche questa base giuridica deve accompagnarsi alla già citata esenzione ex art. 9, par. 2, lett. i) GDPR, al fine di rendere lecito il trattamento dei dati sulla salute.

3.2. *L’uso secondario dei dati nel diritto dell’UE.*

Nell’ambito della conduzione delle sperimentazioni cliniche, i dati personali possono venir utilizzati dal promotore o dallo sperimentatore per fini scientifici diversi da quelli specificati nel protocollo di studio⁵⁵. Ad esempio, un ospedale potrebbe eseguire degli esami medici su un paziente allo scopo di diagnosticare una particolare malattia e, successivamente, decidere di utilizzare i dati raccolti nell’ambito di una sperimentazione clinica. L’uso secondario dei dati clinici è particolarmente diffuso per via della

⁵⁵ B. CUSTERS, H. URŠIČ, *Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal*

Data Protection, in *International Data Privacy Law*, 2016, p. 4.

sempre maggiore disponibilità dei dati dei pazienti che, conservati in registri e archivi sanitari (diari, cartelle mediche elettroniche, banche dati, ecc.), offrono utili spunti di indagine su impieghi innovativi di molecole e/o farmaci, non prevedibili al tempo della loro raccolta. Si tratta del cd. “uso secondario dei dati”, prassi ampiamente diffusa nell’ambito degli studi clinici che, nel GDPR, viene ricondotta, non senza difficoltà, al “trattamento ulteriore” di cui all’art. 5, par. 1, lett. b) secondo cui, qualora i dati siano soggetti ad un nuovo trattamento per finalità di ricerca scientifica, essa non è considerata a priori incompatibile con la finalità iniziale, salvo il rispetto dell’art. 89, par. 1 GDPR ⁵⁶.

Sulla base di questo presupposto normativo, come interpretato sia dall’EDPB ⁵⁷ sia dal GEPD ⁵⁸, il trattamento dei dati personali per uso secondario può godere di una “presunzione di compatibilità” con il trattamento per uso primario, con notevoli effetti in termini di riduzione degli oneri sostanziali e procedurali in capo al titolare.

Il trattamento previsto con finalità “secondary use” non è, tuttavia, privo di condizioni.

Innanzitutto, l’art. 89 GDPR stabilisce l’obbligo di adottare garanzie rafforzate, quali la predisposizione di apposite misure tecniche e organizzative, per la tutela dei diritti e della libertà dell’interessato ⁵⁹. Inoltre, l’art. 6, par. 4 GDPR prevede obblighi aggiuntivi laddove il trattamento non sia fondato sul consenso dell’interessato o su un atto legislativo dell’Unione o degli Stati membri. In tali casi, infatti, il titolare deve tenere conto: “a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell’ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l’interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell’articolo 9 (...); d) delle possibili conseguenze dell’ulteriore trattamento previsto per gli interessati;”.

⁵⁶ Sulle differenze tra “uso secondario”, utilizzato in campo biomedico, e “trattamento ulteriore” di cui al GDPR si rimanda a R. BECKER ET AL., *Secondary Use of Personal Health Data: When Is It “Further Processing” Under the GDPR, and What Are the Implications for Data Controllers?*, in *European Journal of Health Law*, 2023, pp. 135 e ss.

⁵⁷ Il Comitato europeo per la protezione dei dati si è espresso prima con il citato parere 3/2019 e, in seguito alle ulteriori domande poste dalla Commissione eu-

ropea, con il documento di risposta alla domanda di chiarimenti della Commissione europea in merito all’applicazione coerente del GDPR, con un’attenzione particolare alla ricerca in campo sanitario del 2 febbraio 2021.

⁵⁸ V. Garante europeo della protezione dei dati, *A Preliminary Opinion on data protection and scientific research*, cit.

⁵⁹ V. Comitato europeo per la protezione dei dati, *Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research - Final Report*, cit.

Il rispetto di tali disposizioni farebbe venir meno l'obbligo di richiesta di un ulteriore consenso agli interessati, con una conseguente diminuzione di oneri di particolare rilievo, se si pensa alle difficoltà di reperire tutti gli interessati che hanno partecipato alla sperimentazione clinica in cui erano stati precedentemente raccolti i dati. In tal senso può citarsi, ad esempio, l'articolo 14, par. 5, lett. b) GDPR che esenta 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 ⁶⁰.

Tuttavia, come evidenziato anche dall'EDPB, tale "agevolazione" potrebbe incontrare alcuni limiti pratici, dovuti alla libertà concessa agli Stati membri dall'art. 6, par. 2 in merito alla possibilità di prevedere "disposizioni più specifiche" riguardo alle basi giuridiche del GDPR nonché di apporre "ulteriori condizioni, comprese limitazioni" al trattamento dei dati sulla salute *ex art. 9, par. 4* (cd. "Clausole di apertura"). Non deve pertanto stupire che nella legislazione degli Stati membri si riscontrino notevoli differenze sotto i profili sia delle basi giuridiche per il trattamento dei dati sanitari di cui all'art. 6, specificamente laddove esse facciano riferimento al "diritto degli Stati membri" (lett. c) o e)), sia delle esenzioni al divieto di trattamento dei dati personali particolari di cui all'art. 9, par. 2, con specifico riferimento ai casi in cui tali esenzioni dipendano dall'applicazione del diritto nazionale (lett. g), i) o j)) ⁶¹.

L'eterogeneità delle legislazioni nazionali non causa solo la necessità, per la conduzione di una sperimentazione clinica in più Stati membri, di utilizzare più basi giuridiche per il medesimo trattamento dei dati, bensì anche una compressione dei margini di applicabilità della presunzione di compatibilità per il trattamento ulteriore dei dati *ex art. 5* GDPR. Infatti, è possibile che l'esenzione dal divieto di trattamento dei dati sanitari su cui il titolare del trattamento ha fatto affidamento per la finalità originaria non ricorra nella legislazione di un diverso Stato membro ove si intenda condurre il trattamento ulteriore ⁶².

Ad esempio, qualora il diritto di uno Stato membro restringa il

⁶⁰ 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. V. Garante per la protezione dei dati personali, provvedimento n. 285 del 6 luglio 2023, doc. web 9919999.

⁶¹ Commissione europea, Assessment of the EU Member States' rules on health data in the light of GDPR Specific Contract

No SC 2019 70 02 in the context of the Single Framework Contract Chafea/2018/Health/03, 2021, disponibile online all'indirizzo https://health.ec.europa.eu/system/files/2021-02/ms_rules_health_data_en_0.pdf.

⁶² V. COLCELLI, *Applying National Law in Cross-Border Research Activity*, in V. Colcelli, R. Cippitani, C. Brochhausen-Delius, R. Arnold (a cura di), *GDPR Requirements for Biobanking Activities Across Europe*, cit., p. 39.

trattamento dei dati sanitari a ipotesi non presenti laddove si sia svolta la raccolta dei dati, tale trattamento non potrà più ritenersi lecito con dirette ricadute in punto di utilizzo secondario dei dati e relativa presunzione di compatibilità. Ne conseguirà, in siffatti casi, il ripristino degli ordinari adempimenti dettati dal GDPR e duplicazione dei costi e degli oneri per il titolare. È questa una eventualità non solo teorica, come dimostrato dalla scelta adottata dal legislatore nazionale.

4. IL CONSENSO QUALE BASE GIURIDICA PER L'USO PRIMARIO E SECONDARIO DEI DATI PERSONALI: GLI ARTICOLI 110 E 110-BIS DEL CODICE PRIVACY.

Il legislatore italiano, sulla base dell'ampia delega prevista dal citato art. 9, par. 4 GDPR, ha introdotto, con la riforma del 2018, misure più restrittive rispetto a quanto previsto sia dalla previgente normativa nazionale⁶³ sia 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. Tale principio conosce solo due eccezioni.

⁶³ Il Codice Privacy, nella versione previgente all'entrata in vigore del citato d.lgs. 101/2018, prevedeva all'art. 110 che il consenso non fosse necessario nell'ipotesi di impossibilità di informare gli interessati e il programma di ricerca fosse stato oggetto tanto di motivato parere favorevole del competente comitato etico a livello territoriale quanto di autorizzazione del Garante, "anche ai sensi dell'articolo 40". Tale articolo 40, nello specifico, prevedeva la possibilità per il Garante di emettere un'autorizzazione generale riferibile a un'intera categoria di "titolari o di trattamenti". Sulla base di tale richiamo normativo, il Garante aveva emesso, con provvedimento n. 85 del 1° marzo 2012, la "Autorizzazione generale al trattamento di dati personali effettuato per scopi di ricerca scientifica", nella quale specificava che dato "l'elevato numero di trattamenti di dati idonei a rivelare lo stato di salute è effettuato da diversi titolari del trattamento per la conduzione di studi finalizzati alla ricerca scientifica in campo medico, biomedico o epidemiologico" era ritenuto "opportuno pertanto, alla luce dell'esperienza maturata, rilasciare un'autorizzazione generale, ai sensi dell'art. 40 del Codice". Difatti, precisava il provvedimento, "l'autorizzazione di carattere gene-

rale risulta uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati e rende superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento semplificando in tale modo, in maniera significativa, gli adempimenti degli obblighi relativi ai trattamenti di dati per la conduzione di ricerche mediche, biomediche o epidemiologiche". Sebbene l'autorizzazione generale fosse esplicitamente prevista ai sensi dell'art. 36, par. 5 GDPR e potesse ritenersi espressione del principio di responsabilizzazione sancito dall'art. 5, par. 2 GDPR, e nonostante lo stesso Garante ne avesse messo in rilievo l'utilità, in termini di semplificazione procedurale in capo al titolare, l'art. 9, co. 1, lett. b), del D.L. 8 ottobre 2021, n. 139 ha abrogato l'art. 2-*quinqüesdecies* del Codice Privacy che consentiva al Garante l'emissione di tali autorizzazioni generali. Ne consegue che il testo dell'attuale art. 110 limita l'intervento del Garante alla sola emissione di autorizzazioni caso per caso. Crf. D.L. 8 ottobre 2021, n. 139 « Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali », in *GURI* n. 241 del 8 ottobre 2021.

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. 502⁶⁴ oppure quelli previsti 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”. Il titolare deve, inoltre, dimostrare di aver adottato misure appropriate volte alla tutela dei diritti dell'interessato e aver sottoposto la sperimentazione al vaglio tanto del competente comitato etico a livello territoriale, quanto del Garante per la protezione dei dati personali, che sottoporrà al proprio controllo anche le ragioni che ostano al pieno espletamento degli obblighi informativi da parte del titolare⁶⁵.

Inoltre, occorre considerare che gli ulteriori trattamenti e conservazione dei dati personali per scopi di ricerca scientifica sono ammessi nei limiti posti non solo dal quadro normativo di riferimento, sia nazionale che europeo, ma anche dalle “Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica del 5 giugno 2019”⁶⁶ e dalle citate Regole deontologiche.

Le Prescrizioni prevedono, ad esempio, oneri aggiuntivi quali i “motivi di impossibilità organizzativa” che ostano a contattare gli interessati e la relativa dimostrazione che l'inutilizzabilità dei dati di coloro che non sono contattabili, rispetto al numero totale degli interessati, produrrebbe conseguenze significative per lo studio “in termini di alterazione dei relativi risultati”. Tale analisi

⁶⁴ D.lgs. n. 502/1992, recante « Riforma della disciplina in materia sanitaria, a norma dell'articolo 1 della legge 23 ottobre 1992, n. 421 », in *GURI* n. 305 del 30 dicembre 1992.

⁶⁵ L'art. 36 par. 1 GDPR prevede che l'obbligo di consultazione preventiva del Garante trova applicazione nei casi in cui l'esito della cd. valutazione d'impatto sul trattamento riporti un rischio elevato per i diritti e le libertà delle persone fisiche. Tuttavia, l'art. 36, par. 5 GDPR estende l'obbligo di consultazione preventiva anche “in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pub-

blica”. In siffatti casi, il titolare dovrà ottenere autorizzazione preliminare allo svolgimento del trattamento da parte dell'autorità di controllo. V. Garante per la protezione dei dati personali, Parere ai sensi dell'art. 110 del Codice e dell'art. 36 del Regolamento - 30 giugno 2022, doc. web 9791886; Provvedimenti n. 582 del 7 dicembre 2023, doc. web 9971457; n. 406 del 1° novembre 2021, doc. web 9731827; n. 202 del 29 ottobre 2020, doc. web 9517401.

⁶⁶ Garante per la protezione dei dati personali, Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101, in *GURI* n. 176 del 29 luglio 2019, doc. web 9124510.

dovrebbe altresì tener conto dei criteri di inclusione previsti dallo studio, delle modalità di arruolamento, della numerosità statistica del campione prescelto, nonché del periodo di tempo trascorso dalla raccolta dei dati ⁶⁷.

Le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, invece, prevedono l'obbligo di implementare idonee forme di pubblicità, quali l'inclusione dell'informativa sul sito internet del promotore e del centro clinico coinvolto, nel caso in cui la fornitura di una copia a ciascun interessato comporti "uno sforzo sproporzionato rispetto al diritto tutelato" ⁶⁸.

Una serie, quindi, di requisiti procedurali gravosi, che discendono dalla previsione del consenso quale unica base giuridica del trattamento dei dati personali per fini di ricerca scientifica, circostanza questa che rappresenta un *unicum* a livello dell'Unione europea ed ha esposto l'art. 110 a diverse critiche da parte sia della comunità scientifica ⁶⁹ sia degli operatori economici ⁷⁰.

Ancora più restrittiva, da un punto di vista sia pratico che procedurale, è la norma applicabile ai trattamenti dei dati personali svolti da terzi (ossia soggetti differenti rispetto a quello che ha redatto il protocollo di studio) per finalità ulteriori rispetto a quelle originariamente previste nel protocollo: l'articolo 110-bis, rubricato "Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici".

Dal punto di vista pratico, innanzitutto, il trattamento dei dati per finalità ulteriori rispetto a quelle che ne avevano contraddistinto la raccolta (svolta da un precedente titolare) tende, rispetto alle ipotesi di cui all'art. 110, a riguardare interessati non più in grado, per via delle loro condizioni cliniche, di comprendere il contenuto del consenso, oppure decedute o, ancora, non più reperibili, complice anche la distanza temporale e/o geografica tra la sperimentazione originaria e quella ulteriore. Da ciò consegue una elevata complessità, per il nuovo promotore, di riuscire a contattare gli interessati al fine di richiedere loro di prestare nuovamente il proprio consenso.

Dal punto di vista procedurale, invece, mentre le eccezioni all'utilizzo del consenso, quale base giuridica, ricalcano sostanzialmente quanto già previsto dall'art. 110, diverso risulta l'*iter* approvativo del trattamento dei dati ai fini di ricerca. Alla previa

⁶⁷ Ivi, par. 5.3.

⁶⁸ Regole deontologiche, cit., art. 6, co. 3.

⁶⁹ V. Centro di Coordinamento Nazionale dei Comitati Etici (CCNCE), Criticità etiche e normative nel trattamento dei dati personali sanitari nella ricerca osservazionale, 2023, disponibile online all'indirizzo

https://www.aifa.gov.it/documents/20142/1808580/Criticita_etiche_ricerca_osservazionale_06.04.2023.pdf..

⁷⁰ Farindustria, Position Paper Privacy e Sperimentazione Clinica, febbraio 2024, disponibile online all'indirizzo <https://www.farindustria.it/app/uploads/2024/04/Privacy-e-Sperimentazione-Clinica.pdf>.

consultazione del Garante ai sensi dell'art. 36 GDPR, disposta dal citato art. 110, si contrappone l'autorizzazione preventiva di cui all'art. 110-bis per gli utilizzi ulteriori dei dati da parte dei terzi⁷¹. Tale autorizzazione è ottenibile tramite decisione del Garante da adottarsi entro quarantacinque giorni dalla richiesta, decorsi i quali la mancata pronuncia equivale a rigetto.

5. CONCLUSIONE.

Come osservato, il tema dei trattamenti di dati personali nell'ambito della sperimentazione clinica può comportare l'emergere di istanze contrapposte, talora anche in conflitto tra loro.

Si tratta, in primo luogo, del complesso rapporto tra il diritto alla salute e il diritto alla protezione dei dati personali. Il primo è declinabile come il diritto del singolo a vedersi somministrati medicinali i cui profili di sicurezza ed affidabilità siano stati sufficientemente testati, e l'interesse della comunità all'implementazioni della ricerca scientifica, da considerarsi "bene comune", per i suoi effetti sul progresso e la conoscenza medico-scientifica. Dal secondo derivano, in favore dei partecipanti alle ricerche cliniche, le tutele in tema di trasparenza sull'utilizzo che si intenda fare dei loro dati personali, la necessità che il trattamento sia lecito nonché l'applicazione di misure di sicurezza volte a ridurre il rischio di utilizzi impropri dei dati.

Pertanto, i diritti in gioco nelle sperimentazioni cliniche, e i loro corollari, dovrebbero essere sottoposti ad un corretto processo di bilanciamento, a norma tanto del diritto nazionale quanto del diritto dell'Unione europea.

Sul piano nazionale emerge che i dati personali costituiscano una componente essenziale dell'identità dell'individuo e, per tale ragione, devono essere oggetto di una tutela rigorosa.

Il diritto alla riservatezza dei dati personali costituisce, infatti, una manifestazione del diritto fondamentale all'intangibilità della sfera privata, che attiene alla tutela della vita degli individui nei suoi molteplici aspetti e, per tale ragione, trova riferimenti nella Costituzione italiana (artt. 2, 14, 15 Cost.), e protezione, in relazione a differenti ambiti, nella giurisprudenza della Corte Costituzionale⁷².

Tale diritto, specifica la Corte Costituzionale, "si giova, a sua protezione, dei canoni elaborati in sede europea per valutare la legittimità della raccolta, del trattamento e della diffusione dei

⁷¹ Garante per la protezione dei dati personali, provvedimento n. 285 del 6 luglio 2023, cit.; v. S. MELCHIONNA, F. CECAMORE, *Le nuove frontiere della sanità e della ricerca scientifica*, in R. Panetta (a cura di) *Circolazione e protezione dei dati perso-*

nali, tra libertà e regole del mercato, cit., pp. 579 e ss.

⁷² Corte Costituzionale, sentenze n. 173 del 22 aprile 2009, ECLI:IT-COST:2009:173 e n. 135 del 11 aprile 2002, ECLI:IT-COST:2002:135.

dati personali”, quali i principi di proporzionalità, pertinenza e non eccedenza, secondo cui le deroghe e limitazioni alla tutela dei dati personali “devono operare nei limiti dello stretto necessario, essendo indispensabile identificare le misure che incidano nella minor misura possibile sul diritto fondamentale, pur contribuendo al raggiungimento dei legittimi obiettivi sottesi alla raccolta e al trattamento dei dati.”⁷³.

Nei suddetti termini, quindi, la tutela dei dati personali può essere sottoposta ad un esame di coerenza con altri diritti, di par rango⁷⁴. E tale scrutinio, precisa la Corte Costituzionale, “non deve essere effettuato in astratto, tra i valori in sé e per sé considerati, ma in concreto, valutando l’interazione reciproca tra l’accrescimento di tutela dell’uno e la corrispondente diminuzione di garanzia dell’altro, come disposti dal legislatore in vista della composizione del potenziale contrasto”⁷⁵.

A livello dell’UE, tale bilanciamento deve essere effettuato secondo quanto previsto dall’art. 52, par. 1 della Carta dei diritti fondamentali dell’Unione europea, che stabilisce la legittimità delle restrizioni all’esercizio dei diritti fondamentali, a condizione che esse siano: (i) stabilite per legge⁷⁶; (ii) rispettose del nucleo essenziale del diritto compresso⁷⁷; (iii) proporzionate⁷⁸; e (iv) necessarie e dirette a finalità di interesse generale riconosciute dall’UE o alla protezione dei diritti e libertà altrui⁷⁹.

Come precisato dalla Corte di giustizia dell’Unione europea, l’esito di siffatto esame potrà comportare la compressione della tutela dei dati personali, intesa nella sua dimensione individuale, in virtù della valorizzazione della sua funzione sociale, economica e di pubblica sicurezza⁸⁰.

Alla luce di quanto previsto sul piano nazionale e dell’UE, le menzionate misure di pseudonimizzazione costituiscono un utile strumento per garantire la privacy dei soggetti partecipanti alla sperimentazione e, contestualmente, per non comprimere ecces-

⁷³ Corte Costituzionale, sentenza n. 20 del 23 gennaio 2019, ECLI:IT:COST:2019:20.

⁷⁴ Cfr. F. Di Ciommo, *La privacy sanitaria*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, pp. 247 e ss.

⁷⁵ Corte Costituzionale, sentenza n. 372 del 6 novembre 2006, ECLI:IT:COST:2006:372, par. 5.2, in materia di bilanciamento tra il principio della tutela della riservatezza dei dati relativi alle comunicazioni telefoniche di cui all’art. 15 Cost. e l’interesse costituzionale della collettività alla repressione degli illeciti penali.

⁷⁶ Corte di giustizia dell’Unione europea, conclusioni dell’Avvocato generale Vilalón del 14 aprile 2011, *UPC Telekabel*,

causa C-70/10, ECLI:EU:C:2013:781, par. 100.

⁷⁷ Corte di giustizia dell’Unione europea, sentenza del 6 ottobre 2015, *Schrems I*, causa C-362/14, ECLI:EU:C:2015:650, par. 94.

⁷⁸ Corte di giustizia dell’Unione europea, sentenza del 24 novembre 2011, *ASNEF e FECMD*, cause riunite C-468 e 469/10, ECLI:EU:C:2011:777, par. 47.

⁷⁹ Corte di giustizia dell’Unione europea, sentenza del 16 dicembre 2008, *Satamedia*, causa C-73/07, ECLI:EU:C:2008:727.

⁸⁰ Corte di giustizia dell’Unione europea, sentenza del 9 novembre 2010, *Volker und Markus Schecke e Eifert*, cause riunite C-92/09 e C-93/09, ECLI:EU:C:2010:662, par. 48.

sivamente le possibilità di riutilizzo dei dati per ulteriori scopi clinici e di farmacovigilanza. Si tratterebbe pertanto di un esempio virtuoso di detto temperamento.

Di contro, sia l'interpretazione restrittiva del Garante per la protezione dei dati personali sulle tecniche di anonimizzazione dei dati adottata nel citato caso *Thin*, sia l'imposizione da parte del legislatore nazionale del consenso quale base giuridica preferenziale, paiono costituire un'indebita limitazione allo svolgimento della ricerca clinica. Sotto il primo profilo, il *test* sulla anonimizzazione dei dati, soprattutto quando riferiti ai *big data*, dovrebbe basarsi su criteri di sufficienza e ragionevolezza in luogo dell'appiattimento verso indici di assolutezza che ben poco si attagliano ad un contesto, quello tecnologico, in continua e rapida evoluzione. Sotto il secondo profilo, l'uso del consenso in via preferenziale non risulta, anzitutto, trovare riscontro nel GDPR, dove le citate tre basi giuridiche spendibili per trattamenti in ambito di ricerca clinica sono disposte sul medesimo livello di rilevanza. Inoltre, come rilevato, il consenso non sembra garantire sufficientemente la libertà di scelta dell'interessato, date le conseguenze, in termini di salute, di un suo eventuale rifiuto e risulta "squilibrato" se osservato dal punto di vista, in particolare, dell'asimmetria informativa tra il paziente e il promotore della ricerca clinica. Infine, gli artt. 110 e 110-*bis* devono leggersi all'interno della più ampia cornice del diritto dell'Unione europea, segnatamente, del GDPR. Sul punto si è recentemente espressa la Corte di Giustizia dell'Unione europea, con la sentenza *ZQ*⁸¹. Nell'ambito del rinvio pregiudiziale avente ad oggetto l'interpretazione della normativa tedesca sul trattamento dei dati personali particolari svolto da un organismo di controllo medico in qualità non di datore di lavoro, bensì di servizio medico, nei confronti di un proprio dipendente, al fine di valutarne la capacità lavorativa, la Corte si è espressa sugli spazi di libertà concessi dall'art. 9, par. 4 GDPR agli Stati membri. A tal proposito, i Giudici del Lussemburgo hanno 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 non paiono del

⁸¹ Corte di giustizia dell'Unione europea, sentenza del 21 dicembre 2023, *ZQ*,

causa C-667/21, ECLI:EU:C:2023:1022, par. 67.

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.

Un ulteriore contrasto potrebbe svolgersi, invece, tra gli obiettivi principali del GDPR stesso: il contemperamento del diritto alla protezione dei dati personali e l'implementazione della libera circolazione di tali dati, nell'ambito delle sperimentazioni cliniche, pare distante dal trovare una composizione accurata, nonostante l'ambito della ricerca scientifica rientrasse fra quelli ritenuti maggiormente oggetto dell'intervento uniformatore operato proprio attraverso il GDPR. Mentre, quindi, la tutela rafforzata del trattamento dei dati sulla salute sembra costituire una misura ragionevole per la protezione del diritto alla vita privata, le osservate discrepanze tra le discipline nazionali, sotto il profilo delle condizioni di liceità, costituiscono una limitazione alla libera circolazione e all'utilizzo di tali dati che non pare giustificabile alla luce delle norme dei Trattati e in base allo spirito del GDPR stesso.

A tal proposito, l'art. 1, par. 3 del GDPR stabilisce infatti un divieto di limitare la libera circolazione dei dati personali nell'Unione "per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali". Tali limitazioni, a fronte della concezione dei dati personali quali beni di natura economica e del conseguente loro impatto sul mercato unico (digitale) di cui agli artt. 4, par. 2, lett. a), 26, 27, 114 e 115 del trattato sul funzionamento dell'Unione europea (TFUE) e sull'esercizio delle relative libertà fondamentali⁸², possono fondarsi sui motivi di motivi di ordine pubblico, di pubblica sicurezza e di sanità pubblica, da applicarsi alla luce del principio di proporzionalità e della costante giurisprudenza della Corte di Giustizia dell'Unione europea⁸³. Motivi, questi, che non paiono ricorrere nell'ambito della suddetta restrizione alla circolazione dei dati sulla salute trattati al fine di condurre le sperimentazioni cliniche.

Inoltre, le accentuate discrepanze tra le normative nazionali sul trattamento dei dati sulla salute paiono contraddire uno degli

⁸² V. ZENO-ZENCOVICI, *Do "data markets" exist?*, in *MediaLaws*, 2019, pp. 1 e ss.; G. DI LORENZO, *La circolazione dei dati personali tra tutela della persona e ordine giuridico del mercato*, in *Federalismi.it*, 2019, p. 2; F. BRAVO, *Il "diritto" a trattare i dati personali nello svolgimento dell'attività economica*, Padova, 2018, p. 12.

⁸³ G. CACCIGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza*

in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione, in *Medialaws*, 2018, p. 64; F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal Safe Harbour al Privacy Shield)*, in *Rivista di diritto internazionale*, 2016, p. 690.

obiettivi principali del GDPR stesso, secondo cui, infatti, “(a) fine di (...) rimuovere gli ostacoli alla circolazione dei dati personali all’interno dell’Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri”⁸⁴. Nello stesso senso, anche gli osservati spazi di libertà, in capo agli Stati membri, sul mantenimento o introduzione di ulteriori condizioni, anche limitative, al trattamento dei dati relativi alla salute, non devono “ostacolare la libera circolazione dei dati personali all’interno dell’Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi”⁸⁵.

Infine, una seconda criticità pare caratterizzare il GDPR: l’equiparazione della ricerca scientifica alle differenti — dal punto di vista ontologico — fattispecie degli studi storici, statistici, o di archivio. Se, infatti, queste ultime si fondano sul trattamento di dati in chiaro e statici, diversamente, la ricerca scientifica, segnatamente quella clinica, adopera dati codificati o anonimizzati in continuo mutamento, con scarsa attrattività, per via della normativa di settore, per la re-identificazione dei pazienti. Ne consegue che una lettura eccessivamente uniforme di tali fattispecie ne rischia di mortificare le differenze di contesto nel quale operano, comportando difficoltà nello svolgimento di sperimentazioni che assumono un significato esiziale per la piena applicazione del diritto alla salute *ex artt.* 32 Cost. e 35 della Carta dei diritti fondamentali, sotto il profilo dell’accessibilità a farmaci innovativi.

In conclusione, il pianificato intervento ermeneutico dell’EDPB sul tema delle sperimentazioni cliniche, sia le recenti proposte di regolamento sull’intelligenza artificiale⁸⁶ e, soprattutto, sul citato spazio europeo dei dati sanitari potranno costituire un utile strumento per dare risposte adeguate alle suddette criticità, a condizione che tengano sufficientemente da conto il carattere non assoluto del diritto alla protezione dei dati personali che deve essere temperato con l’applicazione di altri diritti fondamentali, in ossequio ai principi delineati dalla giurisprudenza della Corte di Giustizia dell’Unione europea.

Nelle more dell’adozione di tali atti, nel contesto nazionale parrebbe necessaria la rilettura della nozione di anonimizzazione, a mente dei più recenti sviluppi interpretativi, nonché il riferimento alle istanze dei promotori della ricerca clinica, privati e

⁸⁴ Considerando n. 10, GDPR.

⁸⁵ *Ivi*, considerando n. 53.

⁸⁶ Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate

sull’intelligenza artificiale (legge sull’intelligenza artificiale) e modifica alcuni atti legislativi dell’Unione, 21 aprile 2021, COM(2021) 206 def.

pubblici, al fine di riformulare i presupposti di liceità dei trattamenti di dati personali ora previsti dagli artt. 110 e 110-bis.

Abstract

This article examines the use of health data in the context of clinical trials under EU and national regulatory frameworks. Specifically, an analysis of Regulation (EU) 536/2014 on clinical trials, data protection legislation, as well as recent interventions by the Data Protection Supervisor and EU case law, shows that the current regulatory framework is not fully adequate to allow for a proper balance between the development of safe and effective medicines, a corollary of the right to health, and the protection of personal data, as enshrined in Articles 35 and 8 of the EU Charter of Fundamental Rights, respectively. In particular, data pseudonymization, data subject consent as a legal basis for processing, and so-called secondary use are the most critical issues.