La condivisione dei dati nei dispositivi medici connessi (IoMT): tra il Data Act e lo Spazio europeo sui dati sanitari

Francesca Gennari, Federica Casarosa*

DATA SHARING IN INTERNET OF MEDICAL THINGS: BETWEEN THE DATA ACT AND THE EUROPEAN HEALTH DATA SPACE

ABSTRACT: National healthcare systems are increasingly exploiting the benefits of Internet of Things technologies: cloud-connected devices equipped with perceptual sensors can collect highly accurate health data from people even if they do not visit a hospital or private clinic. For potential innovators of new IoT medical devices, the applicable legal framework was so far limited to the application of the General Data Protection Regulation and the Medical Devices Regulation. This article will analyse what will happen when medical data generated by the IoT is shared to create new products or services under the framework now described by the Data Act (DA) and the European Health Data Space (EHDS). As the EHDS and the Data Act both aim at facilitating the secondary use of (health) data, the contribution will compare the two processes established to establish a roadmap for solving the theoretical and practical issues related to health data sharing.

KEYWORDS: access to data; data sharing contracts; Internet of Medical Things; secondary use of data

ABSTRACT: I sistemi sanitari nazionali stanno sfruttando sempre più i vantaggi delle tecnologie dell'Internet of Things: i dispositivi connessi al cloud e dotati di sensori percettivi possono raccogliere dati sanitari molto accurati dalle persone anche se non si recano in ospedale o in cliniche private. Per i potenziali innovatori di nuovi dispositivi medici IoT, il quadro giuridico applicabile era finora limitato all'applicazione del Regolamento generale sulla protezione dei dati personali e del Regolamento sui dispositivi medici. Questo articolo analizzerà cosa accadrà quando i dati medici generati dall'IoT saranno condivisi per creare nuovi prodotti o servizi secondo il quadro ora descritto

* *Francesca Gennari, PhD, Tecnologa di Ricerca presso Sant'Anna, Scuola Superiore Universitaria Pisa, Francesca.Gennari@santannapisa.it. Federica Casarosa, PhD, Tecnologa di Ricerca presso Sant'Anna, Scuola Superiore Universitaria Pisa- Assistant Professor presso l'Istituto Europeo di Firenze- EUI, Federica.Casarosa@santannapisa.it.* *Le autrici hanno in egual misura contribuito alla ideazione del presente contributo; tuttavia, la stesura dei paragrafi 2.2.1 e 3 a F. Gennari, dei paragrafi 2.1, 2.2 e 4 a F. Casarosa, i paragrafi 1 e 5 sono di comune redazione.*
La ricerca svolta da Francesca Gennari è stata finanziata dal progetto BRIEF "Biorobotics Research and Innovation Engineering Facilities "IR0000036" – CUP J13C22000400007. La ricerca di Federica Casarosa è stata svolta nell'ambito del progetto PNRR "SoBigData.it: Strengthening the Italian RI for Social Mining and Big Data Analytics. Contributo sottoposto a doppio referaggio anonimo.

ISSN 2284-4503

dal Data Act (DA) e dallo Spazio europeo dei dati sanitari (EHDS) con particolare riguardo all'Italia. Dato che l'EHDS e il Data Act mirano entrambi a facilitare l'uso secondario dei dati (sanitari), il contributo confronterà i due processi istituiti per stabilire una tabella di marcia per risolvere le questioni teoriche e pratiche relative alla condivisione dei dati sanitari e quali sfide aspettano il legislatore nazionale nella loro applicazione al sistema italiano.

KEYWORDS: Accesso ai dati; contratti di condivisione dei dati; Internet of Medical Things; uso secondario dei dati sanitari

1. Introduzione

Internet of Things (IoT) è la terminologia utilizzata per descrivere un ecosistema di oggetti e dispositivi in grado di raccogliere informazioni sull'ambiente circostante tramite sensori. Questa tecnologia può essere applicata in molti settori, poiché può adattarsi a diversi tipi di strumenti e applicazioni. L'esempio più semplice è quello degli oggetti domotici o smart installati in una casa connessa: dal frigorifero smart all'illuminazione intelligente, i dispositivi sono tutti connessi a Internet e possono raccogliere informazioni dall'utente e reagire a richieste specifiche[1]. Un settore in cui l'IoT è sempre più presente è quello afferente alla salute: i dispositivi indossabili (*wearables*) o impiantabili raccolgono informazioni sulle condizioni di salute dei pazienti, permettono ai medici (o agli ospedali) di personalizzare i servizi medici e di reagire tempestivamente alle emergenze[2]. Chiameremo per facilità le applicazioni della tecnologia IoT applicate al settore medico Internet of Medical Things (IoMT). La pandemia Covid è stata un fattore scatenante per l'aumento dell'uso di queste tecnologie, per evitare il contatto diretto tra pazienti e medici senza ridurre la possibilità di fornire le cure mediche necessarie[3]. Di conseguenza, l'uso dell'IoMT può anche aumentare l'efficienza del sistema, in quanto riduce i costi dei controlli non necessari, dato che il paziente è costantemente monitorato.

[1] L. VIZZONI, *Domotica e diritto. Problemi giuridici della smart home tra tutele e responsabilità*, Milano, 2021; J. CHEN ET AL., *Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption* in *International Data Privacy Law*, 2020, 10, 279.

[2] J. CHANCHAICHUJIT ET AL., *Healthcare 4.0: Next Generation Processes with the Latest Technologies*, Singapore, 24, 2019, http://link.springer.com/10.1007/978-981-13-8114-0 (ultima consultazione 10/01/2025); A. CHACKO, T. HAYAJNEH, *Security and Privacy Issues with iot in Healthcare*, in *Endorsed Transactions on Pervasive Health and Technology*, 2018, 4 EAI 1.

[3] M. KAMAL, A. ALJOHANI, E. ALANAZI, *iot Meets COVID-19: Status, Challenges, and Opportunities*, in *arxiv*, 28 giugno 2020, http://arxiv.org/abs/2007.12268, (ultima consultazione 10/01/2025).

ISSN 2284-4503

La pandemia Covid ha anche evidenziato il fatto che i dati sanitari possono essere preziosi per le attività di ricerca scientifica: grazie ai dati clinici e immunologici raccolti da pazienti già colpiti e sopravvissuti alla malattia, è stato possibile comprendere il virus e la sua struttura e prevedere quali dei suoi componenti avrebbero provocato una risposta immunitaria[4]. Questo è stato un passo fondamentale nella progettazione del vaccino e ha permesso ai team di ricerca di tutto il mondo di accumulare le conoscenze necessarie per produrre un vaccino efficace.

L'IoMT può svolgere un ruolo importante nella raccolta di dati che possono essere successivamente utilizzati per attività di ricerca simili. Tuttavia, i dati raccolti dai dispositivi IoMT possono essere qualificati come dati personali quando sono relativi a elementi che caratterizzano un individuo identificato o identificabile, oppure come dati non personali quando tale caratterizzazione manca. In entrambi i casi, si applicano norme specifiche che regolano tutte le fasi relative al trattamento (primario) dei dati: raccolta, conservazione ed elaborazione, imponendo forti garanzie ogni volta che il trattamento si concentra sui dati personali. Fino a poco tempo fa, la possibilità di un uso successivo dei dati personali non era ritenuta praticabile se non in circostanze specifiche, come per scopi di ricerca o per interesse pubblico in materia di sanità pubblica. Tuttavia, due recenti legislazioni europee hanno segnato un passo fondamentale nella regolamentazione dell'uso secondario dei dati personali, individuando le condizioni che possono consentire agli utenti di sfruttare tali dati per creare nuovi prodotti o servizi. Da un lato, il Data Act (DA)[5] identifica il quadro generale per l'uso secondario dei dati, includendo anche i casi in cui un fabbricante di IoT svolge il ruolo di cosiddetto titolare dei dati. Dall'altro lato, il Regolamento sullo Spazio Europeo dei Dati Sanitari (European Health Data Space, EHDS)[6] prevede norme specifiche per l'uso secondario dei dati sanitari, offrendo un'alternativa alla procedura applicabile secondo il Data Act. In entrambi i casi, il riferimento di base per i due atti legislativi è il quadro fornito dal Regolamento generale sulla protezione dei dati (General Data Protection Regulation, GDPR)[7]; tuttavia, l'interazione tra di essi non è chiara. Vi sono questioni interconnesse che emergono nell'insieme delle legislazioni, come l'incoerenza della terminologia utilizzata e la complessità generale dell'applicazione, nonché

[4] H. DÖGG GUNNARSDÓTTIR ET AL., *The Ethics and Laws of Medical Big Data* in M. IENCA e altri (a cura di), *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights*, Cambridge, 2022 https://www.cambridge.org/core/product/identifier/9781108775038%23CN-bp-4/type/book_part, (ultima consultazione 10/01/2025).

[5] Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati) (Testo rilevante ai fini del SEE).
PE/49/2023/REV/1, GU L, 2023/2854, 22.12.2023.

[6] Proposta di regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari, COM(2022) 197 definitivo. Il documento è stato adottato dal Parlamento europeo il 24 aprile 2024, ma attende ancora l'approvazione del Consiglio. L'analisi fornita in questo contributo si basa sull'ultima versione della proposta, disponibile all'indirizzo https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ43/AG/2024/04-09/1299790EN.pdf. [il testo finale del regolamento è al momento in lingua inglese. L'attuale traduzione è ad opera delle autrici].

[7] 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) (Testo rilevante ai fini del SEE), GU L 119 del 4.5.2016, pagg. 1–88.

questioni intra-correlate che riguardano gli incentivi economici per gli attori del mercato a sfruttare il percorso fornito da ciascun atto legislativo.
Il presente contributo affronterà questi temi, iniziando con l'identificazione della legislazione vigente applicabile all'IoMT, guardando al GDPR e al Regolamento sui dispositivi medici (Medical Devices Regulation, MDR)[8] (sez. 2). Verrà poi presentato il caso specifico dell'uso secondario dei dati, confrontando le regole del DA (sez. 3) con quelle dell'EHDS (sez. 4). Nelle conclusioni verrà presentata una valutazione delle soluzioni più adatte dal punto di vista del fabbricante di un nuovo strumento IoMT.

2. IoMT nella legislazione vigente

2.1 Il contesto del GDPR

La raccolta di dati personali effettuata da qualsiasi prodotto connesso o IoT è soggetta alle norme previste dal GDPR, che individua un quadro orizzontale applicabile al trattamento dei dati con particolare attenzione ai dati sanitari[9].
Il GDPR è applicabile a qualsiasi operazione o insieme di operazioni eseguite manualmente o con mezzi automatizzati su dati personali (art. 4 (2) GDPR). Secondo la definizione fornita dal GDPR, i dati personali comprendono qualsiasi informazione relativa a una persona fisica identificata o identificabile. Pertanto, i dati personali possono essere informazioni oggettive, come le caratteristiche dell'individuo, che raramente cambiano (ad esempio, il colore degli occhi o il luogo di nascita), e informazioni soggettive, come opinioni o valutazioni. Il GDPR non distingue tra dati oggettivi e soggettivi, ma piuttosto tra dati generici e categorie speciali di dati personali. La seconda categoria comprende i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, e il trattamento di dati genetici, dati biometrici, dati relativi alla salute, ecc. In quest'ultimo caso, al trattamento dei dati si applicano regole più severe. Sebbene l'art. 4(15) GDPR fornisca una definizione di dati sanitari, la terminologia utilizzata non è chiara, in quanto i dati relativi alla salute (per semplicità verranno definiti in questo contributo come dati sanitari) sono «dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute». Questa definizione, quasi

[8] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance). OJ L 117, 5.5.2017, pagg. 1–175.
[9] La letteratura sul GDPR è estremamente vasta, l'analisi più completa si trova in L. FEILER, N. FORGÓ, M. WEIGL, *The EU General Data Protection Regulation (GDPR): A Commentary (2° ed.)*, Globe Law and Business, Woking (UK), 2018; I. SPIECKER GENANNT DÖHMANN ET AL., *General Data Protection Regulation: Article-by-Article Commentary*, München, 2023; P. VOIGT, *The EU General Data Protection Regulation (GDPR) A Practical Guide*, (2° ed.), Cham, 2024; I. KAMARA, E. KOSTA E R. LEENES (eds.), *Research Handbook on EU Data Protection Law*, Cheltenham (UK), 2022; G. FINOCCHIARO, A. AVITABILE (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; G. COMANDÉ, G. MALGIERI, *Guida al trattamento e alla sicurezza dei dati personali: le opportunità e le sfide del regolamento UE e del Codice italiano riformato*, Gruppo 24 ore, Milano, 2019.

tautologica[10], può portare a un'interpretazione estremamente ampia che può comprendere anche altri dati personali che alludono indirettamente alle condizioni di salute dell'interessato[11].

Il trattamento dei dati personali che riguardano la salute svolto da un IoMT è pertanto soggetto ai requisiti più severi imposti dall'art. 9 GDPR[12]. Il trattamento dei dati sulla salute è vietato ad eccezione di una serie di casi giuridici specifici, quali il consenso specifico espresso dell'interessato, i dati resi manifestamente pubblici dall'interessato, il trattamento dei dati finalizzato alla prevenzione o alla medicina del lavoro e anche il trattamento dei dati per motivi di interesse pubblico nel settore della sanità pubblica[13]. Queste eccezioni sono fondamentali per l'uso secondario dei dati sanitari, come verrà chiarito nella sezione dedicata all'EDHS[14].

Ai fini di comparazione fra le più recenti normative del Data Act e dell'EHDS, è utile delineare i soggetti coinvolti nel trattamento dei dati personali effettuato da un prodotto connesso, lasciando tuttavia a più specifica letteratura l'analisi dettagliata del quadro normativo del GDPR. Nello caso concreto della raccolta di dati sanitari da un prodotto connesso, dunque, possiamo distinguere tre tipi di attori che sono in grado di raccogliere e trattare i dati personali dell'interessato, ovvero il titolare del trattamento, il responsabile del trattamento e il destinatario dei dati.

L'art. 4(7) GDPR descrive il 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». Dato il ruolo cruciale svolto dal titolare del trattamento nel trattamento, il GDPR adotta un approccio pratico per identificare chi sovrintende a questo ruolo, esaminando gli elementi di fatto o le circostanze di un caso, indipendentemente da qualsiasi dichiarazione formale[15]. Il titolare del trattamento è il soggetto che decide le finalità del trattamento e i mezzi per effettuarlo: il tipo di dati raccolti, la durata del trattamento, i destinatari dei dati e i mezzi tecnici per trattare i dati. Va sottolineato che il titolare del trattamento non è obbligato a controllare fisicamente o direttamente i mezzi; è possibile che l'hardware o il software che raccoglie i dati personali sia affidato a terzi (appunto il responsabile del trattamento). Questo è rilevante nel caso dell'IoMT; ad esempio, l'azienda che produce il software incorporato in un dispositivo che monitora i livelli di zucchero nel sangue per i pazienti affetti da diabete può essere qualificata come titolare del trattamento dei dati, in quanto elabora i dati sanitari al fine di fornire un allarme in caso di aumento del livello di zucchero nel sangue. Tuttavia, la raccolta dei dati può avvenire grazie a sensori che raccolgono i *raw data*, cioè

[10] M. TZANOU (a cura di), *Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses*, Londra, 2021, 6.

[11] Per un approccio alla definizione di dati sanitari basato sul rischio, cfr. W. SCHÄFKE-ZELL, *Revisiting the Definition of Health Data in the Age of Digitalized Health Care*, in *International Data Privacy Law*, 12, 2022, 33.

[12] Si veda la definizione di dati sulla salute di cui all'art. 4(15) del GDPR. 4(15) GDPR. Si noti che la letteratura accademica ha evidenziato la mancanza di chiarezza di questa definizione. M. TZANOU, *op. cit.*; T. MULDER, *The Protection of Data Concerning Health in Europe*, in *European Data Protection Law Review*, 5, 2019, 209.

[13] Si veda l'art. 9 (2) che elenca dieci categorie di esenzioni. 9 (2) elenca dieci categorie di esenzioni.

[14] Si veda *infra* sez. 4.

[15] EDPB, Linee guida 07/2020 sui concetti di titolare del trattamento e responsabile del trattamento nel GDPR, 7 luglio 2021, disponibili all'indirizzo https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf, pag. 13 (ultima consultazione 10/01/2025).

dati non ancora processati (per esempio se vi è un'anomalia del battito cardiaco) dal corpo dell'interessato; tali sensori possono far parte di un dispositivo multifunzione (smart) che raccoglie dati condivisi con più di un software.

Il responsabile del trattamento, ai sensi dell'art. 4(8) GDPR è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento». I responsabili del trattamento possono essere più di uno e occuparsi di diverse fasi del trattamento. Anche in questo caso, le circostanze di fatto e le attività concrete sono fondamentali per identificare se la qualifica di responsabile del trattamento è corretta. Ad esempio, il servizio fornito potrebbe non essere finalizzato al trattamento dei dati personali o non costituire un elemento chiave del servizio: in questi casi, il fornitore del servizio non può qualificarsi come responsabile del trattamento, ma piuttosto come titolare del trattamento. Una situazione diversa può emergere quando il responsabile del trattamento decide di effettuare un trattamento aggiuntivo per le proprie finalità con i dati raccolti; in questo caso, la qualifica è corretta in quanto il responsabile era sotto il controllo diretto o l'autorità del titolare del trattamento, ma il trattamento aggiuntivo porta a una violazione dell'art. 28(10) GDPR. Il ruolo del titolare e del responsabile del trattamento devono essere chiaramente identificati nell'accordo con il responsabile, dove vengono presentati i servizi offerti da quest'ultimo e l'approvazione finale del titolare del trattamento che consente l'adozione di tali servizi nel trattamento dei dati. Ad esempio, se l'IoMT è un dispositivo intelligente con una memoria interna limitata, può utilizzare i servizi di un provider di archiviazione cloud. Il fabbricante del dispositivo svolgerà il ruolo di titolare del trattamento, data la sua decisione di utilizzare questo particolare fornitore di servizi cloud per trattare i dati personali per i suoi scopi[16].

L' Art. 4(9) GDPR aggiunge un altro attore che può svolgere un ruolo importante nel trattamento dei dati, vale a dire il destinatario dei dati, che è definito come «la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi». In linea di principio, il destinatario dei dati non ha obblighi o responsabilità relativamente al trattamento dei dati esistente. Tuttavia, può diventare un nuovo titolare o responsabile del trattamento una volta ricevuti i dati. Ad esempio, quando un titolare del trattamento invia dati personali a un'altra entità, quest'ultima viene qualificata come destinatario. Tale invio può essere giustificato da diversi motivi: condivisione, trasmissione o divulgazione dei dati. Ad esempio, il fabbricante di IoT può condividere i dati elaborati ad altre società per scopi pubblicitari.

2.2.1. Uso primario e secondario dei dati sanitari. Le nuove regole del Codice della Privacy italiano

Secondo il lessico della protezione dei dati personali, i dati possono essere assoggettati a diversi usi e questo tema è cruciale per i dati sanitari e la ricerca e sviluppo biomedica. L'uso primario dei dati personali riguarda l'uso per il quale i dati vengono raccolti. Nel caso dei dati sanitari, l'uso primario è

[16] Si noti che l'EDPB chiarisce che la presenza (o l'assenza) di un accordo scritto, tuttavia, non è decisiva per l'esistenza di una relazione tra responsabile del trattamento e incaricato, poiché anche in assenza di un accordo scritto sul trattamento, la relazione può emergere dalle circostanze di fatto del caso. Tuttavia, l'assenza di una chiara definizione del rapporto tra il responsabile del trattamento e l'incaricato del trattamento può sollevare il problema della mancanza di una base giuridica su cui fondare ogni trattamento, ad esempio per quanto riguarda la comunicazione dei dati tra il responsabile del trattamento e il presunto incaricato del trattamento. Si veda EDPB (n 10), 32.

molto spesso legato alle funzioni di cura, diagnosi, terapia e riabilitazione che la struttura di cura, pubblica o privata, offre e che vengono dettagliati nell'informativa sulla privacy di cui ogni paziente deve prendere visione, comprendere e sottoscrivere. Di regola, all'interno di questo documento devono essere elencati anche quelli che sono considerati gli usi secondari dei dati personali raccolti. Questi usi secondari, nell'ambito medico, sono legati alla possibilità di utilizzare i dati raccolti ai fini di cura per studi clinici (retrospettivi o meno, *in silico*, *dry or wet*, randomizzati o con uso di *real world data*)[17] ottenuti da referti e cartelle cliniche dei pazienti e che fanno progredire la ricerca biomedica e scientifica. Nonostante il GDPR non usi la terminologia di uso primario o secondario dei dati adotta comunque un favor[18] nei confronti della ricerca scientifica: alla base del GDPR, infatti, non vi è solo la ratio di protezione della privacy ma anche della diffusione e uso dei dati anche personali a beneficio della società. Questo si desume anche leggendo il combinato disposto degli Articoli 9(2)(j) e 89 GDPR. Il primo stabilisce l'eccezione al generale divieto di trattamento dei dati personali particolari, elencati all'Articolo 9(1) di cui i dati relativi alla salute, insieme a quelli genetici e biometrici e che ai fini di questo contributo rilevano maggiormente. La lettera (j) del secondo paragrafo dell'Art. 9 GDPR, infatti, ammette il trattamento dei dati personali per «[…] 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 misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato». L'Articolo 89, invece richiede che, per contemperare e rispettare al diritto alla privacy e riservatezza, debbano essere rispettate determinate categorie e deroghe comprendenti misure tecnico organizzative finalizzate in particolare al rispetto del principio di minimizzazione dei dati[19].

Nonostante questa formulazione, le regole riguardanti l'uso e il riuso dei dati sanitari nella ricerca biomedica e scientifica sono state interpretate in maniera restrittiva sia dallo European Data Protection Body (EDPB) che dalle autorità nazionali[20]. In particolare, in Italia è stato ed è ancora il consenso la base giuridica preferenziale per il trattamento dei dati sanitari sia per uso primario che secondario[21]. A sostegno di questa posizione, il Garante della Protezione per i Dati Personali ha stabilito che i modelli

[17] P. AURUCCI, *Il trattamento dei dati personali nella ricerca biomedica. Problematiche Etico-Giuridiche*, Torino-Napoli, 2022, 1-13

[18] P. GUARDA, G. BINCOLETTO, *Diritto comparato della privacy e della protezione dei dati personali*, Milano, 2023, 317-331.

[19] Sull'applicazione dell'articolo 89 nella ricerca biomedica si veda in particolare C. STAUNTON, S. SLOKENBERGA, A. PARZIALE E D. MASCALZONI*, Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research* in *Frontiers in Genetics* 13, 2022, https://doi.org/10.3389/fgene.2022.719317.

[20] Documento del Comitato europeo per la protezione dei dati sulla risposta alla domanda di chiarimenti della Commissione europea in merito all'applicazione coerente del GDPR, con un'attenzione particolare alla ricerca in campo sanitario, 2 febbraio 2021, https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/edpb-document-response-request-european-commission_it (ultima consultazione 10/01/2025). Per l'Italia, si veda 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 [9124510], in particolare l'Allegato n.1 , 5, Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. Gen. 9/2016), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124510#5 (ultima consultazione 10/01/2025).

[21] In questo caso si prende il combinato disposto Artt. 6(1)(a) e 9(2)(a) GDPR.

di informativa sulla privacy che i pazienti devono firmare non possono essere generali, perché questo potrebbe permettere al titolare dei dati di bypassare il ricontatto del paziente[22]. Idealmente, tutti i trattamenti presenti e futuri devono essere descritti in maniera il più possibile puntuale anche nel rispetto delle caratteristiche del consenso informato elencate all'Art. 7 GDPR. Questo pone non pochi problemi per trovare una base giuridica idonea anche solo per il ricontatto dei pazienti[23]. Per quanto riguarda l'Italia, gli Articoli 110 e 110 bis del codice privacy insieme alle linee guida deontologiche hanno improntato la prassi dei ricercatori, qualora non sia possibile il ricontatto del paziente (perché deceduto o perché si potessero ricordare esperienze traumatiche e dolorose). Il problema generato dalla precedente formulazione dell'Art. 110 Cod. Privacy era relativo alla necessità di richiedere un'autorizzazione preventiva *ex* art. 36 GDPR all'autorità garante[24] qualora non fosse possibile il ricontatto del paziente (per i motivi sopra elencati e documentando tali tentativi[25]). Questo procedimento aveva l'effetto di rallentare gli studi specifici (molto frequentemente retrospettivi) spesso finanziati e inclusi in programmi dell'UE e dal ministero competente italiano e sottoposti a scadenze non facilmente prorogabili.

Tuttavia, nel 2024 la modifica agli artt. 110 e 110 bis del codice privacy ha portato ad uno snellimento della procedura. La legge n. 19/2024 ha emendato gli articoli ed ha aggiunto ulteriori ipotesi di giustificazione laddove sia assente il consenso del paziente ottenuto tramite un successivo contatto. La prima ipotesi in cui richiedere il consenso non sia necessario si configura quando la ricerca sia basata su norme nazionali o UE come stabilito dal combinato disposto Artt. 9(2)(j) e 89 GDPR. La seconda ipotesi riguarda invece «particolari ragioni» per cui informare gli interessati sia i) impossibile, ii) sproporzionato o iii) rischia di pregiudicare l'ottenimento della finalità di ricerca. Nella prima ipotesi deve dunque essere presente una norma di diritto nazionale o dell'UE che giustifica il trattamento e l'uso secondario dei dati sanitari per finalità di ricerca scientifica a condizione che venga redatta una valutazione d'impatto (Data Protection Impact Assessment, DPIA) ai sensi dell'Art. 35[26]. Nella seconda ipotesi, invece, i comitati etici territoriali devono accertare che le motivazioni offerte dagli sponsor degli studi clinici a causa delle quali non sia possibile ottenere il consenso dei pazienti siano sufficientemente giustificate e che la valutazione d'impatto *ex* Art. 35 GDPR sia rispondente ai reali rischi e misure di protezione adottate nei confronti dei dati personali degli interessati. Per quanto riguarda le particolari circostanze in cui non sia possibile ottenere il consenso del paziente di cui al secondo paragrafo del

[22] Garante per la protezione dei dati personali, Parere ai sensi dell'art.110 del Codice e dell'art 36 del regolamento – 30 giugno 2022 [9791886], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9791886 (ultima consultazione 10/01/2025).

[23] Le strutture cliniche private potevano fare leva sull'interesse legittimo, mentre invece le strutture pubbliche un compito di interesse pubblico come la ricerca scientifica solo sulla base dell'articolo 6 ma non dell'articolo 9 GDPR. Diventava quindi molto difficile, anche cambiando il documento da sottoscrivere per la privacy, trovare un modo corretto e legale di ricontattare pazienti che magari avevano avuto un trattamento anni prima sulla base di una informativa privacy incompleta o scorretta (nel peggiore dei casi).

[24] Testo Articolo 110 Codice Privacy ante novella.

[25] I tentativi dovevano essere nel numero di tre.

[26] In questa rivista è stato spiegato in dettaglio quali siano le garanzie offerte dai programmi di ricerca europei e nazionali. P. AURUCCI, F. DI TANO, *Dati personali e ricerca medica: condizioni, incoerenze e prospettive giuridiche a fronte dell'evoluzione interpretativa e applicativa del Garante per la protezione dei dati personali* in *Biolaw Journal – Rivista di biodiritto*, 3, 2024, 318-324.

ISSN 2284-4503

novellato Art. 110 Codice Privacy, in data 9 maggio 2024 il Garante Privacy ha pubblicato una serie aggiornata di garanzie da osservare *ex* art 2 quater e 106 del Codice Privacy in virtù della novella legislativa degli articoli 110 e 110 bis[27]. In questa si chiariscono come e quali siano le giustificazioni accettabili dai comitati etici per pazienti deceduti o non facilmente contattabili. I motivi etici utilizzabili sono quelli per cui il ricontatto farebbe riemergere ricordi traumatici e dolorosi; le ragioni tecniche e organizzative invece devono illustrare che la mancata raccolta dei dati riferiti al numero di interessati che non è possibile contattare, rispetto al numero complessivo dei soggetti che si intende arruolare nella ricerca, produrrebbe conseguenze significative per lo studio in termini di qualità dei risultati della ricerca stessa; ciò avuto riguardo, in particolare, a) ai criteri di inclusione previsti dallo studio, b) alle modalità di arruolamento, c) alla numerosità statistica del campione prescelto, d) nonché al periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti. Il fatto che contattare i pazienti implichi uno sforzo sproporzionato è una motivazione con carattere residuale, sia nel caso in cui all'esito di ogni ragionevole sforzo compiuto per contattarli[28] essi risultino al momento dell'arruolamento nello studio, deceduti o non contattabili.

Sparisce l'obbligo per entrambe le ipotesi di consultazione preventiva del Garante *ex* art. 36 ma rimane l'obbligo di una valutazione d'impatto ai sensi dell'Art. 35 GDPR. Si noti però che il fatto di aver eliminato l'obbligo di consultazione preventiva del Garante non esime coloro che devono effettuare il trattamento dei dati per finalità di ricerca a consultare di propria sponte il Garante qualora, nella redazione della DPIA, sussistano forti dubbi in merito alla protezione dei dati personali degli interessati in entrambe le ipotesi delineate dal nuovo Articolo 110.

L'Articolo 110 bis invece riguarda il caso in cui sia un terzo (e quindi non il titolare né il responsabile del trattamento) che abbia bisogno di effettuare un ulteriore trattamento sui dati e il Garante può autorizzarlo. Per esempio, nel caso di uno studio clinico all'interno di un progetto di ricerca internazionale per cui un ospedale universitario italiano deve, come parte di un consorzio, condividere dati in forma pseudonimizzata a un altro partner che possa analizzare tali dati ai fini delle ricerche in oggetto[29].

[27] Garante per la Protezione dei Dati Personali, Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice - 9 maggio 2024 [10016146], https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10016146 (ultima consultazione 10/01/2025).

[28] Questo anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto pubblicamente accessibili.

[29] Tuttavia, il quarto comma dello stesso articolo enuncia che non costituisce un trattamento ulteriore da parte di terzi il trattamento eseguito dagli IRCCS. Tralasciando al momento le ragioni per cui solo gli IRCCS abbiano ottenuto questo trattamento di favore, bisogna aggiungere che il Garante ha pubblicato una serie di FAQ che illustrano come gli IRCCS debbano comportarsi per essere conformi alle nuove regole. Si veda Garante per la Protezione dei Dati Personali, Presupposti giuridici e principali adempimenti per il trattamento da parte degli IRCCS dei dati personali raccolti ai fini di cura della salute e per ulteriori scopi di ricerca, https://www.garanteprivacy.it/temi/sanita-e-ricerca-scientifica/irccs, (ultima consultazione 10/01/2025).

Questa modifica si inserisce nel più ampio processo che vede un incremento di interventi finalizzati a consentire un migliore (e maggiore) accesso ai dati. Come si descriverà meglio anche *infra* 3.4, il concretizzarsi della *digital policy* europea sotto la prima Commissione Von der Leyen[30] ha fatto dell'accesso ai dati una priorità: sia al fine di creare nuovi prodotti e servizi collegati su mercati secondari come nel DA,[31] sia anche la condivisione per ragione di interesse pubblico e principalmente finalizzata all'accesso ai dati sanitari per motivi di ricerca che è la *ratio* sottostante allo spazio sanitario dei dati europei (EHDS)[32].

Nelle more dell'approvazione dell'EHDS, e anticipando le sfide per la sua implementazione, l'Italia ha adottato una strategia multilivello.[33] Il Governo, tramite il Ministero della Salute e il Ministero delle Finanze ha iniziato un dialogo con il Garante al fine di presentare un disegno di legge finalizzato a potenziare il fascicolo sanitario elettronico (FSE 2.0) secondo quanto stabilito dall'EHDS in tema di *personal health records* interoperabili e uniformi in tutta l'UE, contemperando allo stesso tempo la protezione dei dati personali[34].

Gli interventi del legislatore italiano mirano dunque a seguire le scelte europee finalizzate a rendere meno difficoltoso il riuso dei dati ai fini di ricerca. Tuttavia, dopo aver spiegato come si struttura l'obbligo di accesso ai dati nel DA e nel EDHS nelle prossime sezioni si proverà a delineare quali contrasti possano sorgere con la novellata disciplina sul riuso dei dati sanitari.

2.2. Le regole specifiche che emergono dal Regolamento sui dispositivi medici

Un'altra normativa che è applicabile all'IoMT è il Regolamento sui dispositivi medici n. 2017/745 (MDR)[35]. Il MDR ha sostituito due precedenti direttive sui dispositivi medici (la direttiva 90/385/CEE del Consiglio sui dispositivi medici impiantabili attivi (AIMD) e la direttiva 93/42/CEE del Consiglio sui

[30] Si veda la Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Plasmare il futuro digitale dell'Europa, COM/2020/67 final, 7-10. Il consolidamento delle azioni della prima commissione Von der Leyen sono contenute nella recente Proposta di Decisione che istituisce il programma strategico per il 2030 "Percorso per il decennio digitale", COM/2021/574 final.

[31] *Infra* sezione 3 del contributo

[32] *Infra* sezione 4 del contributo

[33] Per il DA questo tipo di ragionamento non si applica in quanto è una legislazione che offre per la maggior parte strumenti di natura contrattuale e la creazione di strutture amministrative non inficia la più facile applicazione da parte dei privati. Si veda la sezione 3 e la 5 per maggiori dettagli.

[34] Si veda in particolare Garante per la protezione dei dati personali, Parere sullo schema di decreto del Ministero della salute sull'ecosistema Dati Sanitari (EDS), ai sensi dell'art. 12, comma 15-quater, del decreto-legge 18 ottobre 2012, n. 179 - 26 settembre 2024 [10062302]https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10062302,(ultima consultazione 10/01/2025) ; Garante per la protezione dei dati personali, Parere sullo schema di decreto del Ministero della salute che modifica il decreto del Ministero della salute del 7 settembre 2023, introducendo una disciplina transitoria delle disposizioni sul FSE 2.0 (art. 27 - bis) - 26 settembre 2024 [10061545] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10061545 (ultima consultazione 10/01/2025).

[35] Il regolamento MDR è collegato al regolamento 2017/746 sui dispositivi medico-diagnostici in vitro e abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione. Tuttavia, quest'ultima esula dallo scopo della presente analisi.

dispositivi medici (MDD) il 26 maggio 2021)[36]. Il nuovo quadro normativo ha portato anche alcune novità per quanto riguarda la definizione di dispositivi medici[37].

La presente analisi si concentra solo sull'IoMT qualificati come dispositivi medici. Secondo l'art. 2(1) MDR, un dispositivo medico è «qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione», per uno degli obiettivi specifici elencati nelle righe successive dello stesso articolo[38]. L'aggiornamento importante è l'inclusione del software tra i tipi di dispositivi medici, sia quelli autonomi che quelli collegati ad altri software, nonché quelli offerti come servizio a un altro dispositivo medico[39]. È importante notare che quando il software si qualifica come accessorio, cioè è in grado di pilotare le prestazioni di un dispositivo ma come componente indipendente non esegue azioni mediche, non si qualifica come dispositivo medico ed è regolato dal Regolamento sulla Sicurezza Generale dei Prodotti (General Product Safety Regulation, GPSR)[40] o, a seconda del caso, da legislazioni armonizzate più specifiche come il nuovo Regolamento Macchine (Machinery Regulation, MR)[41]. La distinzione tra software "normale" e software per dispositivi medici (medical devices, MD) si è già dimostrata poco chiara. Ad esempio, si può immaginare che il software medico possa essere scaricato su un oggetto IoT. Questo nuovo prodotto connesso con un servizio correlato potrebbe costituire un nuovo IoMT, quindi un nuovo dispositivo medico? Nello scenario meno problematico, l'IoT su cui viene

[36] Si noti che la revisione del quadro legislativo è stata innescata dal cosiddetto scandalo PIP, che ha messo a rischio la sicurezza di oltre 400 mila donne che hanno utilizzato silicone industriale nelle protesi mammarie.

[37] T. MULDER, *The impact of the European Medical Device Regulations on the Development and Use of Mhealth Apps in Europe*, in J. MADIR (a cura di), *healthtech*, Cheltenham, 2020; H. YU, *Regulation of Digital Health Technologies in the European Union: Intended versus Actual Use*, in G. COHEN E ALTRI (a cura di), *The Future of Medical Device* Regulation, Cambridge, 2022, 103 ; K. BICZYSKO-PUDEŁKO, The Regulatory Environment for the Safety of the Internet of Medical Devices Users in the European Union and the United States, in *European Journal of Risk Regulation*, 2024, 1.

[38] L'elenco è il seguente:
Diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie,
Diagnosi, monitoraggio, trattamento, attenuazione o compensazione di una lesione o di una disabilità,
Studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico,
Fornire informazioni attraverso l'esame in vitro di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati,e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere coadiuvata da tali mezzi.
Si considerano dispositivi medici anche i seguenti prodotti:
Dispositivi per il controllo del concepimento o il supporto al concepimento,
I prodotti specificamente destinati alla pulizia, disinfezione o sterilizzazione dei dispositivi.

[39] 'Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 -MDR and Regulation (EU) 2017/746- IVDR' (MDCG 2019) 11; K. LUDVIGSEN, S. NAGARAJA E A. DALY, *When Is Software a Medical Device? Understanding and Determining the "Intention" and Requirements for Software as a Medical Device in European Union Law*, in *European Journal of Risk Regulation*, 13, 2022,78.

[40] Art. 2(1) GPRS, Regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio del 10 maggio 2023 relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e la direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, e che abroga la direttiva 2001/95/CE del Parlamento europeo e del Consiglio e la direttiva 87/357/CEE del Consiglio (Testo rilevante ai fini del SEE) PE/79/2022/REV/1 GU L 135 del 23.5.2023, pagg. 1–51

[41] Regolamento (UE) 2023/1230 del Parlamento europeo e del Consiglio, del 14 giugno 2023, relativo alle macchine e che abroga la direttiva 2006/42/CE del Parlamento europeo e del Consiglio e la direttiva 73/361/CEE del Consiglio (Testo rilevante ai fini del SEE) PE/6/2023/REV/1 GU L 165 del 29.6.2023, pagg. 1–102.

scaricato il software non è un dispositivo medico. Pertanto, secondo il MDR, l'oggetto IoT può essere considerato un accessorio di un dispositivo medico[42]. Molto probabilmente, però, l'IoT è già un dispositivo medico il cui funzionamento viene migliorato dal software. Dunque, il risultato potrebbe essere un nuovo dispositivo medico o, più probabilmente, un gruppo generico di dispositivi[43] o un sistema[44], a cui si applicano complessivamente le norme del MDR.

Inoltre, la definizione di cui all'art. 2 (1) MDR fornisce i due criteri cumulativi che distinguono tra dispositivi medici e software per il benessere[45]. Se lo scopo è tra quelli elencati[46], il dispositivo/software si qualifica come dispositivo medico. L'art. 2 (12) MDR stabilisce che la finalità d'uso del dispositivo medico è indicata dal fabbricante. Pertanto, spetta al fabbricante fornire informazioni sullo scopo del dispositivo sull'etichetta, nelle istruzioni per l'uso o nel materiale promozionale o di vendita o nelle dichiarazioni.

Il MDR fa riferimento al GDPR in termini di protezione dei dati personali, ai sensi dell'art. 110 MDR. Pertanto, i ruoli di titolare e/o responsabile del trattamento dei dati possono essere individuati nell'accordo sul trattamento dei dati effettuato dal dispositivo medico. A seguito della descrizione precedente, possiamo individuare e distinguere diverse ipotesi a seconda delle caratteristiche tecniche dell'IoMT. La più comune è il caso di un IoMT come dispositivo autonomo (*standalone*): in questo caso, il ruolo di titolare del trattamento dei dati può essere attribuito al fabbricante del dispositivo. Tuttavia, a seconda della possibilità per un esperto medico di verificare i risultati del dispositivo applicato a un paziente, può verificarsi un controllo congiunto con l'esperto medico. Questo è il caso di HomeKit Lite[47], che è un dispositivo medico autonomo certificato progettato per la riabilitazione dei pazienti con deficit cognitivi sia in ospedale che a casa. Il dispositivo comprende un insieme di componenti e sensori che consentono al paziente di eseguire diversi esercizi: esercizi cognitivi, ma anche logopedici, posturali, facciali, respiratori, motori e di abilità neuromotorie. Il sistema può essere utilizzato offline, raccogliendo informazioni sulle attività del paziente e in collegamento con il terapista, che può monitorare i risultati precedenti raccolti dal dispositivo e adattarsi alle esigenze del paziente. In questo caso, sebbene il dispositivo medico sia un dispositivo autonomo che non sfrutta alcun servizio esterno per l'archiviazione e l'elaborazione (come, ad esempio, un servizio di cloud computing), i dati sanitari relativi al paziente vengono condivisi anche direttamente con il terapeuta.

Finora, la legislazione applicabile al trattamento dei dati da parte dell'IoMT si è limitata alle suddette disposizioni del GDPR e del MDR. Supponiamo che i produttori siano interessati a sviluppare nuovi IoT nel settore medico, come applicazioni e dispositivi che integrano i dispositivi esistenti. In questo caso,

[42] Articolo 2 (2) MDR.

[43] Art. 2(7) MDR. 2(7) MDR. Si riferisce a «[...]Serie di dispositivi con destinazioni d'uso identiche o analoghe o che condividono la stessa tecnologia, cosicché possono essere classificati in modo generico, senza tenere conto di caratteristiche specifiche».

[44] Art. 2(11) MDR. 2(11) MDR. Secondo tale articolo, per sistema si intende «[...] Una combinazione di prodotti, confezionati insieme o non, che sono destinati a essere interconnessi o combinati per raggiungere una specifica destinazione d'uso medica».

[45] H. VAN KOLFSCHOOTEN, *The mhealth Power Paradox: Improving Data Protection in Health Apps through Self-Regulation in the European Union*, in I. GLENN COHEN e altri (a cura di), *The Future of Medical Device Regulation*, Cambridge, 2022.

[46] Vedi *supra* n. 39.

[47] Cfr. Https://khymeia.com/en/products/homekit/ (ultima consultazione 10/01/2025).

ISSN 2284-4503

non possono sfruttare le strutture di dati già disponibili nei dispositivi esistenti. Ad esempio, lo sviluppo di un software medico basato sull'intelligenza artificiale che consenta il riconoscimento di formazioni tumorali può essere meglio addestrato e testato con i dati e i modelli rilevati dai dispositivi medici esistenti. In questo caso, il fabbricante potrebbe non essere in grado di accedere a tali dati, se non applicando le specifiche eccezioni previste dagli articoli 6 e 9 del GDPR[48]. Inoltre, le condizioni per la condivisione dei dati non sono definite nel GDPR e, ad esempio, nel caso di standard di interoperabilità specifici per l'interpretazione e l'utilizzo dei dati, la mancanza di coordinamento e coerenza può ridurre i vantaggi della condivisione dei dati. Queste limitazioni sono affrontate e provvisoriamente risolte dal DA e dalla legislazione EHDS recentemente adottati.

3. L'impatto del Data Act sullo sviluppo di IoMT

L'IoMT sarà inoltre soggetto alle regole definite nel Data Act (DA)[49]. Per chiarire come il DA influenzerà le scelte dei fabbricanti, è necessario comprendere la ratio di questo atto legislativo confrontandolo con la struttura e il funzionamento di un IoMT (3.1). In secondo luogo, verrà descritto il funzionamento del DA, concentrandosi sugli schemi contrattuali di condivisione dei dati e sulla loro applicabilità all'IoMT (3.2). Infine, verranno affrontate le sovrapposizioni, i contrasti e la possibile armonizzazione dei soggetti coinvolti nella condivisione dei dati della DA con quelli del GDPR (3.3)[50].

3.1. L'origine, le *rationes* e l'applicazione del DA

Il DA deve essere preso in considerazione quando si discutono le pratiche di condivisione dei dati (*data sharing*) degli oggetti IoMT per due motivi. In primo luogo è la normativa più generale (orizzontale, nella terminologia del diritto dell'UE) in materia di condivisione dei dati e riguarda sia i dati personali (sanitari) sia i dati non personali, come stabilito dall'art. 1, paragrafi 1 e 2, del DA. 1(1) e (2) del DA. Il DA intende basarsi sui principi di condivisione dei dati del GDPR e della Free Flow of Data Initiative[51] e applicarli alle nuove tecnologie basate sui dati, come l'IoT e, in prospettiva, alcuni tipi di IA. A meno

[48] R. BECKER E ALTRI, *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*, 30, 2022, 129; S. SLOKENBERGA, *Scientific Research Regime 2.0? Transformations of the Research Regime and the Protection of the Data Subject That the Proposed EHDS Regulation Promises to Bring Along*, in *Technology and Regulation*, 2022, 135; M. SHABANI E S. YILMAZ, *Lawfulness in Secondary Use of Health Data Interplay between Three Regulatory Frameworks of GDPR, DGA & EHDS*, in *Technology and Regulation*, 2022, 128. Si noti che in alcuni casi, ai sensi dell'art. 9 (4) del GDPR, gli Stati membri mantengono la libertà di prevedere un livello di protezione più elevato o la possibilità di stabilire limitazioni al trattamento dei dati sanitari e genetici.

[49] Citato *supra* 1. In questa parte dell'articolo saranno presenti confronti con la precedente proposta di Data Act (proposta DA) i cui riferimenti bibliografici sono i seguenti: Proposta di Regolamento del Parlamento Europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati) COM/2022/68 final.

[50] Come limite metodologico, non considereremo la prospettiva della cybersecurity. In questo caso, per quanto riguarda l'IoMT, il MDR prevede per i produttori obblighi di cybersecurity per i dispositivi medici.

[51] 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 (Testo rilevante ai fini del SEE.). PE/53/2018/REV/1 GU L 303 del 28.11.2018, pagg. 59–68.

che non vi sia una futura normativa più specifica riguardante l'IoMT, il DA sarà applicabile principalmente per scenari di condivisione di dati sanitari tra soggetti *business-to-business* (B2B) e *business-to-consumer* (B2C), anche se la prima ipotesi appare più probabile. È inoltre importante sottolineare che questa condivisione di dati avverrà per lo più attraverso contratti, cosa non ovvia quando è iniziato il dibattito sul regolamento[52]. In secondo luogo, uno degli obiettivi del DA è quello di rendere disponibili «[...] i dati del prodotto connesso e di un servizio correlato all'utente del prodotto connesso o del servizio correlato» (art. 1(a) DA). I dati del prodotto sono generati da un prodotto connesso, che non è altro che un oggetto IoT[53]. Infatti, l'art. 2(5) DA descrive il prodotto connesso come «[...]un bene che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente e che è in grado di comunicare dati del prodotto tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo, e la cui funzione primaria non è l'archiviazione, il trattamento o la trasmissione dei dati per conto di una parte diversa dall'utente». La definizione del DA è più dettagliata di quella della proposta per quanto riguarda il modo in cui l'IoMT funziona mentre è collegato ad altri IoT, a prese o al corpo umano (che, nel caso dell'IoMT, sarà una possibilità più che probabile) e le scelte di accesso[54]. Data la generalità di questa definizione, anche un IoMT, come un dispositivo indossabile per il monitoraggio del battito cardiaco, è un tipo di prodotto connesso.

Per quanto riguarda le tecnologie considerate, il DA prende in considerazione l'Intelligenza Artificiale (IA), nel prossimo futuro, soprattutto quando si occupa dei dati dei servizi connessi al dispositivo, generati dai "servizi correlati". Il termine servizio correlato non è nuovo per la politica digitale dell'UE, in quanto è apparso con nomi leggermente diversi come parte di servizio digitale dei beni con elementi digitali nelle due direttive "gemelle" relative alla vendita di beni[55] e alla fornitura di contenuto digitale

[52] L.A. BYGRAVE, *The Predilection for Contract in Governing Digital Networks: Micro-Management's Face Off with Accountability*, in *SSRN*, 2023, https://papers.ssrn.com/abstract=4417972 , ultimo consultazione 10/01/2025); L. TRAKMAN, R. WALTERS, B. ZELLER, *Is Privacy and Personal Data Set to Become the New Intellectual Property?*, 3 settembre 2019, https://papers.ssrn.com/abstract=3448959,(ultima consultazione 10/01/2025); H. ULLRICH, *Technology Protection and Competition Policy for the Information Economy. From Property Rights for Competition to Competition Without Proper Rights?*, in *SSRN*, https://papers.ssrn.com/abstract=3437177, (ultima consultazione 10/01/2025); J. DREXL, *Designing Competitive Markets for Data* Between *Propertisation and Access*, in *Max Planck Institute for Innovation & Cometition Research paper*, N. 16-13, 2017, 257.

[53] D. BANDYOPADHYAY, J. SEN, *Internet of Things: Applications and Challenges in Technology and Standardization*, in *Wireless Personal Communications*, 58, 2011, 49; A. RAYES E S. SALAM, *Internet of Things From Hype to Reality: The Road to Digitization*, Cham- Svizzera, 2019.

[54] Questa definizione è più dettagliata rispetto alla definizione di (solo) prodotto contenuta nella proposta iniziale, che recitava: «Per "prodotto" si intende un oggetto tangibile e mobile, anche se incorporato in un oggetto immobile, che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente e che è in grado di comunicare dati tramite un servizio di comunicazione elettronica accessibile al pubblico e la cui funzione principale non è la memorizzazione e l'elaborazione di dati».

[55] Art. 2, paragrafo 5, lettera b) Direttiva (UE) 2019/771 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di vendita di beni, che modifica il regolamento (UE) 2017/2394 e la direttiva 2009/22/CE, e che abroga la direttiva 1999/44/CE (Testo rilevante ai fini del SEE.) PE/27/2019/REV/1 GU L 136 del 22.5.2019, pagg. 28–50.

e servizi digitali[56], e nella più recente modifica della Direttiva sulla responsabilità del prodotto (PLDU)[57]. Tutte queste definizioni di servizio correlato presentano due aspetti comuni: in primo luogo, il servizio è integrato in qualche modo nel prodotto (scaricandolo o meno) e, in secondo luogo, «la sua assenza impedirebbe al prodotto collegato di svolgere una o più delle sue funzioni»[58] Nel DA è presente anche un'ulteriore specificazione relativa al servizio correlato: «che è successivamente connesso al prodotto dal fabbricante o da un terzo al fine di ampliare, aggiornare o adattare le funzioni del prodotto».

3.2. La regolazione dei contratti nel DA

Per spiegare l'applicazione del DA, è necessario innanzitutto descrivere i soggetti coinvolti nella condivisione dei dati (a) e, in secondo luogo, analizzare la struttura dei futuri contratti di condivisione dei dati o *data sharing* basati sul DA (b).

a) I soggetti che condividono i dati

I soggetti coinvolti nei contratti di condivisione dei dati sono principalmente tre e li descriveremo fornendo esempi pratici di chi potrebbe essere ciascun soggetto nel contesto IoMT.

Il primo è l'*utente*. Può essere non solo un consumatore ma anche un professionista. L'art. 2(12) DA stabilisce che l'utente è una persona fisica o giuridica «che possiede un prodotto connesso o a cui sono *stati trasferiti contrattualmente diritti temporanei di utilizzo*[59] di tale prodotto connesso o che riceve un servizio correlato»[60]. Tuttavia, se pensiamo all'IoMT, è improbabile che il paziente/consumatore che utilizza un IoMT o un software MD abbia le conoscenze, le risorse e l'iniziativa per stipulare un contratto di condivisione dei dati. È più probabile che il contratto di condivisione dei dati sia negoziato da un professionista, come un medico, o da una struttura sanitaria che ha acquistato o noleggiato un oggetto IoMT (ad esempio un IoMT intelligente per il monitoraggio cardiaco a distanza) o un software MD correlato (per esempio, un'applicazione di diagnostica per immagini basata sull'intelligenza artificiale per i tumori).

Il secondo soggetto coinvolto nel processo di condivisione dei dati è il *titolare dei dati*. L'art. 2(13) DA lo descrive come «persona fisica o giuridica che *ha il diritto o l'obbligo*[61], 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». Seguendo l'esempio precedente, il titolare dei dati potrebbe essere il fabbricante del prodotto connesso, ovvero l'azienda che commercializza l'IoMT per il monitoraggio della

[56] Art. 2, paragrafo 3, Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali (Testo rilevante ai fini del SEE.) PE/26/2019/REV/1 GU L 136 del 22/05/2019, pagg. 1–27

[57] Art. 4(3), Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio (Testo rilevante ai fini del SEE) PE/7/2024/REV/1 GU L, 2024/2853, 18.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2853/oj

[58] Art. 2(6) DA.

[59] Enfasi aggiunta dalle autrici.

[60] Enfasi aggiunta dalle autrici.

[61] Enfasi aggiunta dalle autrici.

salute a distanza. In questo caso, lo sviluppatore sarà il titolare dei dati del servizio correlato sviluppato, come l'applicazione di diagnostica per immagini basata sull'intelligenza artificiale per i tumori.
L'ultimo soggetto coinvolto è il *destinatario dei dati*. Ai sensi dell'art. 2(14) DA il destinatario dei dati è «una persona fisica o giuridica, che agisce per fini connessi alla sua attività commerciale, imprenditoriale, artigianale o professionale, *diversa dall'utente di un prodotto connesso o di un servizio correlato*, a disposizione della quale il titolare dei dati mette i dati, e che può essere un terzo in seguito a una richiesta da parte dell'utente al titolare dei dati o conformemente a un obbligo giuridico ai sensi del diritto dell'Unione o della legislazione nazionale adottata conformemente al diritto dell'Unione». Il destinatario dei dati è innanzitutto definito come una persona diversa dall'utente, che può essere una persona fisica o giuridica ma non un consumatore, in quanto è specificato che agisce per motivi professionali (*lato sensu*). Inoltre, il destinatario dei dati non può essere un titolare, in quanto è specificato che deve ricevere i dati dal titolare stesso. Può essere, invece, una *terza parte* che ha ricevuto dall'utente l'autorizzazione a chiedere l'accesso ai dati al titolare. Questo destinatario dei dati/terzo può anche agire autonomamente, ma solo se esiste un obbligo legale ai sensi del diritto dell'UE o del diritto nazionale che attua il diritto dell'UE. Quest'ultima possibilità sembra rientrare nell'ipotesi di condivisione obbligatoria dei dati con le istituzioni e gli organismi dell'UE in caso di emergenza[62]. Per continuare con gli esempi precedenti, la terza parte può essere un medico o una società di software che vuole sviluppare nuove applicazioni software compatibili con l'IoMT per il monitoraggio cardiaco, come ad esempio le applicazioni di e-wellness. Per quanto riguarda il secondo esempio, un'azienda di dispositivi medici che sviluppa IoMT, come dispositivi medici per la radioterapia o la chemioterapia, potrebbe essere interessata ad avere accesso ai dati del programma diagnostico basato sull'intelligenza artificiale per capire quale tipo di tumore è più frequente e come è distribuito tra una popolazione target (per esempio, i pazienti dell'ospedale per i quali questo software è stato utilizzato a fini diagnostici. Per i profili relativi al rapporto tra il titolare dei dati ai sensi del DA e del GDPR si veda *infra* 3.3).

b) I due principali schemi contrattuali di condivisione dei dati

Questa parte cerca di descrivere la struttura dei due principali tipi di contratti di condivisione dei dati previsti dagli articoli 4 e 5 del DA. Il primo è caratterizzato dall'assenza di intermediari tra l'utente e il titolare dei dati (b-1); il secondo, invece, è più sfaccettato, in quanto richiede una triangolazione di contratti, nessuno dei quali coinvolge direttamente tutti e tre i soggetti interessati, che sono l'utente, il titolare dei dati e il destinatario/terzo (b-2).

b-1) L'utente e il titolare dei dati. Un rapporto senza intermediari

In questo scenario, ci sono solo due parti/soggetti: l'utente e il titolare dei dati. L'utente che vuole accedere ai dati del prodotto o del servizio connesso per sviluppare un altro prodotto o servizio connesso. Questo nuovo prodotto o servizio non deve essere in concorrenza con quello originale, ai sensi dell'art. 4 (10) DA.

[62] Le regole per questo caso sono contenute nel Capitolo V del DA, in particolare gli articoli 14-22 del DA, ma non le discuteremo in questo contributo.

In linea di principio, il titolare dei dati dovrebbe costruire il prodotto o il servizio in modo da garantire una sorta di principio di "accessibilità by default e by design", analogo al principio di "privacy by default and by design" di cui all'art. 25 GDPR. Il titolare dei dati deve garantire l'accesso ai dati del prodotto e dei servizi correlati in modo che l'utente possa accedervi liberamente, ai sensi dell'art. 3 (1) DA. Inoltre, il titolare dei dati deve, come serie di doveri precontrattuali, informare in modo chiaro e comprensibile sulle qualità dei dati e la frequenza della raccolta dei dati eseguita dal prodotto connesso (art. 3(2) DA) e dai servizi correlati (art. 3(3) DA).

Se non è possibile accedere direttamente ai dati, è sufficiente che l'utente invii un modulo di richiesta mediante "mezzi elettronici" qualora sia fattibile per il titolare dei dati secondo l'art 4(1) DA. Inoltre, sempre ai sensi dell'art. 4(1) DA, il titolare dei dati è tenuto a rendere disponibili i dati, compresi i metadati. Dunque, esiste un parallelo tra il modo in cui un titolare e un responsabile del trattamento dei dati, ai sensi degli articoli 12-15 del GDPR, devono dare accesso ai dati. Infatti, nel contesto del DA, l'art. 4(1)DA obbliga il titolare dei dati a fornire i dati all'utente «senza indebito ritardo, con la stessa qualità di cui dispone il titolare dei dati, in modo facile, sicuro, gratuitamente, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove pertinente e tecnicamente possibile, modo continuo e in tempo reale».

Inoltre, secondo l'art. 4(5) DA, il titolare dei dati non può chiedere un numero sproporzionato di informazioni per identificare l'utente e sfruttarle per dedurre informazioni sulla sua situazione economica, come stabilito anche dal paragrafo 13 dello stesso articolo.

Il DA include un elenco esteso di doveri e obblighi reciproci delle parti, fino alle norme relative alla protezione della proprietà intellettuale e al diritto di presentare un reclamo. Il contratto tra il titolare dei dati e l'utente è lo strumento attraverso il quale vengono elencati i doveri e gli obblighi reciproci tra i due soggetti citati. Sia gli utenti che i titolari dei dati possono limitare o vietare contrattualmente l'accesso o l'ulteriore condivisione dei dati se, in questo modo, si possono compromettere i requisiti di sicurezza dell'oggetto, ai sensi dell'art. 4(2) DA. Inoltre, il titolare dei dati ha il dovere di non rendere difficoltoso l'esercizio dei diritti degli utenti. Questo obbiettivo può essere raggiunto utilizzando anche determinati design e suggerendo opzioni, ai sensi dell'art. 4(4) DA. In maniera speculare, l'utente non può approfittare delle lacune dell'infrastruttura tecnica del titolare dei dati, che è progettata per proteggere i dati dall'accesso.[63] Stabilendo obblighi di buona fede *de facto* tra le parti,[64] gli articoli 3 e 4 del DA sembrano implicare che sia l'utente che il titolare dei dati abbiano lo stesso potere contrattuale

[63] Art. 4(11) DA.

[64] Il termine buona fede, in questo contesto, viene desunto per interpretazione dal testo di legge che si limita ad elencare gli obblighi delle parti in ambito pre- e contrattuale. Se nella tradizione inglese questi doveri sono *duties of care* ed espressione di *fairness* e *good faith*, (sul tema si veda, ad esempio, *ex multis*, J. BEATSON, D. FRIEDMAN, *Good Faith and Fault in Contract Law*, Oxford, 1997; S. WEATHERHILL, *Contract Law of the Internal Market*, Cambridge, 2016),la traduzione italiana dei precitati concetti non può prescindere dalla nozione di buonafede contrattuale, degli obblighi di correttezza e buona fede e, per una parte della dottrina, degli obblighi di protezione. La letteratura in merito nella dottrina italiana è praticamente sterminata. *Ex multis*, M.C. BIANCA, *Dell'adempimento delle obbligazioni*, Bologna, 1967; E. DELL'AQUILA, *La correttezza nel diritto privato*, Milano, 1980; A. DI MAJO, *Delle obbligazioni in generale*, Bologna, 1988, A. D'ANGELO, *Il contratto in generale: tomo IV la buona fede*, Torino, 2004, A. SCALISI, *La comune intenzione dei contraenti: dall'interpretazione letterale del contratto all'interpretazione secondo buona fede*, Milano, 2003; ma anche, con un focus sulla teorica degli obblighi di protezione, L. LAMBO, *Obblighi di protezione*, Padova, 2007, C. CASTRONOVO, *La responsabilità civile*, Milano, 2018.

e negoziale, soprattutto per quanto riguarda diritti di proprietà intellettuale come per i segreti commerciali e industriali. Ciò è confermato dall'art. 13 DA, che stabilisce il carattere non vincolante di un contratto, istituendo una nullità di protezione, nel caso in cui una clausola "si discosti gravemente dalle buone pratiche commerciali in materia di accesso e utilizzo dei dati, in contrasto con la buona fede e la correttezza". Per quanto riguarda la protezione di diritti di proprietà intellettuale, è molto probabile che dando accesso a dati e metadati si possano esporre diritti di proprietà intellettuale come i segreti industriali e commerciali[65].

L'ultima serie di obblighi riguarda il diritto di presentare un reclamo, che si può individuare nei paragrafi 3 e 9 dell'art. 4 DA. Il loro contenuto è simile, in quanto entrambe le procedure di reclamo non pregiudicano l'azione legale presso le corti nazionali, ma la prima si riferisce a disaccordi riguardanti i vincoli di sicurezza menzionati nel secondo paragrafo dello stesso articolo; il paragrafo 9 riguarda invece la protezione dei segreti commerciali. Sia nell'art. 4(3) e (9), il diritto di presentare il reclamo può essere esercitato seguendo la procedura di cui all'art. 37(5)(b) DA o concordando con il titolare dei dati di risolvere la questione con un organismo di risoluzione delle controversie di cui all'art. 10(1) DA.

L'ultimo elemento rilevante è l'Art. 4 DA, che collega esplicitamente il DA al GDPR. In particolare, si spiega quale base giuridica del GDPR si debba utilizzare quando si dà accesso a dati personali che non sono (solo) quelli dell'utente[66] Il paragrafo si limita a sottolineare che sia l'Art. 6 e l'art. 9 GDPR sono lasciati impregiudicati, così come l'art. 5(3) della direttiva E-privacy.[67] Questo aspetto, in relazione agli scenari pratici che coinvolgono gli stakeholder dell'IoMT, sarà trattato in modo approfondito nella sez. 3.3.

[65] Una prima forma di armonizzazione europea di nozione di segreti industriali e commerciali è stata data dalla direttiva sulla protezione del know-how e delle informazioni commerciali riservate (segreti commerciali) che al suo articolo 2(1) definisce il termine segreto commerciale come un insieme di informazioni che soddisfano cumulativamente tre requisiti "a) sono segrete nel senso che non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione: b) hanno valore commerciale in quanto segrete; c) sono state sottoposte a misure ragionevoli, secondo le circostanze, da parte della persona al cui legittimo controllo sono soggette, a mantenerle segrete". Direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti (Testo rilevante ai fini del SEE) GU L 157 del 15.6.2016, pagg. 1–18.

[66] Art. 4(12) DA. Per maggiori informazioni sull'interpretazione di questo paragrafo in relazione all'IoMTt si veda *infra* 3.3.

[67] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), GU L 201 del 31.7.2002, pag. 37.

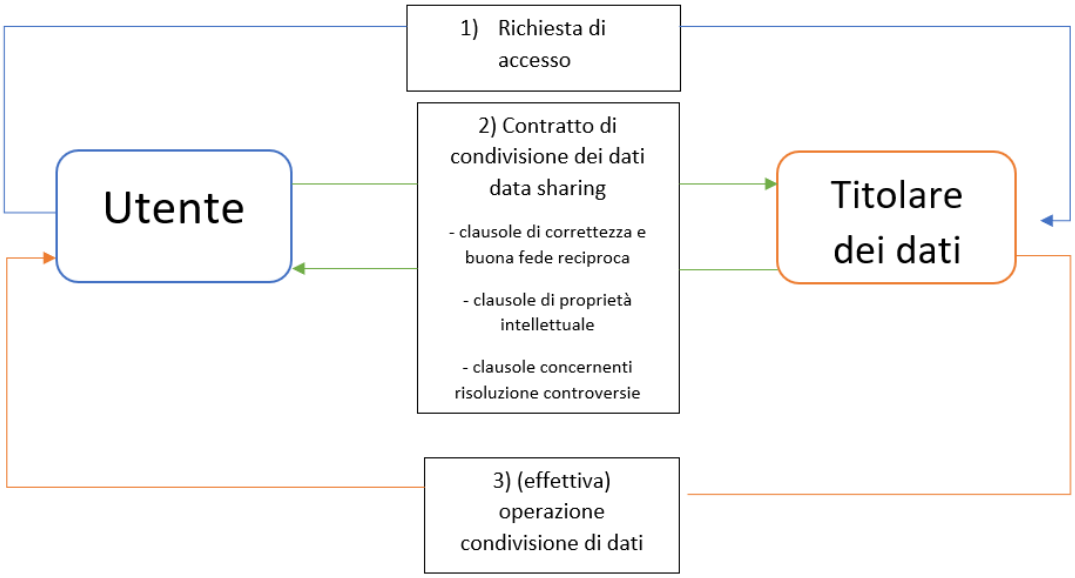

Figura 1. Il primo schema di contratto di condivisione dei dati. Utente - Titolare dei dati

b-2) Titolari dei dati, destinatari dei dati, utenti e terzi. Relazioni triangolari

Il secondo schema di condivisione dei dati è più complesso del precedente anche perché la rubrica dell'articolo in esame presenta una rubrica un po' ambigua. Si tratta del "diritto dell'utente di condividere i dati con terzi". Sembra che in questo caso i termini destinatario dei dati e terzo siano usati in modo intercambiabile. Nella parte di definizioni, il termine terza parte usato nell'articolo 5 non viene definito. Rimane quindi solo il termine destinatario dei dati. Il fatto che il DA consideri terzi e destinatari in modo interscambiabile si può dedurre dal fatto che l'art. 5 DA menziona solo i terzi, mentre l'art. 8 DA, che riguarda le «condizioni alle quali i titolari dei dati mettono i dati a disposizione dei destinatari dei dati», fa un riferimento incrociato con l'art. 5 DA. Questa mancanza di chiarezza potrebbe avere un impatto sulla futura applicazione di queste norme nei contratti di condivisione dei dati. Per ragioni metodologiche e per evitare confusione, utilizzeremo i termini destinatario dei dati e terzo in modo intercambiabile. Tuttavia, è importante notare che, ai sensi dell'art. 2(14) DA, i terzi sono una delle categorie di destinatari dei dati, ma questa definizione non è completamente sovrapponibile con il termine destinatario. Chi possono essere i terzi, se non quelli scelti dall'utente? Nonostante questa ambivalenza, l'art. 5 DA descrive due diversi sottoinsiemi di contratti di condivisione dei dati che corrispondono alla doppia definizione del termine destinatario dei dati analizzata al punto (a).

L'art. 5(1) DA descrive il primo sottoinsieme di contratti di condivisione dei dati. In questa prima ipotesi, l'utente può chiedere al titolare dei dati di mettere i dati a disposizione di un terzo/destinatario

dei dati di sua scelta[68]. L'alternativa, invece, è che un destinatario di dati/terzo chieda di ottenere l'accesso ai dati relativi al prodotto/servizio per conto dell'utente al titolare dei dati[69]. In base alla definizione di destinatario dei dati, potrebbe esserci anche un'altra ipotesi, ovvero quando la terza parte chiede al titolare dei dati di accedere ai dati in base a un obbligo di legge nazionale o dell'UE. Quest'ultima ipotesi sembra essere collegata al Capitolo V, che prevede l'obbligo di rendere disponibili i dati agli enti pubblici, alla Commissione UE, alla BCE e agli organi dell'Unione in caso di necessità eccezionale[70].

Una delle differenze tra gli articoli 4 e 5 riguarda la presenza di un divieto soggettivo nell'ultimo articolo. L'art. 5(3) DA impedisce all'utente di designare un *gatekeeper* ai sensi del Regolamento europeo sui mercati digitali (DMA)[71]. Questo perché qualsiasi piattaforma, fornitore di servizi cloud o altro dall'elenco dei soggetti interessati che rispondono ai criteri dell'art. 3 DMA, detiene un potere economico e tecnologico tale da poterne trarre vantaggio per diventare leader nei mercati secondari dei prodotti connessi o dei servizi correlati, pur essendo già *di fatto* dominante per quanto riguarda alcuni prodotti connessi o servizi correlati su altri mercati[72].

A parte questi sottoinsiemi di altri contratti, l'Art. 5 DA è simile all'art. 4 DA per quanto riguarda gli obblighi reciproci di "buona fede" tra il titolare dei dati e i terzi/destinatari dei dati. Si tratta, ad esempio, del dovere del terzo di rispettare i beni di proprietà intellettuale (segreti commerciali) del titolare dei dati[73]. Ma la terza parte/il destinatario dei dati ha anche una serie di obblighi nei confronti dell'utente stabiliti dall'art. 6 DA che possono essere sintetizzati come parte degli obblighi di correttezza e buona fede nei confronti dell'utente[74]. 6 DA. Inoltre, solo nel caso in cui vi sia un destinatario dei dati, il titolare può chiedere a quest'ultimo il pagamento di un corrispettivo, che dovrà essere calcolato secondo i principi di equità, ragionevolezza e non discriminazione (FAIR), esclusivamente nei contratti b2b[75].

[68] Art. 5(1) DA prima parte. 5(1) DA prima parte.

[69] Art. 5(1) DA seconda parte. 5(1) DA seconda parte.

[70] Si tratta di un'opzione che l'amministrazione nazionale e quella dell'UE possono utilizzare solo in pochi casi, meglio specificati all'art. 15 DA.

[71] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati contendibili ed equi nel settore digitale e recante modifica delle direttive (UE) 2019/1937 e (UE) 2020/1828 (Regolamento sui mercati digitali) PE/17/2022/REV/1 GU L 265 del 12.10.2022, pag. 1, http://data.europa.eu/eli/reg/2022/1925/oj.

[72] In particolare, per qualificare una impresa come *gatekeeper*, questa deve offrire un servizio di piattaforma di base definita all'Articolo 2(2) e che ricomprende varie categorie (dai motori di ricerca, agli assistenti virtuali, ai servizi di social network), Poi l'impresa deve rispettare i criteri di soglia definiti all'Articolo 3 e che, se rispettati, fanno presumere che la presenza dell'impresa stessa sul mercato interno eserciti un impatto significativi, nel senso che da sola può consentire o meno l'accesso a un mercato. Si veda sull'argomento anche F. CHIRICO. *Digital Markets Act: A Regulatory Perspective*, in *Journal of European Competition Law and Practice* 12,7, 2021, 493-499, P. BONGARTZ, S. LANGSTEIN, R. PRODSZUN, *The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers*, in *Journal of European Competition Law and Practice,* 10, 2, 2021 60-67.

[73] Art. 5 (7), (8), (9), (10) da. 5 (7), (8), (9), (10) DA.

[74] Per esempio, tra questi possiamo trovare, l'obbligo di non rendere all'utente difficile l'esercizio dei suoi diritti stabiliti dallo stesso articolo 5 in maniera non neutrale (a); oppure utilizzare i dati ottenuti con l'accesso per la profilazione (fatta eccezione per l'Articolo 22 lettere a e c del GDPR)(b); e non mette a disposizione dei *gatekeeper* i dati ottenuti.

[75] Art. 9(1) DA.

L'unica questione che rimane da trattare riguarda i contratti tra l'utente e il terzo/destinatario dei dati. Nella prima parte dell'Art. 5 DA, è implicito che la conclusione di un contratto relativo all'uso corretto dei dati nella disponibilità del titolare dei dati tra l'utente e il destinatario dei dati per la creazione del nuovo IoMT precede il contratto/accordo tra il titolare dei dati e il destinatario dei dati. Il contenuto di quest'ultimo contratto, descritto in precedenza, comprende clausole di buona fede e correttezza reciproca nell'esecuzione del contratto, clausole relative alla proprietà intellettuale ed eventuali restrizioni alla condivisione dei dati e clausole di risoluzione delle controversie. Tuttavia, si può anche immaginare il contenuto del contratto che deve esistere tra l'utente e il destinatario dei dati, anche se non è esplicitamente descritto nel DA. Per certi versi, potrebbe essere simile al contratto di condivisione dei dati, ma ci sono almeno due elementi diversi. Il primo insieme di queste clausole specifiche è il progetto dei nuovi IoMT o delle relative caratteristiche del servizio. Quasi certamente, potrebbero esserci clausole relative alla gestione dei diritti di proprietà intellettuale (ad esempio, se cercare di brevettare una soluzione o se mantenerla come segreto commerciale o se rendere open-source un'ipotetica soluzione software medica basata sull'intelligenza artificiale). Inoltre, potrebbero esserci clausole relative alla risoluzione delle controversie che coinvolgono le norme di diritto privato internazionale, se necessario. La seconda serie di clausole riguarda solo il secondo tipo di contratto descritto dall'art. 5, in cui il destinatario dei dati si rivolge direttamente al titolare per l'operazione di condivisione dei dati. Tuttavia, tra l'utente e il destinatario dei dati/terzo potrebbe già esistere non solo un contratto precedente sulla realizzazione del nuovo IoMT o servizio, ma anche un contratto di mandato/rappresentanza. Questo può anche esistere in un documento separato, ma conterrà l'autorizzazione formale dell'utente al destinatario dei dati per chiedere al titolare dei dati l'accesso ai dati pertinenti. Sarà la legge nazionale a disciplinare le regole di questo contratto di mandato/rappresentanza.
In sintesi, questi sottoinsiemi di contratti alludono a una relazione triangolare (titolare dei dati, destinatario dei dati e utente), ma tutti prevedono almeno due contratti distinti in cui solo due delle parti sono direttamente coinvolte. Nella prima ipotesi, c'è un contratto/richiesta da parte dell'utente di mettere i dati a disposizione di un destinatario/terzo e un contratto/insieme di doveri reciproci tra il destinatario e il titolare dei dati e, molto probabilmente, un contratto tra l'utente e il destinatario dei dati. Nella seconda ipotesi, l'utente delega (attraverso un contratto) la terza parte/destinatario dei dati a chiedere l'accesso ai dati a un titolare. Anche in questo caso, dovrebbe esistere un contratto tra il titolare dei dati e il destinatario dei dati che agisce per conto dell'utente, di cui l'utente non fa formalmente parte.

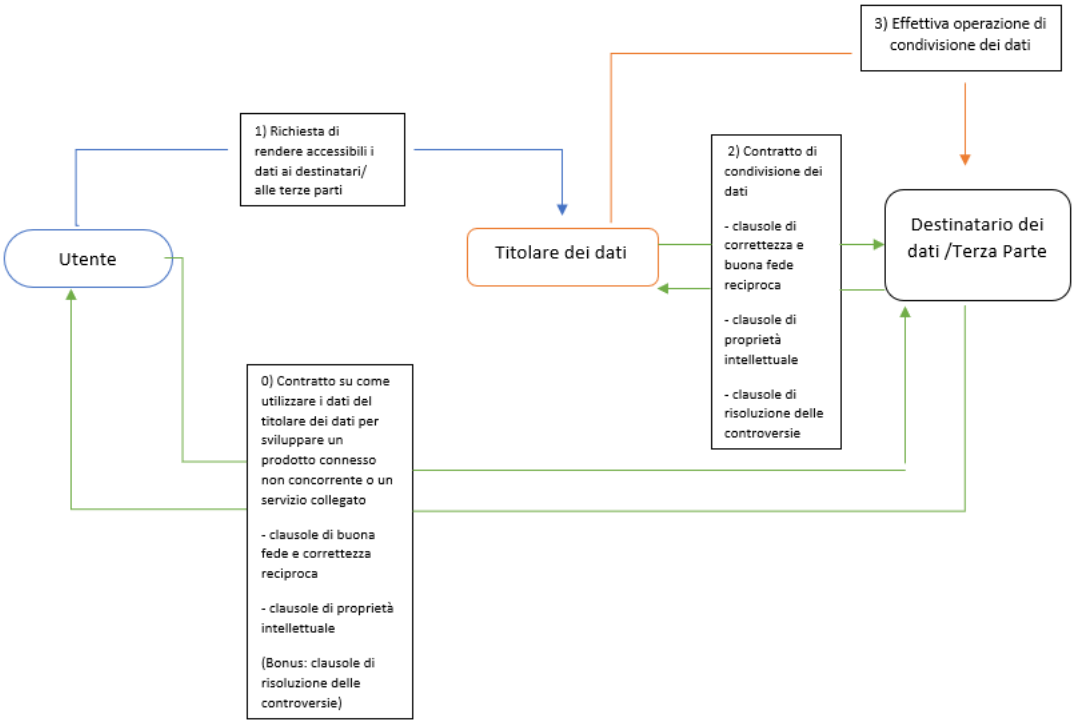

Figura 2. Il secondo schema di contratto di condivisione dei dati. Richiesta dell'utente - Titolare dei dati

Figura 3. Il secondo schema di contratto di condivisione dei dati. Richiesta dell'utente al destinatario dei dati/terza parte

3.3. Sovrapposizioni e incongruenze con il quadro normativo in materia di protezione dei dati personali

Se teniamo presente l'obiettivo di questo articolo, che è quello di trovare le potenziali sovrapposizioni, i contrasti e l'applicazione congiunta della politica digitale dell'UE per quanto riguarda gli oggetti IoMT, allora è il momento di fare riferimento ai paragrafi 4(12) e 5(7) DA che creano il collegamento con il testo del GDPR nel contesto della condivisione dei dati[76].

Il contenuto di questi due paragrafi è lo stesso, ma si applica rispettivamente al contratto di condivisione dei dati tra utente e titolare e alle varie relazioni contrattuali "triangolari" tra utenti, titolari dei dati e terzi/destinatari dei dati. Il loro campo di applicazione è uno solo: «Se l'utente non è l'interessato i cui dati personali sono richiesti, i dati personali generati dall'uso di un prodotto connesso o di un servizio correlato sono messi a disposizione dell'utente dal titolare dei dati solo se esiste una valida base giuridica del trattamento a norma dell'articolo 6 [GDPR] e, ove pertinente, se sono soddisfatte le condizioni di cui all'articolo 9 [GDPR] e all'articolo 5, paragrafo 3, della direttiva 2002/58/CE».

[76] Si noti che il riferimento è superfluo, poiché il quadro giuridico del GDPR si sarebbe comunque applicato a tale trattamento dei dati.

Nonostante il DA affermi di salvaguardare l'applicazione del GDPR[77], condividendo anche alcune delle sue definizioni[78], vi sono dubbi sul coordinamento tra il GDPR e il DA. Gli stessi European Data Protection Board (EDPB) e lo European Data Protection Supervisor (EDPS) hanno già definito questa relazione potenzialmente problematica nel loro parere congiunto del 2022[79].

In realtà, per i fabbricanti di dispositivi IoMT è più utile sapere se esista o meno una sovrapposizione (anche parziale) tra il GDPR e i soggetti DA non solo per motivi di conformità al GDPR ma anche per capire meglio come coordinare queste due legislazioni e, se possibile, semplificare il processo di conformità alle stesse.

La definizione di utente nel DA può in parte sovrapporsi a quella di interessato del GDPR. Questo perché l'utente può chiedere di accedere ai dati che il prodotto o il servizio correlato ha raccolto ed elaborato non solo su di sé, ma anche su altre persone. Facciamo alcuni esempi. Considerando l'art. 4 DA, il contratto di condivisione dei dati è tra l'utente e il titolare dei dati, senza intermediari. L'utente è generalmente colui che ha acquistato, noleggiato, affittato o, comunque, ha la disponibilità immediata del prodotto connesso o del servizio correlato e lo utilizza, in questo caso, per scopi terapeutici. Se l'utente è un consumatore (esperto di tecnologia) e un paziente che utilizza l'IoMT, può chiedere al titolare dei dati di mettere a sua disposizione i dati del suo prodotto connesso o del servizio correlato. I tipi di dati a cui il consumatore/paziente/utente può accedere sono i dati personali, come i dati relativi alla salute o i dati biometrici, i dati non personali come i registri (*log*) relativi al funzionamento e all'attività del prodotto o del servizio connesso e i metadati connessi. Se il consumatore/paziente/utente è l'unico a utilizzare il prodotto connesso o il servizio correlato, i dati personali a cui ha accesso sono i suoi e non ci sono problemi di protezione dei dati, a condizione che la base giuridica su cui ha concordato il trattamento dei suoi dati da parte del prodotto connesso o del servizio correlato sia legittima. Un esempio è quello di un paziente che ha acquistato un esoscheletro connesso per la riabilitazione (prodotto connesso) o che ha bisogno di utilizzare alcuni *exergames* basati sulla realtà aumentata per la riabilitazione (servizio correlato). In questo caso, non ci sarebbe bisogno di preoccuparsi dell'art. 4(12) DA relativo alla base giuridica del GDPR, poiché l'utente è l'unico soggetto interessato. L'art. 4(12) DA deve essere applicato nel caso dell'utente/paziente/consumatore solo se qualcun altro ha utilizzato il dispositivo[80].

Esiste una differenza significativa, invece, per l'applicazione dell'art. 4(12) DA se l'utente è un professionista ai sensi del diritto UE. Il caso potrebbe essere quello di un medico o di un ospedale universitario che utilizza un dispositivo medico, che potrebbe essere un prodotto connesso (IoMT) o un servizio

[77] Considerazione 7 DA.

[78] Come, ad esempio, la definizione di dati personali di cui all'art. 2(3), il trattamento di cui all'art. 2(3), trattamento all'art. 2(7) e di persona interessata all'art. 2(10) DA. 2(10) DA.

[79] Parere congiunto EDPB-EDPS 2/2022 sulla proposta del Parlamento europeo e del Consiglio relativa a norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (Data Act)< https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en, (ultima consultazione 10/01/2025) .

[80] Nell'esempio precedente, i figli degli utenti potrebbero annoiarsi e decidere di giocare con gli *exergame* di realtà aumentata, AR, perché non possono uscire a giocare. Se è necessario registrare dati personali (nome, cognome) o se ci sono sensori collegati che possono percepire la differenza tra l'utente e i suoi figli, si applica l'art. 4(12) DA. In questo caso, se i figli sono minori, non si dovrebbero considerare solo gli articoli 6 e 9, ma anche l'articolo 8 del GDPR relativo al consenso dei minori, con tutte le sue diverse implementazioni nazionali.

correlato. Prendiamo l'esempio di una CAT-SCAN o macchina per le TAC di ultima generazione che opera in un ospedale su più persone ogni giorno dell'anno. In questo caso, sia il titolare dei dati che l'utente sono già contitolari del trattamento ai sensi dell'art. 26 del GDPR per il trattamento dei dati connesso al servizio sanitario[81].

Nell'ambito dei trattamenti previsti dal DA, il ruolo del titolare del trattamento potrebbe essere condiviso tra diversi soggetti. Il primo titolare del trattamento in ordine cronologico è il titolare dei dati sia per l'art. 4 che per l'art. 5 del DA. Il titolare dei dati può essere il fabbricante del prodotto connesso[82], così come il fornitore del servizio correlato[83]. Quindi, per quanto riguarda l'Art. 4 DA, l'utente può diventare un titolare ai sensi del GDPR per questa ulteriore operazione di trattamento dei dati al fine di creare un nuovo prodotto connesso/servizio correlato. Se l'utente è un professionista, per richiedere il riutilizzo dei dati personali dovrà applicare gli articoli 6 e 9 del GDPR. A seconda della forza contrattuale dell'utente e del contesto del contratto di condivisione dei dati, non è da escludere che l'utente possa diventare un contitolare del trattamento dei dati ai sensi dell'art. 26 GDPR. Seguendo l'esempio precedente, i dati raccolti dalla CAT-SCAN possono aiutare i ricercatori dell'ospedale universitario a sviluppare un nuovo e più performante software per l'IoMT per riconoscere specifici tipi di cancro. Potrà dunque esserci un rapporto di contitolarità tra l'ospedale universitario e il fabbricante della macchina CAT-SCAN. Nel caso dell'art. 5, le cose sono più complesse in quanto il terzo/destinatario dei dati viene aggiunto come nuovo titolare ai sensi del GDPR per ulteriori attività di trattamento. Il titolare dei dati nell'Art. 5 DA coincide sempre con il titolare del trattamento originario ai sensi del GDPR. Indipendentemente dal fatto che la richiesta di condivisione dei dati provenga dall'utente o dal destinatario/terzo con l'autorizzazione dell'utente, il titolare dei dati deve avvisare tutti gli interessati (compreso l'utente) dell'ulteriore trattamento dei loro dati personali, che può essere lecito solo se basato sugli articoli 6 e 9 del GDPR e sulle leggi nazionali di attuazione relative alla liceità dell'uso secondario dei dati sanitari.[84] Più sfumata è la posizione del destinatario/terzo in termini di GDPR. Nell'art. 5, prima parte, il destinatario/terzo diviene rilevante dopo la richiesta formale dell'utente. Tuttavia, l'unico contratto regolato dal DA sarà un contratto di condivisione dei dati tra il titolare e il destinatario/terzo. Il contratto di condivisione dei dati conferirà al destinatario dei dati il ruolo di titolare del trattamento ai sensi del GDPR. In seguito, la terza parte e l'utente possono diventare contitolari del trattamento, a seconda del contratto che verrà stipulato per sviluppare un nuovo IoMT o un servizio correlato e di quanto l'utente sarà coinvolto nella creazione del nuovo prodotto o servizio. Ciò è ancora più probabile se si pensa all'art. 5, seconda parte. In questo caso, è il destinatario dei dati che contratta per primo con il titolare dei dati, dopo aver ricevuto un mandato/contratto di rappresentanza da parte dell'utente. Quali potrebbero essere i fattori che spingono un utente a optare per l'art. 5,

[81] In effetti, il titolare dei dati (fabbricante) dovrebbe includere una clausola specifica per i propri pazienti nel documento informativo sulla privacy, specificando quale base giuridica è necessaria per questa specifica forma di trattamento dei dati. Allo stesso modo, anche l'ospedale dovrà valutare la base giuridica del GDPR per il trattamento dei dati. Trattandosi di dati sanitari, l'art. 9 (2) del GDPR sarà la base giuridica principale.

[82] Si veda l'art. 3 (2) DA.

[83] Si veda l'art. 2(6) DA.

[84] Si veda nel caso italiano *supra* sez. 2.2.1.

prima parte o seconda parte, per rappresentare al meglio i propri interessi, se non le capacità tecnologiche e la forza economica del destinatario dei dati/terzo? In entrambi i casi, l'utente non controllerà direttamente i dati raccolti dal destinatario dei dati/terzo.

Se l'utente è anche un soggetto interessato (ad esempio un paziente), ci saranno due attività coordinate per il trattamento dei dati. In primo luogo, ai sensi dell'art. 5, prima parte (figura 1), l'utente/interessato include nel contratto di mandato al destinatario/terzo il proprio consenso al trattamento dei suoi dati personali. In secondo luogo, il titolare dei dati DA dovrà chiedere all'utente/interessato il consenso per l'ulteriore trattamento dei suoi dati in base agli articoli 6 e 9 del GDPR e all'interpretazione delle autorità nazionali sull'uso secondario dei dati sanitari.

Un altro aspetto da chiarire è la posizione dell'utente professionale (l'ospedale universitario, per continuare con lo stesso esempio) nei confronti degli interessati, che dovranno decidere se acconsentire o meno a un ulteriore trattamento dei dati. Nel caso in cui l'informativa sulla privacy dell'utente professionale non contempli questo specifico tipo di uso secondario, l'utente professionale privato potrebbe utilizzare la base del legittimo interesse[85]. Altrimenti, se si tratta di un ente pubblico, dovrà ricontattare gli interessati che potrebbero utilizzare l'IoT sulla base dell'interesse pubblico. Questo ulteriore trattamento dei dati coincide con il contratto di condivisione dei dati nei termini del DA, di cui l'utente non farà parte, ai sensi dell'art. 5 DA. In base all'art. 4 DA, è più semplice qualificare l'utente professionale in termini di GDPR che nella sovraccitata ipotesi. Si tenga l'esempio di un contratto tra un ospedale universitario e un fabbricante. In questo caso, l'ospedale è già il titolare del trattamento di almeno alcune categorie di dati personali degli interessati/pazienti. In questo caso, potrebbe essere necessario aggiornare la propria informativa sulla privacy e chiarire quali tipi di usi secondari possono essere fatti dei dati dei pazienti, e dunque includere i dati personali estratti dai dispositivi IoT prestati ai pazienti per scopi riabilitativi.

[85] Art. 6 (1)(f) GDPR.

ISSN 2284-4503

Tabella 1: Traduzione del quadro DA secondo le interazioni del GDPR.

Soggetti coinvolti nella condivisione dei dati / Contratti che implicano un trattamento dei dati	Contratto tra Uc e T (Art. 4 DA)	Contratto tra Up e T (Art. 4 DA)	(Mandato dell' Uc) contratto tra DD e and T (Art. 5 DA)	(Mandato dell' Up) contratto tra DD e T (Art. 5 DA)
Utente – consumatore (Uc)	Interessato (titolare solo se dati personali appartenenti ad altrə sono condivisi)	Interessato	Interessato	Interessato
Utente – professionista (Up)	Non applicabile (NA)	Titolare dei dati o titolare congiunto	NA	Terza parte o con
Titolare dei dati (T)	Titolare (GDPR)	Joint controller	-	-
Terza parte/Destinatario dei Dati (DD)	NA	NA	Titolare dei dati	Titolare dei dati o titolare congiunto

Verde: Terminologia e contratti DA
Blu: terminologia GDPR

4. Il valore aggiunto del Regolamento EHDS

Gli interventi del legislatore europeo finalizzati a facilitare l'uso secondario dei dati non si sono limitati all'adozione del Data Act che, come detto sopra, ha una applicazione orizzontale, indipendente dal settore di riferimento. Infatti, nello specifico ambito sanitario, la pandemia COVID-19 ha fornito una spinta verso la definizione di regole che consentissero una condivisione di dati sanitari più semplice e immediata, pur nel rispetto del GDPR. In questo contesto, si situa il Regolamento sullo Spazio Europeo dei Dati Sanitari (European Health Data Space - EHDS)[86].

Il regolamento EHDS mira a fornire «uno spazio comune in cui le persone fisiche possano facilmente controllare i propri dati sanitari elettronici. Inoltre, consentirà a ricercatori, innovatori e responsabili politici di utilizzare questi dati sanitari elettronici in modo affidabile e sicuro, preservando la privacy»[87]. L'EHDS previsto dalla Commissione europea è quindi il contesto in cui non solo sarà possibile l'uso primario dei dati sanitari (come l'assistenza sanitaria e l'amministrazione sanitaria), ma si prevede anche un uso secondario dei dati sanitari per promuovere la ricerca e l'innovazione in campo sanitario.

Per quanto riguarda l'uso primario dei dati, il regolamento EHDS prevede una serie di diritti per l'interessato in merito ai propri dati sanitari elettronici personali, in particolare il diritto di accesso «immediatamente [...] gratuito e in forma facilmente leggibile, consolidata e accessibile»[88]. Per migliorare l'uso primario dei dati anche nel caso di servizi transfrontalieri, il regolamento incarica la Commissione europea di istituire una piattaforma centrale per la sanità digitale per fornire servizi e facilitare lo scambio di dati sanitari elettronici.[89] Questo approccio consentirebbe di superare le difficoltà che emergono nella fornitura di assistenza sanitaria transfrontaliera e la frammentazione degli standard digitali applicabili ai servizi sanitari, garantendo agli interessati la possibilità di accedere ai propri dati sanitari elettronici[90].

Va sottolineato che il tipo di dati coperti dal regolamento EHDS è più ampio della definizione di dati sanitari fornita dall'art. 9 GDPR[91]. I dati interessati dalla definizione comprendono sia quelli che rientrano pacificamente nella categoria che già conosciamo con il GDPR, come il contenuti delle cartelle cliniche elettroniche, i dati genomici, i dati sulle cartelle cliniche dei pazienti, ma anche altre categorie di dati che solo indirettamente possono essere qualificati come dati sanitari[92], come i «dati sui fattori

[86] Proposta di regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari, COM(2022) 197 definitivo. Il documento è stato adottato dal Parlamento europeo il 24 aprile 2024, ma attende ancora l'approvazione del Consiglio. L'analisi fornita in questo contributo si basa sull'ultima versione della proposta, disponibile all'indirizzo https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ43/AG/2024/04-09/1299790EN.pdf. [il testo finale del regolamento è al momento in lingua inglese. L'attuale traduzione è ad opera delle autrici].

[87] *Ibidem*, p. 1

[88] Art. 8a Regolamento EHDS.

[89] Art. 12 Regolamento EHDS.

[90] T. PETROCNIK, *Health Data between Improving Health(Care) and Fuelling the Data Economy,* in *Technology and Regulation*, 2022, 124.

[91] Si veda il precedente par. 3.

[92] I dati sanitari elettronici inclusi nel Regolamento EHDS possono essere sia personali che non personali, poiché alcune delle informazioni raccolte non si riferiscono a una persona fisica identificata o identificabile (ai sensi dell'art. 4(1) del GDPR.

che hanno un impatto sulla salute, compresi i determinanti socioeconomici, ambientali e comportamentali», nonché «i dati amministrativi relativi all'assistenza sanitaria, compresi i dati relativi alle erogazioni, alle richieste di rimborso e ai rimborsi» e anche «i dati provenienti da applicazioni per il benessere (*wellness application*)», nonché «i dati aggregati sui bisogni di assistenza sanitaria, sulle risorse destinate all'assistenza sanitaria, sulla fornitura e sull'accesso all'assistenza sanitaria, sulla spesa e sul finanziamento dell'assistenza sanitaria»[93]. Ad esempio, per quanto riguarda i dati generati dai dispositivi di wellness, è possibile che questi dati diventino dati sanitari se vengono elaborati per identificare specifiche condizioni di salute o se vengono elaborati insieme ad altri dati relativi alla salute[94]. Un esempio potrebbe essere quello dei dati raccolti da un dispositivo wellness relativi all'attività fisica di un individuo, che possono diventare dati sanitari se vengono collegati alle prescrizioni mediche di un dottore relative alle strategie per ridurre il livello di colesterolo. Come sottolineato da una valutazione dell'iniziale proposta da parte di EDPB e European Data Protection Supervisor (EDPS)[95], è chiaro che i requisiti di qualità e le caratteristiche dei dati relativi alla salute generati dalle applicazioni wellness sono inferiori a quelli generati dai dispositivi medici.

Questo ampio concetto di dati sanitari è anche alla base del secondo obiettivo dell'EHDS, ovvero la possibilità di sfruttare i dati raccolti «al fine di creare valore e qualità scientifica, innovativa e sociale»[96], cioè, per l'uso secondario dei dati[97]. L'EHDS stabilisce una serie di obblighi e strumenti per raggiungere questo obiettivo. Per raggiungere tale obiettivo, peraltro, il regolamento definisce una costellazione di attori e di relazioni che vanno a sovrapporsi con il quadro sopra definito dal GDPR.

Un passo preliminare è la creazione del catalogo nazionale dei dataset sanitari[98] che include la fonte e la natura dei dati sanitari elettronici ospitati da enti che offrono servizi o svolgono attività di ricerca nel settore sanitario o assistenziale, qualificati come *titolari di dati sanitari* dal regolamento. In questo caso, la definizione comprende sia enti pubblici, come ospedali, centri di ricerca e agenzie, sia sviluppatori e produttori di applicazioni IoMT e wellness[99]. L'organismo incaricato di ricevere queste informazioni e di creare il catalogo nazionale dei set di dati è il neonato *Organismo responsabile dell'accesso ai dati sanitari* (Data Access Body, *DAB*). Il DAB è un'autorità indipendente istituita a livello nazionale[100]

[93] L'art. 33 Regolamento EHDS elenca diciassette categorie di dati che possono essere raccolti. Queste categorie di dati sono quelle che i titolari dei dati sono tenuti a rendere disponibili per l'uso secondario.

[94] Le applicazioni per il benessere sono qualificate come «qualsiasi apparecchio o software destinato dal fabbricante a essere utilizzato da una persona fisica per il trattamento di dati sanitari elettronici specificamente per fornire informazioni sulla salute di singole persone, o per la fornitura di cure per scopi diversi dalla fornitura di assistenza sanitaria», cfr. Art. 2, paragrafo 2, lettera aea), del regolamento EHDS.

[95] Parere congiunto EDPB-EDPS 03/2022 sulla proposta di regolamento sullo spazio europeo dei dati sanitari, 12 luglio 2022, pag. 12, disponibile su https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf.

[96] Si veda il considerando 39b del regolamento EHDS.

[97] Si noti che il considerando 39 regolamento EHDS giustifica espressamente questo approccio, affermando che i dati trattati per uso secondario "dovrebbero essere sufficientemente ampi e flessibili per soddisfare le esigenze in evoluzione degli utenti dei dati sanitari". Si veda P. TERZIS, *Compromises and Asymmetries in the European Health Data Space*, in *European Journal of Health Law*, 2022,30 ,345.

[98] Art. 37 (1) (q) (i) Regolamento EDHS.

[99] Art. 2(2)(y) Regolamento EHDS.

[100] Art. 36 del Regolamento EHDS.

con il compito di moderare l'accesso a tali dataset per gli *utenti*[101]. I titolari dei dati sanitari sono tenuti a informare il DAB a livello nazionale, seguendo le regole relative agli elementi informativi minimi che descrivono i loro set di dati[102]. Questa prima parte della procedura prende in considerazione anche i diritti di proprietà intellettuale e i segreti commerciali che possono essere applicabili agli insiemi di dati: l'art. 52 del Regolamento EHDS prevede che il DAB adotti misure per tutelare i diritti dei titolari dei dati sanitari. La base giuridica del trattamento dei dati effettuato dal titolare per condividere i dati con il DAB è l'art. 6 (1)(c) GD. 6 (1)(c) GDPR, ossia il fatto che il «trattamento è necessario per adempiere a un obbligo legale al quale è soggetto il titolare del trattamento». Allo stesso tempo, l'EHDS soddisfa anche i requisiti stabiliti per il trattamento dei dati sanitari, ovvero l'art. 9(2)(i) e (j), in quanto il trattamento è necessario per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica o storica o per finalità statistiche ai sensi dell'art. 89(1) GDPR sulla base del diritto dell'Unione o degli Stati membri[103].

La seconda fase della procedura è la richiesta di dati da parte degli utenti dei dati sanitari. Va sottolineato che la definizione di utente dei dati sanitari non coincide con quella contenuta nel DA, poiché l'EHDS definisce gli utenti dei dati sanitari come qualsiasi persona fisica o giuridica che possa giustificare l'accesso ai dati sanitari elettronici per uso secondario. Essi possono presentare due tipi di richieste: una richiesta di dati oppure una domanda di accesso ai dati, in entrambi i casi basate sugli scopi elencati nell'art. 34 del Regolamento EHDS[104]. La differenza tra i due tipi di richiesta sta nella tipologia di dati a cui si può accedere. Dopo una richiesta di dati, l'utente riceverà dal titolare dei dati sanitari la versione anonimizzata e statistica dei dati[105], senza fornire l'accesso ai dati che sono stati utilizzati per fornire la risposta alla richiesta[106]. Nel secondo caso, la domanda di accesso ai dati sarà esaminata dal DAB, che avrà il compito di decidere se concedere o meno l'accesso ai dati e di rilasciare - in caso affermativo - un cosiddetto permesso di accesso ai dati[107]. In questo caso, l'utente dei dati deve anche giustificare la sua richiesta con una base giuridica tra quelle di cui all'art. 6(1)(e) e (f) GDPR, ossia che

[101] Si noti che nel caso di dati sanitari elettronici non personali, il titolare dei dati ha la possibilità, attraverso il controllo della progettazione tecnica di un prodotto e dei servizi correlati, di rendere disponibili alcuni dati direttamente all'utente dei dati, ai sensi dell'art. 2 (2(y)(b) Regolamento EHDS.

[102] L'articolo 55 regolamento EHDS attribuisce alla Commissione la responsabilità di individuare tali elementi minimi di informazione attraverso atti di esecuzione.

[103] Considerando 37 regolamento EHDS.

[104] Si noti che l'Art. 34 Regolamento EHDS elenca le seguenti finalità: ad attività per motivi di pubblico interesse nell'ambito della sanità pubblica e della medicina del lavoro; sostegno agli enti pubblici nello svolgimento dei loro compiti; produzione di statistiche ufficiali relative ai settori della salute o dell'assistenza; attività di istruzione o insegnamento nei settori della salute o dell'assistenza; ricerca scientifica relativa ai settori della salute o dell'assistenza, comprese le attività di sviluppo e innovazione di prodotti e servizi e la formazione, il collaudo e la valutazione di algoritmi, compresi i dispositivi medici, i dispositivi medico-diagnostici in vitro, i sistemi di intelligenza artificiale e le applicazioni digitali per la salute; miglioramento dell'erogazione delle cure, ottimizzazione dei trattamenti e fornitura di assistenza sanitaria personalizzata.

[105] Art. 47(1) Regolamento EHDS.

[106] Art. 47 Regolamento EDHS richiede una serie di informazioni da includere nella domanda, come una spiegazione dettagliata dell'uso previsto dei dati sanitari elettronici, una descrizione dei dati sanitari elettronici richiesti, il loro formato e la fonte dei dati, una descrizione del contenuto della statistica, una descrizione delle garanzie previste per prevenire qualsiasi uso improprio dei dati sanitari elettronici, una descrizione di come il trattamento sarebbe conforme all'articolo 6(1) del GDPR.

[107] Art. 46 Regolamento EHDS.

il trattamento dei dati è effettuato nel pubblico interesse o ai fini dei legittimi interessi del responsabile del trattamento. Nel primo caso, il Regolamento EHDS indica già che l'utente deve fare riferimento a un'altra legge dell'UE o nazionale che gli impone di trattare i dati sanitari personali per adempiere ai suoi compiti[108]. Nel secondo caso, sarà l'autorizzazione al trattamento dei dati rilasciata dal DAB a definire le condizioni per l'accesso, in particolare i tipi e il formato dei dati sanitari elettronici a cui si accede, lo scopo per cui i dati sono resi disponibili, la durata dell'autorizzazione, le condizioni tecniche per l'ambiente di trattamento sicuro, nonché le tariffe che l'utente dei dati sanitari deve pagare.
Quando viene rilasciata l'autorizzazione, l'utente dei dati si coordinerà con il DAB per accedere ai dati attraverso un ambiente di elaborazione sicuro senza che i dati lascino l'archivio[109]. L'utente dei dati sanitari diventerà il responsabile del trattamento, mentre il DAB agirà come incaricato del trattamento per i dati resi disponibili nell'ambito di una determinata autorizzazione[110].
Di conseguenza, il processo per la gestione dei dati sanitari in caso di uso secondario segue le fasi presentate nella Figura 4.

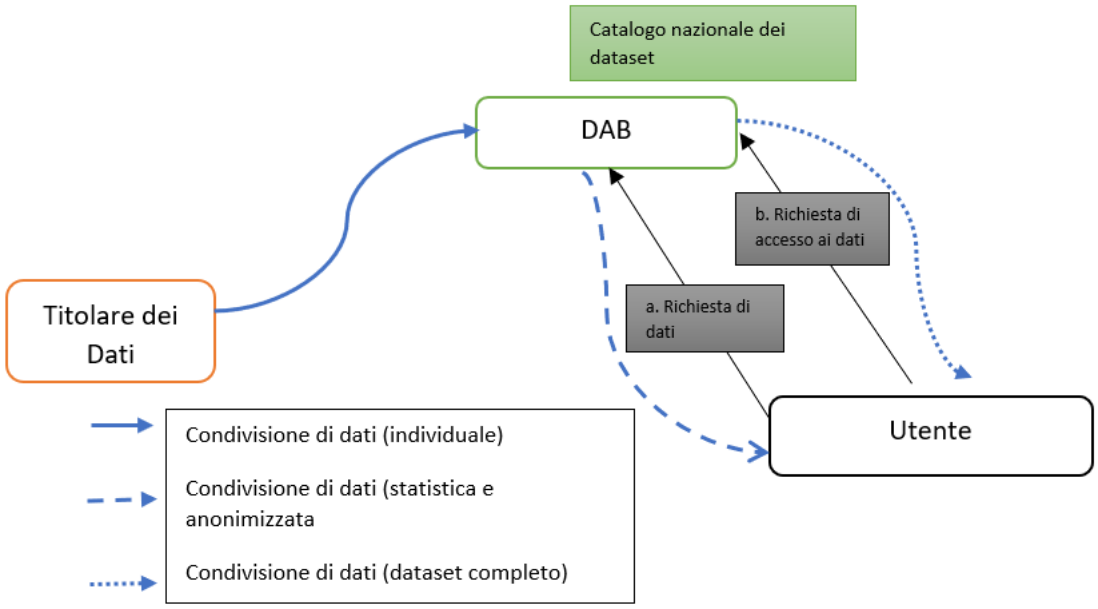

Figura 4. La condivisione dei dati sulla base dell'EHDS

Se traduciamo questo processo nel contesto dell'IoMT, dobbiamo chiarire se e come i produttori di dispositivi medici (o di software) rientrano nella categoria dei titolari di dati sanitari secondo il regolamento EHDS ed eventualmente possano anche qualificarsi come potenziali utenti. Come già accennato, la definizione di titolari di dati sanitari è abbastanza ampia da comprendere non solo i produttori

[108] Considerando 37 del regolamento EHDS.
[109] Art. 50 Regolamento EHDS.
[110] Art. 51 Regolamento EHDS.

di dispositivi medici, ma anche molte altre applicazioni sanitarie che, pur non rientrando nella categoria dei "soggetti che svolgono attività di ricerca", raccolgono dati sanitari che possono potenzialmente supportare tale ricerca[111]. Pertanto, in linea di principio, i produttori di dispositivi medici saranno qualificati come titolari di dati e tenuti a condividere i loro set di dati con il DAB.

Per quanto riguarda l'utente, la definizione è ancora più ampia, in quanto richiede solo che la persona fisica o giuridica sia in grado di soddisfare una o più delle finalità elencate nel suddetto art. 34 del regolamento EHDS, senza richiedere che l'utente dei dati appartenga alla sfera sanitaria. È chiaro che i produttori di IoMT saranno capaci di giustificare gli scopi delineati nell'art. 34(1)(e)(i) e (ii) del regolamento EHDS. Ad esempio, lo scopo di formare, testare e valutare algoritmi si riferisce già all'applicazione in dispositivi medici, sistemi di intelligenza artificiale e applicazioni di salute digitale, contribuendo alla salute pubblica o alla sicurezza sociale.

In base alle definizioni, quindi, un fabbricante che voglia sviluppare un IoMT può compilare una richiesta di accesso ai dati per utilizzare i dati precedentemente raccolti da un diverso titolare dei dati, ad esempio per addestrare l'algoritmo utilizzato nell'IoMT[112]. In questo modo, la richiesta di accesso ai dati potrebbe evitare al fabbricante la necessità di chiedere il consenso di ciascun soggetto interessato, così come la necessità di identificare un progetto specifico per rientrare nelle condizioni definite per l'applicazione della c.d. "esenzione per la ricerca scientifica" già prevista dall'art. 9(2)(j) GDPR[113].

Dati i rischi che possono essere associati all'uso secondario dei dati[114], le salvaguardie incluse nel regolamento EHDS dovrebbero essere applicate rigorosamente. In particolare, il ruolo di monitoraggio del DAB sarà fondamentale. La valutazione della richiesta di accesso ai dati richiederà non solo un mero controllo formale dello scopo dell'uso secondario tra quelli elencati nell'art. 34 dell'EHDS, ma anche un'analisi sostanziale della documentazione richiesta dall'art. 45(2) dell'EHDS.

A differenza dell'analisi precedente per la DA, l'EHDS non prevede accordi contrattuali specifici tra il titolare dei dati sanitari e l'utente dei dati sanitari[115]. Le relazioni tra gli attori coinvolti sono definite

[111] P. TERZIS, *Compromises and Asymmetries in the European Health Data Space*, in *European Journal of Health Law*, 30, 2022, 345.

[112] Si noti che in questo caso il Regolamento EHDS non prevede alcun divieto per lo sviluppo di prodotti direttamente concorrenti, come quello incluso nella DA.

[113] Ai sensi dell'art. 89 GDPR, il trattamento per la ricerca scientifica «è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure adeguate e specifiche per salvaguardare i diritti fondamentali e gli interessi dell'interessato». Si noti che queste misure di salvaguardia non sono definite e possono essere soggette a interpretazione, vedi CIARA STAUNTON ET AL., *Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research*, in *Frontiers in Genetics*, 13, 2022, https://www.frontiersin.org/articles/10.3389/fgene.2022.719317, consultato il 18 gennaio 2024.

[114] L. MARELLI, G. TESTA, I. VAN HOYWEGHEN, *Big Tech Platforms in Health Research: Re-Purposing Big Data Governance in Light of the General Data Protection Regulation's Research Exemption*, in *Big Data & Society*, 8, 2021, 20539517211018783; P. TERZIS *op. cit.*; S. SLOKENBERGA, *op.cit*.; S. SLOKENBERGA, O. TZORTZATOU and J. REICHEL (a cura di), *GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation across Europe*, Cham, 2021, https://link.springer.com/10.1007/978-3-030-49388-2 (ultima consultazione il 10/01/2025).

[115] Fa eccezione il caso di accordi contrattuali relativi a dati contenenti informazioni o contenuti protetti da diritti di proprietà intellettuale o segreti commerciali. Questa ipotesi è prevista dall'art. 33a (1) (c) del Regolamento EHDS, dove si specifica anche che la Commissione può raccomandare termini contrattuali modello non vincolanti per tali accordi.

dal regolamento stesso, basandosi in ogni caso sul quadro del GDPR. Se ci concentriamo sulle attività di trattamento, la tabella 2 chiarisce il ruolo di ciascun attore.

Tabella 2: Traduzione del quadro EDHS secondo le interazioni del GDPR.

Tipo di trattamento /Attori coinvolti	Condivisione del dataset per il catalogo nazionale	Gestione del catalogo nazionale dei dataset	Condivisione dei dati previa richiesta di accesso	Trattamento di pseudonimizzazione dei dati
Titolare dei dati	Titolare dei dati	-	-	-
Utente	-	-	Destinatario dei dati	Titolare dei dati
DAB	Destinatario dei dati	Titolare dei dati	Titolare dei dati	Titolare dei dati

Verde: Terminologia e relazioni Regolamento EHDS
Blu: terminologia GDPR

5. Conclusioni: che cosa potrebbe accadere in Italia

Gli IoMT avranno sempre maggiore importanza nel futuro prossimo, dunque appare necessario comprendere in che modo i dati sanitari utilizzati per il loro sviluppo possono essere legittimamente ottenuti e trattati. Il DA e il regolamento EDHS si applicano all'IoMT, ma individuano modalità e strumenti giuridici diversi per la condivisione dei dati. Poiché il regolamento EDHS non ha ancora concluso l'iter legislativo, il DA è attualmente l'unico strumento legislativo applicabile nelle more dell'implementazione del regolamento EHDS stesso.
È quindi importante comprendere le differenze tra queste due ultime legislazioni e i loro diversi obbiettivi, i quali consentono di ottenere risultati diversi. Si tratta di un primo elenco non conclusivo delle caratteristiche positive e negative di queste due legislazioni, che potrà essere aggiornato e perfezionato nel prossimo futuro.
Innanzitutto, vale la pena di sottolineare alcune analogie. La prima è *ratione materiae*: il regolamento EDHS e il DA possono applicarsi agli stessi insiemi di oggetti. In questo articolo ci siamo concentrati sui dispositivi IoMT, che sono destinati a diventare sempre più utilizzati non solo in ospedale ma anche in ambiente domestico come supporto alla terapia o come terapia a distanza. Un'altra somiglianza è la centralità del titolare dei dati, che, convertendo la terminologia sia del DA che del regolamento EDHS secondo il vocabolario del GDPR si traduce nel titolare del trattamento. Questo ruolo influisce sui compiti e sugli obblighi del titolare dei dati sia nel regolamento EDHS che nel DA. Nel DA, il titolare dei dati è il destinatario della richiesta dell'utente e oppure un destinatario/terzo che agisce su autorizzazione

e in rappresentanza dell'utente[116]. Nel regolamento EHDS, il titolare dei dati è tenuto a mettere a disposizione il proprio dataset all'organismo di accesso ai dati (DAB), successivamente, la richiesta dell'utente al DAB permette di trasferire o consentire l'accesso ai dati. Sia nel caso del regolamento EHDS che del DA, è il titolare dei dati il punto di riferimento per l'uso secondario dei dati.

Le differenze riguardano sia le finalità per cui un attore chiede di accedere ai dati, sia le modalità con cui avviene l'operazione di trasferimento.

Secondo il regolamento EHDS, lo scopo principale dell'uso secondario dei dati è la ricerca e, eventualmente, lo sviluppo di dispositivi medici e non (strettamente) medici (ad esempio, app per il benessere non certificate come dispositivi medici). Ciò giustifica l'accesso a una quantità molto maggiore di dati che possono essere resi disponibili per corroborare la ricerca scientifica. Questa quantità di dati è essenziale per la progettazione dell'IoMT, perché l'MDR richiede che i dispositivi medici abbiano prove cliniche della loro sicurezza e non danneggino i pazienti attraverso i dati clinici[117]. Un'altra caratteristica è che il regolamento EHDS prevede una procedura più centralizzata e soggetta a controllo amministrativo. Gli organi amministrativi incaricati di esercitare i compiti del DAB richiedono l'attuazione da parte degli Stati e un coordinamento che probabilmente sarà rallentato nelle prime fasi di applicazione. È probabile che l'attuazione del regolamento EHDS richieda più anni di quelli specificati nel testo legislativo. Una volta implementato, consentirà di accedere più facilmente a una maggiore quantità di dati rispetto al DA.

Al contrario, il DA ha una funzione di regolamentazione orizzontale e ha lo scopo di creare dispositivi IoT in generale, ma anche dispositivi IoMT, in assenza di una legislazione specifica sull'IoMT. Tra le caratteristiche positive di questa normativa c'è l'approccio decentralizzato, derivante dall'iniziativa autonoma di attori privati o anche pubblici (ad esempio, un ospedale universitario che vuole sviluppare un nuovo IoMT o un servizio correlato attraverso i suoi gruppi di ricerca). La caratteristica principale del DA è la regolamentazione tramite contratti. Si tratta, in linea di principio, di un processo più flessibile rispetto a quello basato sull'amministrazione centralizzata adottata invece nel regolamento EHDS. Tuttavia, il fatto che tutto sia regolato attraverso contratti potrebbe anche aggiungere alcune difficoltà nel rendere il mercato veramente competitivo e nell'applicare il principio del libero flusso dei dati. Nonostante l'art. 13 DA affermi la nullità delle clausole vessatorie, la stesura e la gestione di tutti questi rapporti (quasi) triangolari sarà un costo nascosto che non molti utenti o terzi potrebbero essere in grado di sostenere, soprattutto se il dispositivo IoMT è prodotto da un importante fabbricante di MD. Questo squilibrio potrebbe emergere anche negli obblighi relativi ai diritti di proprietà intellettuale che l'utente o la terza parte/destinatario dei dati dovrebbe rispettare. Inoltre, l'utente o la terza parte deve avere accesso a diversi IoMT o avere la disponibilità di un IoMT, che crea una notevole quantità di dati, per raccogliere una quantità di dati sufficiente a identificare i pattern e ad addestrare un algoritmo. Un'altra variabile che potrebbe influire negativamente sul successo della DA dipende dalla forza di mercato, rispettivamente, del titolare dei dati, dell'utente e della terza parte. La combinazione delle norme sul DA e dei principi del GDPR sulla portabilità dei dati sono le uniche norme che possono essere

[116] Articoli 4 e 5 prima parte DA.
[117] Cfr. *supra* sez. 3.

applicate direttamente anche dai produttori di IoMT che non sono dominanti sul mercato e dai ricercatori medici che vogliono commercializzare i risultati dei loro studi. Pertanto, sino ad ora, il Data Act è la disciplina più completa, insieme al GDPR, da utilizzare per portare innovazione nel settore IoMT.
Un ulteriore quesito che si pone è se davvero le regole del GDPR e le relative applicazioni nazionali, inclusa quella italiana, avranno ancora una rilevanza all'atto pratico una volta che il regolamento EHDS sarà attuato?[118]
Infatti, la base giuridica per la raccolta dei dati nel regolamento EHDS sia per garantire l'uniformità e la portabilità dei dati dei singoli cittadini sia per l'uso secondario ai fini di ricerca non è più il consenso, ma l'interesse pubblico.
In realtà, anche il DA, per quanto la sua natura sia di rimedio di natura contrattuale, nel senso inglese del termine, e quindi basato sul consenso (espressione della volontà contrattuale), ha comunque una parte (il capitolo V) che riguarda la condivisione "coatta" di dati in caso di calamità o necessità impreviste come la pandemia Covid[119]. In questo contributo vi si è fatto solo un rapido cenno per via della sua natura residuale ma, comunque, questa esiste. Allo stesso tempo, anche rimanendo nei confini dei contratti di condivisione dei dati, la logica del GDPR di protezione del diritto alla privacy e riservatezza si scontra contro il principio di accesso ai dati. A prima vista, si potrebbe dire che il DA altro non è che l'applicazione del principio di trasparenza dell'Art.15 GDPR, ma non sarebbe del tutto vero poiché gli IoMT di oggi non hanno ancora raggiunto un livello di applicazione automatica di *privacy by design e by default* del loro funzionamento tale da consentire un diritto di accesso generalizzato senza automaticamente ledere i diritti di terzi. Questo limite si riscontra anche dall'attenzione posta nel quadro del DA al rispetto dei diritti di proprietà intellettuale che potrebbero emergere: in quanto potrebbero verificarsi atti di c.d. reverse engineering quando si accede ai dati del prodotto o del servizio collegato. Queste sono le ipotesi sia dell'Art. 4 DA quando l'utente è professionista sia anche dell'Articolo 5, in entrambe le tipologie di contratti di condivisione dei dati elencati qualora vi siano dati di terzi coinvolti.
Ora che entrambe le legislazioni sono approvate ci si deve chiedere quale sarà il percorso di coesistenza di queste norme tra di loro e con il GDPR. In sé, la convivenza tra DA e il regolamento EHDS sarebbe pacifica perché hanno *rationes* diverse nonostante gli oggetti possano coincidere. Appare più complicato ipotizzare come il GDPR si affiancherà nella pratica alle modalità di applicazione del DA e del regolamento EHDS.
Si può ipotizzare una prima fase in cui sia applicabile nei fatti solo il DA anche per il riuso dei dati sanitari (con tutte le limitazioni del caso già elencate *supra*)[120]. In questo frangente, la novella degli articoli 110 e 110 bis, stante l'eliminazione dell'obbligo di consultazione preventiva del garante salvo dubbi o impossibilità di garantire la protezione dei dati personali degli interessati, non si discosterebbe così tanto dalla pratica attuale specialmente per gli studi retrospettivi. Quello che cambierebbe è un dato tecnologico concernente la fonte dei dati: riprendendo gli esempi fatti prima, il gruppo di ricerca di un ospedale universitario non avrebbe solo a disposizione le cartelle cliniche ma anche i dati delle macchine utilizzate per analisi e referti per dedurre ulteriori dati e integrando i c.d. *real world data* che

[118] Il MDR infatti non preoccupa sotto questo aspetto in quanto si configura come una legislazione di conformità dei dispositivi medici e quindi si occupa solamente della sicurezza materiale del prodotto.
[119] Si veda il capo V DA.
[120] Questa sembra l'ipotesi più probabile perché per la completa attuazione del regolamento EHDS servirà tempo.

sono nell'immediata disponibilità di una struttura. Si renderebbe comunque necessario aggiornare le informative sulla privacy su questa modalità di estrazione di dati personali o tramite i quali è possibile identificare una persona. Una delle difficoltà emergenti sarebbe quella che la terminologia del DA e quella del GDPR sono in parte sovrapponibili, soprattutto per quanto concerne il ruolo di titolare dei dati ma per altre no, come terza parte o destinatario dei dati. I dati della tabella 1 forniscono una griglia di lettura per i responsabili legali degli ospedali per non confondere i rispettivi ruoli a seconda del contesto di applicazione.

Stante l'attuale mancanza di casi sull'applicazione pratica delle due legislazioni, DA e GDPR, si possono fare soltanto delle ipotesi, ma l'esito non dipenderà dal dato normativo in sé, quanto dall'interpretazione delle norme che verrà fatta. Se gli operatori del settore sanitario propenderanno verso una cautela smisurata anche rispetto alla effettiva delicatezza in concreto dello studio (o futuro prodotto/ servizio da realizzare) chiedendo la consultazione preventiva al garante in maniera sistematica, saranno soprattutto le regole del GDPR a diventare un ostacolo alla ricerca scientifica e biomedica. Dall'altro lato, non facendo ricorso generalizzato all'autorizzazione preventiva si "appalta" ai comitati etici territoriali il fardello di valutare la bontà di progetti di ricerca ulteriore e innovativi. Gli unici problemi che sembrano essere più concreti in questa sub-ipotesi sono: i) la difformità delle interpretazioni anche per casi analoghi e ii) una prevalenza della valutazione dell'aspetto del GDPR a discapito di studi che possano essere fortemente innovativi e con un carattere imprenditoriale non così secondario come in passato. La prevalenza nella valutazione delle norme del GDPR rispetto ad altre più recenti deriverebbe probabilmente dal fatto che i comitati etici si sono specializzati ad applicare queste norme e non altre. A questo si deve aggiungere l'ulteriore livello di complessità richiesto agli IoMT in applicazione del MDR, in quanto il processo di valutazione della conformità dovrà tener conto anche delle regole ivi indicate. Dunque, eventuali IoMT e software medici creati con i dati a cui si è avuto accesso dovranno essere sottoposti a indagini cliniche molto rigorose al fine di ottenere il marchio CE di conformità[121]. Ne consegue che sarà sempre meno appetibile la scelta di predisporre prototipi esclusivamente per ricerca pura in ambito medico, quanto, piuttosto, sarà definita la scelta di creare prototipi in vista di una commercializzazione sul mercato per cui, per ottenere la conformità, è necessario prepararsi ab origine a un processo lungo e costoso.

Con l'effettiva attuazione del regolamento EHDS, quello che si avrà probabilmente è che la *ratio* della ricerca a fini scientifici e statistici dell'Art. 9(2)(j) GDPR sarà in realtà assorbita dalla ragione di interesse pubblico. Il focus quindi si sposterà sull'amministrazione (DAB) che concederà accesso ai dati sulla base della richiesta e l'applicazione delle misure tecniche organizzative dell'Art. 89 e richiamate dall'GDPR Art. 9(2)(j) GDPR per contemperare alla necessità di tutela degli interessati. Questo spostamento del ruolo di controllo verso il DAB porterebbe a limitare, se non annullare, il ruolo del Garante e dei comitati etici per l'autorizzazione all'accesso ai dati. La rilevanza rimarrebbe tuttavia a monte dell'accesso e quindi nell'autorizzazione allo studio preliminare volto a indagare una condizione clinica e, eventualmente, a curarla tramite IoMT di nuova generazione.[122] Il potenziale scontro che potrebbe creare uno

[121] Si veda il Capo VI su valutazione clinica e indagini cliniche nel MDR.

[122] Ciò è confermato anche dal fatto che, ai sensi dell'art. 65 EHDS, il ruolo dei garanti nazionali è limitato all'applicazione del c.d. diritto di *opt out* previsto dall'art. 71 EHDS. Indicando comunque che potrà esservi collaborazione anche con i DAB nell'ambito delle rispettive competenze.

stallo nell'applicazione del regolamento EHDS è il permanere del consenso come base giuridica primaria per gli usi secondari dei dati sanitari della disciplina nazionale a fronte dell'obbligo trasversale di interesse pubblico di condivisione dei dati ai fini di creare cataloghi di dataset per i DAB. In questo caso dunque lo scenario potrebbe essere il seguente: le regole dell'art 110 e 110 bis novellate rimarrebbero nel novero delle disposizioni richiamate da coloro che presentano una richiesta a un comitato etico (o autorizzazione preventiva facoltativa al garante) ma se le garanzie *ex* Art. 89 GDPR sono state ben implementate, sia i comitati che il garante potrebbero essere portati ad approvare la richiesta. Di conseguenza, la garanzia sul rispetto delle misure tecniche organizzative di protezione dei dati ricadrebbe in parte sui DAB, ma soprattutto sulla serie di soggetti che deve fornire i dati per i cataloghi di dataset e quindi non solo le strutture private o pubbliche ospedaliere ma anche produttori di dispositivi medici e di dispositivi e-health come le applicazioni di wellness.

Questo contributo ha portato quindi una prima descrizione approfondita dei plessi normativi applicabili all'IoMT, vale a dire il GDPR, l'MDR e i prossimamente applicabili il DA e l'EHDS. L'obbiettivo è stato quello di cominciare a tracciare una via e un percorso di riferimento per capire come i plessi normativi presentati interagiscano tra di loro. In particolare, si è tentato di delineare possibili scenari futuri di convivenza, soprattutto con il GDPR e con il DA, che sarà già applicabile dal 2025, mentre invece l'EHDS richiederà una implementazione più lunga e complessa, non solo dal punto di vista amministrativo ma anche per la creazione di infrastrutture che garantiscano la sicurezza nelle procedure di accesso ai dati. L'analisi ha mostrato che le nuove regole sul riuso dei dati presentano delle incongruenze tra la disciplina del DA e il GDPR. Si è cercato di investigare quali potrebbero essere gli scenari possibili in Italia per un'armonica convivenza di DA e GDPR nel quadro dell'uso negli IoT medici, immaginando degli scenari ipotetici. Attraverso l'analisi dei ruoli dei soggetti principali nel GDPR e DA si è visto che, nonostante una formale subordinazione al GDPR, il DA in realtà offre una logica di condivisione dei dati che, anche se non del tutto incompatibile con quella del GDPR diviene complessa da gestire in termini di compliance dal lato del fabbricante IoT medico. Riprendendo la tabella 1, si comprende che spesso un soggetto per il DA può ricoprire il ruolo di diversi soggetti in termini di GDPR. Allo stesso modo, l'applicazione del DA rischia di aggiungersi al puzzle già abbastanza confuso e contraddittorio delle regole italiane sul riuso dei dati sanitari, solo di recente leggermente modificato con una decentralizzazione verso i comitati etici territoriali. Centrale sarà l'atteggiamento con cui, chi disegna studi clinici, utilizzerà le norme sulla condivisione dei dati del DA e su come i comitati etici territoriali valuteranno l'uso di tali regole insieme a quelle del GDPR. Se l'applicazione sarà eccessivamente cauta anche nel contesto di riuso dei dati sanitari finalizzato a creare nuovi prototipi di oggetti IoMT, il GDPR rischia di diventare più un ostacolo alla ricerca scientifica non sempre giustificata più che una forma legittima di protezione dei diritti degli individui. L'EHDS risponde meglio alle richieste dei ricercatori biomedici per la qualità, quantità dei dati e sicurezza agli interessati quando ai loro dati viene dato accesso a terzi. Tuttavia, l'EHDS è sottoposto a una implementazione che già si presenta lunga e difficoltosa da un punto di vista amministrativo e di effettiva operatività (cfr. sez. 4). Quello che è certo, è che la ricerca più innovativa non passa solo dal riuso dei dati dei pazienti, ma anche tramite la valutazione di come le apparecchiature IoMT già presenti nell'ambiente sanitario funzionino al fine di creare nuovi strumenti e servizi correlati. È necessaria quindi un'opera di formazione del personale ricercatore come

dei membri dei comitati etici alle potenzialità di un'applicazione delle regole della *digital policy* e della protezione dei dati personali funzionali alla ricerca.

ISSN 2284-4503