

Il diritto alla *privacy* nello stato di emergenza. Riflessioni sull'applicazione della telemedicina quale possibile tecnologia per contrastare la diffusione del Covid-19

di

Francesca Filosa*

SOMMARIO: 1. Premessa. 2. Il trattamento dei dati necessario per la protezione da gravi minacce per la salute. 3. Tecnologie avanzate al banco di prova. 4. Considerazioni tecniche conclusive.

1. Premessa

Viviamo in un'epoca che è stata definita «l'era dei dati, considerata un movimento rivoluzionario per l'innovazione tecnologica e i meccanismi di ricerca»¹. Abbiamo infatti a disposizione enormi quantità di dati, Big Data², grazie alle tecnologie digitali e ai sistemi di ricerca e comunicazione sempre più globalizzati, tanto da aver creato un modello di innovazione "datocentrico". I dati generano conoscenza e, a seconda della situazione in cui vengono utilizzati, assumono un valore diverso: possono essere valorizzati in tanti modi e per motivi diversi e proprio per il carattere della loro molteplicità sono interessanti oggetto di analisi. Analizzando i dati raccolti è possibile creare dei servizi personalizzati e ottimizzati, basati sull'uso dell'intelligenza artificiale³, che agisce attraverso algoritmi⁴ in grado di attingere a vaste fonti di dati⁵

* Dottoranda di ricerca in Scienze politiche, Università degli Studi Roma TRE.

¹ Cfr. S. LEONELLI, *La ricerca scientifica nell'era dei Big Data. Cinque modi in cui i Big Data danneggiano la scienza, e come salvarla*, Meltemi editore, Milano, 2018, p. 10.

² Una definizione di Big Data è fornita da S. CALZOLAIO, *Protezione dei dati personali*, in *Digesto delle discipline pubblicistiche*, Milano, Utet Giuridica, Wolters Kluwer, 2017, p. 599, il quale afferma che per Big Data, si intende «una situazione in cui si hanno a disposizione quantità enormi di dati (volume) di contenuto e provenienza variegata (*variety*), alta e rapida capacità di analisi (*velocity*), cui più di recente si è aggiunto il profilo della qualità e affidabilità dei dati (*veracity*) e del loro valore (*value*). Per un'analisi più dettagliata e tecnica, si veda G. D'ACQUISTO - M. NALDI, *Big Data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Giappichelli Editore, Torino, 2017, p. 5.

³ Per intelligenza artificiale si intendono «quei sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi». *Intelligenza artificiale e diritto*, in AA. VV., F.

sulle persone e sulle loro condizioni di vita⁶. È infatti sempre più frequente l'uso di applicazioni, più comunemente "app", scaricabili sui *devices*, in particolare *smartphones* e *smartwatches*, che tracciano i passi, la distanza, i percorsi effettuati, monitorano continuamente il battito cardiaco calcolando con precisione le calorie bruciate; tracciano finanche le fasi del sonno e sono inoltre connessi attraverso il GPS. I dati che questo tipo di applicazioni raccolgono per poter offrire il servizio richiesto riguardano la nostra persona e il nostro corpo. Si tratta di dati che il Regolamento UE 2016/679⁷, d'ora in avanti anche Reg. UE 2016/679 o Regolamento, definisce dati personali⁸ e,

SARZANA DI S. IPPOLITO – M. NICOTRA, *Diritto della Blockchain, Intelligenza artificiale e IoT*, Milano, Wolters Kluwer, 2018, p. 193.

⁴ Per algoritmo, si intende qualunque schema o procedimento sistematico di calcolo. Più precisamente, in informatica si definisce algoritmo una sequenza finita di operazioni elementari, eseguibili facilmente da un elaboratore che, a partire da un insieme di dati I (input), produce un altro insieme di dati O (output) che soddisfano un preassegnato insieme di requisiti. In Enciclopedia Treccani, <http://www.treccani.it/enciclopedia/algoritmo/>. Per un approfondimento sull'utilizzo degli algoritmi per le decisioni rilevanti per le libertà fondamentali della persona, e quindi sull'analisi dell'impatto delle tecnologie sul diritto costituzionale, si veda A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, n.1/2019, p. 67 e ss.

⁵ Il processo descritto è riferito al *machine learning*. Come spiegato da M. FASAN, *La tecnologia ci salverà? Intelligenza artificiale, salute individuale e salute collettiva ai tempi del Coronavirus*, in *BioLaw Journal*, Special Issue 1/2020, pp. 678 – 679, «un insieme di tecniche che permettono al sistema dotato di intelligenza artificiale di migliorare, attraverso l'esperienza, le prestazioni delle proprie funzioni. L'Intelligenza Artificiale può apprendere e migliorare grazie a specifici esempi, ai dati raccolti e alla propria esperienza e, in questo modo, può perfezionare il modello da utilizzare».

⁶ S. LEONELLI, *op. cit.*, p. 10 e ss.

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) (GU L 119 del 4 maggio 2016).

⁸ La definizione di dato personale è fornita dal Reg. Ue 2016/679 all'art. 4, par. 1, punto 1): "qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato'); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale". In merito alla definizione di dati personali si veda, *ex multis*, L. BENCI, *Sulla nozione di dato personale, sulla nozione di trattamento e dei soggetti che lo effettuano nel recente codice della privacy*, in *Rivista di diritto delle professioni sanitarie*, 2004; G. PINO, *L'identità personale*, in AA.VV., *Gli interessi protetti nella responsabilità civile*, vol. II, Torino, Utet, 2005; dello stesso autore si veda *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, tomo 1, Milano, Giuffrè, 2006; L. TEMPESTINI - G. D'ACQUISTO, *Il dato personale oggi tra le sfide dell'anonimizzazione e le tutele rafforzate dei dati sensibili*, in G. BUSIA - L. LIGUORI - O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali*, Roma, Aracne editrice, 2016; M. COPPOLA - F.

poiché le applicazioni “*Health & Fitness*” raccolgono e trattano anche i dati relativi alla salute⁹, si parla di categorie particolari di dati personali¹⁰. Queste app pensate per il benessere e lo stile di vita, destinate a mantenere o migliorare le abitudini sane e la qualità della vita delle persone, possono “dialogare” con dispositivi medici o sensori¹¹, creando nuove opportunità nel campo della salute.

Tale contesto diventa quindi il terreno di gioco dell'avvicinarsi di due diritti fondamentali da tutelare: il diritto alla salute, previsto all'art. 32 della Costituzione, e il diritto alla privacy¹², ora disciplinato dal Reg. UE 2016/679.

GUERRIERI, 4. *Definizioni*, in G.M. RICCIO - G. SCORZA - E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario. Regolamento Ue 2016/679 del 27 aprile 2016. Decreto di adeguamento – D. Lgs. n. 101/2018, Codice privacy – D. Lgs. n. 196/2003*, Milano, Wolters Kluwer, 2018, p. 36 ss. Di rilievo sul concetto di dati personali, è il Parere n. 4 del 20 giugno 2007 del Gruppo dei Garanti Europei, WP29, il quale precisa l'esistenza di un'ampia nozione di dati personali. L'esigenza dell'elaborazione del parere in questione nasceva per definire l'ambito di applicazione della normativa nazionale e di quella europea, in virtù della vigenza della direttiva. Ad oggi, con il Regolamento Ue 2016/679, che data la sua natura è direttamente applicabile in tutti gli stati membri dell'Unione, il parere del WP29 rimane un punto di riferimento essenziale per comprendere appieno il significato del concetto di dato personale considerando l'evoluzione tecnologica. In particolare, il riferimento è alla formulazione dell'espressione “qualsiasi informazione”, presente nella definizione di dato personale, il quale è oggetto di un'ampia interpretazione.

⁹ Per dati relativi alla salute, si intendono, ai sensi dell'art. 4.15 del Reg. UE 2016/679, “i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute”. I dati relativi alla salute, già nella direttiva 95/46/CE, erano considerati categorie particolari di dati personali, con una differenza rispetto a quanto previsto oggi dal Reg. UE 2016/679. Il Reg. UE 2016/679 prevede una definizione specifica nell'art. 4.15 e le regole generali per il trattamento all'art. 9, mentre, nella direttiva 95/46/CE, e nella disciplina nazionale non era presente questa puntuale distinzione tra la definizione e la disciplina del trattamento. Infatti, sia nella prima legge in materia di protezione dei dati personali, la legge n. 675/1996, che nel d. lgs. n. 196/2003, Codice in materia di protezione di dati personali, per i dati “idonei a rivelare lo stato di salute” rientranti nella categoria dei dati sensibili, erano solamente stabilite delle regole di trattamento. Per un approfondimento sul tema, si veda R. ACCIAI, *op. cit.*, p. 478-479; C. COLAPIETRO – F. LAVIOLA, *I trattamenti di dati personali in ambito sanitario*, in S. SCAGLIARINI (a cura di), *Il “nuovo” codice in materia di protezione dei dati personali. La normativa italiana dopo il d.lgs. n. 101/2018*, Giappichelli editore, Torino, 2019.

¹⁰ Le categorie particolari di dati personali sono disciplinati dal Reg. Ue 2016/679 all'art. 9, par.1: «(...) i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona» di cui si rimanda al paragrafo successivo l'approfondimento.

¹¹ COMMISSIONE EUROPEA, *Libro Verde sulla sanità mobile (“mHealth”)*, 10.4.2014, COM (2014) 219 final, p. 3.

¹² Il diritto alla privacy esprime l'evoluzione del diritto alla riservatezza. La riservatezza è definita da S. RODOTÀ, *Riservatezza* (voce), in *Enciclopedia italiana*, VII appendice, 2007, Roma,

2. Il trattamento dei dati necessario per la protezione da gravi minacce per la salute

La normativa in materia di protezione di dati personali, sia in ambito internazionale che comunitario¹³, ha da sempre previsto un generale divieto di trattamento per le categorie particolari di dati personali, meglio conosciuti come dati sensibili¹⁴, con la

Treccani, come la “possibilità di godere appieno della propria intimità”. Nasce infatti come rivendicazione di una sfera di riserbo per la quale il soggetto interessato preclude a terzi la possibilità di conoscere le proprie vicende personali. Come indicato dall’autore la riservatezza in origine era un privilegio riconosciuto alla classe borghese per via delle trasformazioni socioeconomiche legate alla rivoluzione industriale. È proprio in questo periodo che viene pubblicato l’ormai famoso saggio di S.D. WARREN, L.D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, 1890, il quale dà vita alla teoria del right to be let alone. Per approfondire il tema, *ex multis*, si veda M. TIMIANI, *Un contributo allo studio sul diritto alla riservatezza*, in *Studi parlamentari e di politica costituzionale*, n. 2/2012; S. SCAGLIARINI, *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Roma, Aracne editrice, 2013, p. 23 ss. Ancora, L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, editoriale scientifica, 2016, p. 9 ss., p. 51 ss. La normativa italiana ha affermato il diritto alla privacy prima con la legge del 31 dicembre 1996, n. 675, successivamente con il decreto legislativo del 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali ed in fine, a seguito dell’entrata in vigore del Reg. UE 2016/679, con la modifica al d. lsg. n.196/2003, avvenuta con il decreto legislativo del 10 agosto 2018, n. 101. La giurisprudenza si occupa del tema in questione in seguito a due importanti casi giudiziari. Si tratta del caso Caruso, il tenore Enrico Caruso e del caso Petacci, Claretta Petacci, legata sentimentalmente a Mussolini. Nel primo caso, gli eredi ritenevano leso il diritto alla riservatezza da un’opera cinematografica sulla sua vita, e i giudici individuavano il fondamento nell’analogia con l’art. 10 del cod. civ., mentre nell’altro, i congiunti di Claretta Petacci, parte ricorrente rispetto ad un’opera narrativa inerente alla biografia della stessa Petacci, il fondamento era individuato dai giudici nell’art. 8 CEDU. Nel caso Caruso, la Corte di Cassazione, a definizione della vicenda, nel 1956, afferma che non sussiste violazione dell’intimità privata, a meno che non sia stato reso l’onore o la reputazione. I giudici delle Corti inferiori insistono nella loro posizione affermando l’esistenza del diritto alla riservatezza nell’art. 2 Cost. e nell’art. 8 CEDU, appena ratificata nell’ordinamento italiano. È così che con la sentenza n. 990 del 1963, la Corte di Cassazione, dopo aver maturato la consapevolezza del variare dei tempi, riconosce una tutela del diritto alla riservatezza nel più ampio e unico diritto della personalità, quindi trovando il fondamento positivo nell’art. 2 della Cost. Qualche anno più tardi, con la sentenza n. 2129 del 1975, celebre caso della ex principessa di persia Soraya Esfandiari, la Corte di Cassazione estende in riconoscimento del diritto alla riservatezza non solo ad altre disposizioni costituzionali, quali, oltre all’art. 2 e 3 co. 2, agli articoli 13, 14, 15, 27, 29 e 41 Cost., ma trova dei riferimenti espliciti anche nella legislazione ordinaria, ad esempio nello statuto dei lavoratori, nella disciplina delle intercettazioni e la legge sullo stato civile. Sull’analisi giurisprudenziale di cui sopra, si veda S. SCAGLIARINI, *La riservatezza e i suoi limiti*, cit., p. 51 ss.

¹³ Il riferimento è alla Convenzione n. 108 del 1981, alle raccomandazioni n. R(81)1 del 1981, n. R(86)1 del 1986, n. R(89)2 del 1989, alla Direttiva 95/46/CE, anche conosciuta come Direttiva Madre, ed al più recente Reg. UE 2016/679.

¹⁴ La definizione di dati sensibili era disciplinata all’art. 4, par. 1, lett. d) del Codice in materia di protezione dei dati personali, d.lgs. 30 giugno 2003, n. 196, articolo abrogato dal d.lgs. 10 agosto 2018, n. 101, recante “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento Ue 2016/679 del parlamento europeo e del Consiglio, del 27 aprile

sola possibilità di derogarvi al verificarsi di determinate situazioni¹⁵ e alla presenza di adeguate misure di garanzia da parte del diritto interno¹⁶.

In caso di conflitto tra diritti di pari livello¹⁷, occorrerà quindi procedere ad un ragionevole contemperamento fra i diversi interessi che, come in questo caso, il diritto alla privacy e il diritto alla salute mirano a tutelare¹⁸. Ciò comporta che, la soddisfazione di un interesse potrebbe implicare il bilanciamento di un altro contrapposto¹⁹.

2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/Ce (regolamento generale sulla protezione dei dati)” (in G.U. 4 settembre 2018 n. 205). Il testo del decreto che ha novellato il suddetto Codice, precisa però, all’art. 22, co.2, che «a decorrere dal 25 maggio 2018, per «dati sensibili» (...) si intendono rispettivamente quelle categorie particolari di dati previste all’art. 9 del Reg. UE 2016/679(...)».

¹⁵ Si tratta delle deroghe previste all’art. 9, par. 2 del Reg. Ue 2016/679, che permettono il trattamento delle categorie particolari di dati personali per motivi di interesse pubblico rilevante; per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali; per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute.

¹⁶ Per un approfondimento si veda, *ex multis*, R. ACCIAI, *op. cit.*, p. 476 e ss. e A. CATALETA, *Categorie particolari di dati: le regole generali e i trattamenti specifici*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n.2016/679 e d. lgs. 10 agosto 2018*, n. 101, Bologna, Zanichelli ed., 2019, p. 206-208.

¹⁷ Il Garante per la protezione dei dati personali ha affrontato la tematica dei diritti di pari rango nel provvedimento generale *Dati sanitari. Provvedimento generale sui diritti di 'pari rango'* - 9 luglio 2003, doc web n. 29832, in www.garanteprivacy.it. L’Autorità precisa che «quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare (...) è di rango almeno pari ai diritti dell’interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile».

¹⁸ Per approfondire il tema del diritto alla salute e il suo bilanciamento con i diritto alla privacy, si veda, *ex multis*, R. ACCIAI, *op. cit.*, p. 477; L. CALIFANO, *Privacy: affermazione e privacy di un diritto fondamentale*, cit., p. 153 ss.; G. VACCARI, *Diritti fondamentali e biobanche a fini terapeutici e di ricerca: i bilanciamenti p(rop)osti dalle fonti (e “non fonti”) esistenti in materia*, in C. CASONATO - C. PICIOCCHI - P. VERONESI (a cura di), *La disciplina delle biobanche a fini terapeutici e di ricerca*, Forum biodiritto 2010, Università degli Studi di Trento, 2012; C. COLAPIETRO - F. LAVIOLA, *op. cit.*, p. 206.

¹⁹ L. GRECO, *op. cit.*, p. 245. Sul punto si veda anche L. CALIFANO, *Trasparenza e privacy: la faticosa ricerca di un bilanciamento mobile*, in L. CALIFANO - C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, Editoriale Scientifica, 2014, p.55. L’autrice afferma che nell’esigenza di individuare un bilanciamento mobile fra i diversi valori in continua evoluzione nel tempo, la dignità dell’individuo, intesa nel senso più ampio del diritto alla privacy, non deve essere travolta. Quanto affermato è il frutto di una riflessione sul contemperamento tra il diritto alla privacy ed il dovere di trasparenza amministrativa, che si traduce nell’ottemperanza agli obblighi di pubblicazione, anche di dati personali, di determinati soggetti individuati dal d. lgs. n. 33/2013, cc.dd. testo unico sulla trasparenza amministrativa.

Un esempio che ci permette di analizzare meglio la situazione suddetta, è reso possibile dall'emergenza sanitaria causata dal contagio da nuovo Coronavirus²⁰ (d'ora in poi anche Covid -19), che in Italia è stata dichiarata con delibera del Consiglio dei Ministri del 31 gennaio 2020²¹, e considerata una grave minaccia per la salute²², che mette in relazione proprio il diritto alla salute ed il diritto alla *privacy*. A tal proposito la normativa in materia di protezione dei dati personali, europea e nazionale, fornisce un buon tessuto normativo per poter trattare i dati personali al verificarsi di tali situazioni²³. Infatti, il Regolamento al considerando 46 rende lecito il trattamento dei dati personali per "tenere sotto controllo l'evoluzione di epidemie e la loro diffusione"; all'art. 6, par. 1, lett. c) ed e) individua l'adempimento ad un obbligo di legge e l'esecuzione di un interesse pubblico quali basi giuridiche che legittimano il trattamento, ribadendo la possibilità di trattare le categorie particolari di dati personali all'art. 9, par. 2, lett. c), g), h), i). La normativa italiana, il Codice in materia di protezione dei dati personali²⁴, si occupa del trattamento delle categorie particolari di dati personali per motivi di interesse pubblico rilevante all'art. 2-sexies, co. 2, lett. u), v)

²⁰ Il Coronavirus ha iniziato a diffondersi nel periodo a cavallo tra il 2019 e il 2020 e avrebbe avuto origine nella città cinese di Wuhan. L'Italia è stata interessata a fine gennaio 2020 e ad oggi il contagio ha interessato tutto il mondo, tanto che si parla di pandemia globale. Dalla definizione riportata dal dizionario on line Treccani, <http://www.treccani.it/vocabolario/pandemia/>, termine pandemia sta ad indicare una epidemia che tende a diffondersi ovunque, invadendo rapidamente vastissimi territori e continenti.

²¹ Delibera del Consiglio Dei Ministri 31 gennaio 2020, *Dichiarazione dello stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili*. (20A00737) ([GU Serie Generale n.26 del 01-02-2020](http://www.gazzettaufficiale.it/eli/id/2020/02/01/20A00737/sg)) consultabile al link <https://www.gazzettaufficiale.it/eli/id/2020/02/01/20A00737/sg>

²² Secondo la Decisione n. 1082/2013/UE del Parlamento europeo e del Consiglio del 22 ottobre 2013 relativa alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 2119/98/CE (Testo rilevante ai fini del SEE), sono definite «gravi minacce alla salute a carattere transfrontaliero»: un rischio per la salute in grado di mettere a repentaglio la vita del soggetto o comunque grave, di origine biologica, chimica, ambientale o di origine ignota, che si diffonde o comporta un rischio significativo di diffondersi oltre i confini nazionali degli Stati membri, e che può richiedere un coordinamento a livello di Unione al fine di garantire un livello elevato di protezione della salute umana.

²³ Sul punto si veda *ex multis* C. FILIPPI – S. MELCHIONNA, *I trattamenti di dati in ambito sanitario*, in G. BUSIA – L. LIGUORI – O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Roma, Aracne, 2016; G. DRUETTA, 9. *Trattamento di categorie particolari di dati personali*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario. Regolamento Ue 2016/679 del 27 aprile 2016. Decreto di adeguamento – D. Lgs. n. 101/2018, Codice privacy – D. Lgs. n. 196/2003*, Milano, Wolkers Kluwer, 2018, p. 89 -88.

²⁴ Il riferimento è al testo del decreto legislativo del 30 giugno 2003, n. 196, come modificato dal d. lgs. del 10 agosto 2018, n. 101.

e z), considerando rilevante interesse pubblico ciò che concerne i compiti del servizio sanitario e quelli spettanti la sicurezza e la salute della popolazione, la gestione dell'assistenza sanitaria e la vigilanza sulle sperimentazioni, la farmacovigilanza e ciò che è relativo all'immissione in commercio di farmaci²⁵.

L'Autorità Garante per la protezione dei dati personali²⁶ (d'ora in poi anche Autorità o Garante), a seguito del provvedimento governativo, in data 2 febbraio 2020 si è espressa con parere²⁷ favorevole sulla bozza di ordinanza emessa dalla protezione civile²⁸, rispetto alla possibilità di trattare i dati personali di cui agli artt. 9 e 10 del Reg. Ue 2016/679²⁹, da parte dei «soggetti operanti nel Servizio nazionale di protezione civile (...) e di soggetti attuatori, individuati anche tra gli enti pubblici economici e non economici e soggetti privati, che agiscono sulla base di specifiche direttive» allo scopo di fronteggiare l'emergenza sanitaria³⁰.

Contestualmente, diverse aziende operanti sul territorio nazionale, per consentire l'accesso ai luoghi di lavoro, hanno ritenuto opportuno far presentare delle

²⁵ Per la ricostruzione normativa, si veda D. POLETTI, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza*, in *Persona e Mercato* n.2/2020, p. 68.

²⁶ Il Garante per la protezione dei dati personali istituito dalla legge sulla privacy (legge 31 dicembre 1996, n. 675) è disciplinato dal Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003 n. 196), come modificato dal Decreto legislativo 10 agosto 2018, n. 101. Quest'ultimo ha confermato che il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (art. 51). Per un approfondimento sui compiti e sull'indipendenza del Garante, si veda, A. PATRONI GRIFFI, *L'indipendenza del Garante*, in L. CALIFANO - C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, editoriale scientifica, 2017, p. 267 e ss.; L. CALIFANO, *La protezione dei dati personali e il ruolo del Garante in ambito pubblico*, in G. BUSIA - L. LIGUORI - O. POLLICINO (a cura di), *op. cit.*, p. 25 e ss.

²⁷ Parere sulla bozza di ordinanza recante disposizioni urgenti di protezione civile in relazione all'emergenza sul territorio nazionale relativo al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili - 2 febbraio 2020, doc web n. 9265883, in www.garanteprivacy.it

²⁸ Presidenza Del Consiglio Dei Ministri Dipartimento Della Protezione Civile, Ordinanza 3 febbraio 2020, *Primi interventi urgenti di protezione civile in relazione all'emergenza relativa al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili*. (Ordinanza n. 630). (GU Serie Generale n.32 del 08-02-2020), la versione consolidata è consultabile al seguente link <https://www.gazzettaufficiale.it/eli/id/2020/02/08/20A00802/sg>

²⁹ Il riferimento è alle categorie particolari di dati personali di cui all'art. 9 del Reg. UE 2016/679, la cui analisi è stata in parte affrontata nel paragrafo precedente e di cui si continuerà a parlare successivamente; e all'art. 10 del Reg. UE 2016/679 che ha ad oggetto i dati personali relativi a condanne penali e reati.

³⁰ Il riferimento è all'art. 5 dell'ordinanza che ha ad oggetto la disciplina del trattamento dei dati personali.

autodichiarazioni³¹ ai dipendenti e ai visitatori, mirate alla raccolta di dati personali e relativi alla salute dei singoli individui. Questa è stata ritenuta, dalle stesse aziende, un'adeguata misura di prevenzione e protezione della salute e della sicurezza sui luoghi di lavoro³².

A tal proposito il Garante, in data 2 marzo 2020, ha precisato in una nota³³ che la possibilità di raccogliere i dati e le informazioni relative ai sintomi tipici del Coronavirus e le informazioni sugli spostamenti degli individui, deve essere limitata solamente ai soggetti preposti ed indicati nell'ordinanza della protezione civile, ossia agli operatori sanitari e agli operatori della protezione civile stessa. Al contempo, nella medesima nota, l'Autorità non ha riconosciuto tale possibilità ai soggetti pubblici e privati in qualità di datori di lavoro.

Successivamente si sono succeduti ulteriori e numerosi provvedimenti emergenziali³⁴ emanati anche dal Governo³⁵, tra cui i Decreti del Presidente del Consiglio dei Ministri dell'8 e del 9 marzo 2020, che hanno limitato drasticamente i movimenti degli individui

³¹ L'associazione di categoria Assolombarda ha messo a disposizione sul proprio sito *web* un modello di autodichiarazione, disponibile al seguente link <https://www.assolombarda.it/servizi/assolombarda-e-confindustria/informazioni/coronavirus-covid-19-indicazioni-ispirate-alla-prudenza-per-la-prevenzione-e-la-continuita-operativa>

³² Le aziende italiane, così come previsto dal decreto legislativo 9 aprile 2008, n. 81: "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro., d. lgs. n. 81/2008", a seguito della dichiarazione dello stato di emergenza da parte del Consiglio dei Ministri, hanno effettuato una valutazione del rischio in materia di salute e sicurezza sui luoghi di lavoro, ritendendo l'autodichiarazione una valida misura di prevenzione, laddove è definita prevenzione «il complesso delle disposizioni o misure necessarie (...) per evitare o diminuire i rischi professionali nel rispetto della salute della popolazione e dell'integrità dell'ambiente esterno», art. 1, co.1, lett. n) del d. lgs. n. 81/2008.

³³ Garante per la protezione dei dati personali, *Coronavirus: Garante Privacy, no a iniziative "fai da te" nella raccolta dei dati. Soggetti pubblici e privati devono attenersi alle indicazioni del Ministero della salute e delle istituzioni competenti*, 2 marzo 2020, docweb n. 9282117, in www.garanteprivacy.it

³⁴ Nella sezione "aree tematiche", alla voce "Coronavirus", è disponibile la "Raccolta degli atti recanti misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19" contenente tutti i provvedimenti emergenziali adottati dal Governo, dal Dipartimento della protezione civile, dal Commissario straordinario COVID-19, dal Ministero della Salute, dal Ministero dell'Economia e delle Finanze, dal Ministero dello Sviluppo Economico, dal Ministero dell'Interno e dal Ministero della Giustizia. I provvedimenti possono essere consultati al seguente link <https://www.gazzettaufficiale.it/dettaglioArea/12>

³⁵ Sulla natura dei provvedimenti emergenziali adottati dal Governo, si veda B. CARAVITA, *L'Italia ai tempi del coronavirus: rileggendo la Costituzione italiana*, in federalismi.it, Editoriale, 18 marzo 2020, n. 6/2020, p. VI.

sul territorio nazionale³⁶. Rilevante per il presente contributo è la previsione dell'art. 14 del d.l. 9 marzo 2020, n. 14³⁷, abrogato dalla legge del 24 aprile 2020, n. 27³⁸, ma il cui contenuto è stato interamente riproposto dall'17-bis della predetta legge di conversione³⁹. Le misure da adottare in tema di trattamento dei dati personali, previste inizialmente dall'art. 14 del d.l. 9 marzo 2020, n. 14, rubricato "*Disposizioni sul trattamento dei dati personali nel contesto emergenziale*", ed oggi disciplinate dal decreto n. 17-bis della legge n. 27/2020, concedono la possibilità di effettuare operazioni di trattamento riguardanti le categorie particolari dei dati personali di cui agli artt. 9 e 10 del Reg. UE 2016/679, «per motivi di interesse pubblico nel settore della sanità pubblica e, in particolare, per garantire la protezione dall'emergenza sanitaria a carattere transfrontaliero determinata dalla diffusione del COVID-19»⁴⁰.

Nel rispetto delle già citate deroghe al divieto di trattamento⁴¹ previste dal par. 2 dell'art. 9 del Reg. UE 2016/679, che riconoscono margini di discrezionalità legislativa

³⁶ Con il DPCM dell'8 marzo, sono stati attuati dei provvedimenti particolarmente restrittivi a livello locale, nello specifico per le seguenti regioni, Lombardia e nelle province di Modena, Parma, Piacenza, Reggio Emilia, Rimini, Pesaro e Urbino, Alessandria, Asti, Novara, Verbanco-Cusio-Ossola, Vercelli, Padova, Treviso, Venezia, disponendo di "evitare" gli spostamenti se non per ragioni di lavoro, di salute o di comprovate necessità; imponendo la sospensione delle attività scolastiche di ogni ordine e grado, la chiusura degli impianti sportivi; condizionando l'apertura dei luoghi di culto alla possibilità di accedervi mantenendo una distanza superiore al metro tra i presenti; limitando l'orario di apertura dei locali di ristorazione tra le sei e le diciotto. Inoltre, vietando di lasciare la propria abitazione per quanti siano in quarantena o comunque risultati positivi al contagio. il giorno seguente, con il DPCM del 9 marzo 2020, tali misure sono state estese all'intero territorio nazionale. Per un approfondimento si veda M. CAVINO, *Covid-19. Una prima lettura dei provvedimenti adottati dal Governo*, in federalismi.it, Osservatorio Emergenza Covid-19, Paper 18 marzo 2020.

³⁷ Decreto legge del 9 marzo 2020, n. 14: "*Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza COVID-19*". (GU Serie Generale n.62 del 09-03-2020). Entrata in vigore del provvedimento: 10/03/2020.

³⁸ Legge 24 aprile 2020, n. 27: "*Conversione in legge, con modificazioni, del decreto-legge 17 marzo 2020, n. 18, recante misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19. Proroga dei termini per l'adozione di decreti legislativi.*" (GU Serie Generale n.110 del 29-04-2020 - Suppl. Ordinario n. 16). Entrata in vigore del provvedimento: 30/04/2020.

³⁹ Sul punto si veda D. POLETTI, *op. cit.*, p. 67.

⁴⁰ F. P. MICOZZI, *Le tecnologie, la protezione dei dati e l'emergenza coronavirus: rapporto tra il possibile e il legalmente consentito*, in *BioLaw Journal*, Special Issue 1/2020, p. 630.

⁴¹ Sul divieto di trattamento delle categorie particolari di dati personali, di cui all'art. 9, par.1, del Reg. Ue 2016/679, si veda C. FILIPPI – S. MELCHIONNA, *I trattamenti di dati in ambito sanitario*, in G. BUSIA – L. LIGUORI – O. POLLICINO (a cura di), *op. cit.*, p. 481. In tal senso, gli autori, fanno un'analisi delle previsioni del Reg. Ue 2016/679 e il Codice in materia di protezione dei dati personali, d. lgs. n. 196/2003, come da ultimo modificato dal d. lgs.

agli Stati membri⁴², il legislatore nazionale ha provveduto a regolamentare l'emergenza sanitaria con la sovra illustrata disciplina⁴³. Da ciò si evince che è possibile effettuare il trattamento delle categorie particolari di dati personali per la gestione dell'emergenza per due ordini di motivi: *in primis*, perché il contagio da Covid-19 è da considerarsi una grave minaccia per la salute ed *in secundis*, perché tale trattamento è necessario per motivi di interesse pubblico rilevante nel settore della sanità pubblica ed in relazione al sistema sanitario nazionale⁴⁴.

Al fine di contenere il contagio, è emersa sia la possibilità di controllare le condizioni di salute degli individui attraverso l'uso di apposite applicazioni che raccolgono dati relativi alla salute⁴⁵, sia la possibilità di effettuare il trattamento dei dati degli individui usufruendo di tecnologie avanzate di *tracing*, ossia tracciandoli attraverso l'uso dei Big Data, ad esempio analizzando le transazioni delle carte di credito o altri mezzi di

n.101/2018. Sul punto si veda L. GRECO, *Sanità e protezione dei dati personali*, in G. FINOCCHIARO, *La protezione dei dati personali in Italia. Regolamento UE n.2016/679 e d. lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli ed., 2019, p. 250.

⁴² La discrezionalità a cui si fa riferimento è quella contenuta nelle previsioni dell'art. 9, par. 2. Così come indicato da F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, Giappichelli ed., 2016, p. 20 -21. Il legislatore europeo in alcuni articoli del Reg. UE 2016/679 consente ed in altri impone al legislatore statale di adottare delle normative nazionali. Si tratta di regolare quegli aspetti specifici che consentono agli Stati membri di introdurre precisazioni o ulteriori requisiti.

⁴³ Per una lettura più agevole della frammentata normativa relativa all'emergenza sanitaria e alla protezione dei dati, il Garante per la protezione dei dati personali ha elaborato una "Raccolta delle principali disposizioni adottate in relazione allo stato di emergenza epidemiologica da Covid-19 aventi implicazioni in materia di protezione dei dati personali" in continuo aggiornamento e consultabile sul sito web dell'Autorità al seguente link: <https://www.garanteprivacy.it/documents/10160/0/Raccolta+delle+principali+disposizioni+adotte+in+relazione+allo+stato+di+emergenza+epidemiologica+da+Covid-19+aventi+implicazioni+in+materia+di+protezione+dei+dati+personali+%28AGGIORNATO+AL+3+GIUGNO+2020%29.pdf/a3c13c1b-f14a-2cb3-c63b-d65dce1df8b7?version=1.15>

⁴⁴ Come indicato da M. MIDIRI – S. PIVA, *L'interesse pubblico come base giuridica e come finalità del trattamento dei dati personali*, in S. SCAGLIARINI (a cura di), *op. cit.*, p. 22, «nella definizione degli interessi pubblici rilevanti, il Regolamento definisce una cornice generale, ma agli Stati membri è riconosciuta una parziale autonomia normativa, tanto che si parla di potestà statale integrativa». Infatti, nel caso italiano, una dettagliata indicazione di interesse pubblico rilevante è fornita dal Codice in materia di protezione dei dati personali, come modificato dal d. lgs. n. 101 del 2018 all'art. 2-sexies, co. 2, identificandolo quale relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri in alcune materie, tra cui le attività connesse al sistema sanitario nazionale. Sul punto vedi G. DRUETTA, *op. cit.*, p. 101 e ss.

⁴⁵ Sul punto si veda A. CORDASCO, *Il difficile bilanciamento degli interessi in gioco tra privacy e dati sanitari al tempo del COVID 19*, in *IUS et SALUS, Rivista di diritto sanitario e farmaceutico*, fasc. n.1/2020, p.20.

pagamento, i dati di geolocalizzazione a disposizione dei gestori telefonici⁴⁶, oppure ancora, facendo installare agli individui, sui propri *smartphone*, delle applicazioni *ad hoc*, che permettano di tracciare i soggetti incontrati e i luoghi frequentati dalle persone contagiate, così da indicare quali siano le zone da evitare e cercando di limitare la propagazione del virus sul territorio⁴⁷. A tal proposito, il governo è intervenuto emanando il d.l. 30 aprile 2020, n. 28. Con l'art. 6, infatti, viene istituita la piattaforma unica nazionale per la gestione del sistema di allerta Covid-19⁴⁸, e sono disciplinate dettagliatamente le condizioni necessarie affinché sia possibile l'implementazione delle tecnologie di *tracing*⁴⁹.

3. Tecnologie innovative al banco di prova

Il Ministro per l'innovazione tecnologica e la digitalizzazione in accordo con il Ministero della Salute, a seguito di una call per il contrasto alla diffusione del Covid-19⁵⁰, il 31 marzo del 2020, ha istituito una Task force⁵¹ composta da un gruppo multidisciplinare di esperti⁵², chiamata a valutare e proporre soluzioni tecnologiche di

⁴⁶ Per un approfondimento si veda F. P. MICOZZI, *op.cit.*, p. 626, D. POLETTI, *op. cit.*, p. 66.

⁴⁷ Ancora F. P. MICOZZI, *op.cit.*, p. 626.

⁴⁸ D.l. 30 aprile 2020, n. 28, art. 6: "(...) è istituita una piattaforma unica nazionale per la gestione del sistema di allerta dei soggetti che, a tal fine, hanno installato, su base volontaria, un'apposita applicazione sui dispositivi di telefonia mobile. (...)".

⁴⁹ In particolare, il titolare del trattamento, il Ministero della salute, dovrà scegliere le misure di sicurezza da adottare, previste dall'art. 32 del Reg. Ue 2016/679, a seguito della valutazione d'impatto effettuata ai sensi dell'art. 35 del Regolamento. Il Ministero della salute deve altresì assicurarsi che sia consegnata l'informativa al trattamento dei dati ai sensi degli artt. 13 e 14 del Reg. Ue 2016/679; che per impostazione predefinita siano raccolti e trattati solamente i dati necessari al raggiungimento della finalità preposta (avvisare del possibile contatto avuto con un soggetto positivo al Covid-19) nel rispetto dei principi sanciti dall'art. 5 del regolamento. Inoltre, devono essere garantiti i diritti, previsti dall'art. 15 a 22 del reg. UE 2016/679, riconosciuti all'interessato e soprattutto che al termine dell'emergenza tutti i dati raccolti e trattati devono essere cancellati.

⁵⁰ Il riferimento è alla fast call promossa dal Ministro per l'innovazione tecnologica e la digitalizzazione, finalizzata all'individuazione di soluzioni tecnologiche di teleassistenza di pazienti domestici e per il tracciamento continuo, l'*alerting* e il controllo tempestivo del livello di esposizione al rischio delle persone e conseguentemente dell'evoluzione dell'epidemia sul territorio <https://innovazione.gov.it/telemedicina-e-sistemi-di-monitoraggio-una-call-per-tecnologie-per-il-contrasto-alla-diffusione-del-covid-19/>

⁵¹ Nasce la task force italiana per l'utilizzo dei dati contro l'emergenza Covid-19 <https://innovazione.gov.it/nasce-la-task-force-italiana-per-l-utilizzo-dei-dati-contro-l-emergenza-covid-19/>

⁵² Il Ministro per l'innovazione tecnologica ha selezionato il gruppo di esperti, scelti in collaborazione con il Ministero della Salute, l'Istituto Superiore di Sanità e l'Organizzazione

*data-driven*⁵³ per la gestione dell'emergenza sanitaria, economica e sociale legata alla diffusione del virus. La Task force, con il compito di valutare "le migliori soluzioni digitali disponibili relativamente ad app di telemedicina e assistenza domiciliare dei pazienti e a tecnologie e strategie basate sulle tecnologie per il monitoraggio "attivo" del rischio di contagio", ha tra gli obiettivi principali proprio quello di esaminare i profili giuridici della gestione dei dati connessa all'emergenza, analizzando i vincoli normativi per l'utilizzazione e la condivisione dei dati personali tra soggetti pubblici e tra soggetti privati e pubblici, predisponendo una strategia di garanzia dei diritti e delle libertà fondamentali⁵⁴, in particolare per tutelare il diritto alla salute e alla privacy⁵⁵.

Come si evince dalle indicazioni disponibili sul sito web del ministero⁵⁶, si tratta di individuare delle valide soluzioni nell'ambito della telemedicina⁵⁷ e del tracciamento

Mondiale della Sanità e tra componenti direttamente designati dall'Autorità garante della concorrenza e del mercato, dall'Autorità per le garanzie nelle comunicazioni e dal Garante per la protezione dei dati personali, in base a comprovata esperienza nelle rispettive discipline di riferimento. Si tratta di soggetti che possono dare il proprio contributo data la loro appartenenza a specifiche discipline.

⁵³ Per *data-driven innovation*, si intende la produzione e l'utilizzo crescente di dati, ossia uno dei vettori principali della evoluzione tecnologica, degli investimenti e della crescita economica. Sul punto si veda S. CALZOLAIO, *Protezione dei dati personali*, in *Digesto delle discipline pubblicistiche*, Milano, Utet Giuridica, Wolters Kluwer, 2017. Per approfondire il tema della *data-driven innovation* si veda OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD publishing, Paris, 2015, <https://doi.org/10.1787/9789264229358-en>.

⁵⁴ In merito agli obiettivi da perseguire, si può consultare quanto riportato sul sito ufficiale del Ministro dell'innovazione tecnologica al seguente link: <https://innovazione.gov.it/nasce-la-task-force-italiana-per-l-utilizzo-dei-dati-contro-l-emergenza-covid-19/>

⁵⁵ In merito a quanto sostenuto da D. DE FALCO E M. L. MADDALENA, *La politica del tracciamento dei contatti e dei test per covid-19 alla luce delle ultime direttive OMS: nessun ostacolo giuridico impedisce di utilizzare il "modello coreano" anche in Italia*, in *federalismi.it*, Osservatorio Emergenza Covid-19, Paper del 28 marzo 2020, p. 8, è opportuno, a parer di chi scrive, fare delle precisazioni rispetto «ai problemi di carattere giuridico anche connessi alla tutela della privacy». È auspicabile superare quel gap culturale che considera la privacy un "problema giuridico". Da diverso tempo, ormai, la privacy è un diritto fondamentale riconosciuto agli individui. Inoltre, il combinato disposto tra gli artt. 9, comma 2, e 23 del Reg. UE 2016/679, non «consentono limitazioni alla privacy per motivi di sanità pubblica», ossia, non consentono limitazioni della privacy intesa quale diritto fondamentale, ma prevedono la possibilità di limitare alcuni obblighi previsti dal Reg. UE 2016/679. Il riferimento particolare è alle previsioni degli artt. da 12 a 22, riguardanti le informazioni e le modalità con le quali queste devono essere fornite all'interessato e i diritti riconosciuti allo stesso; dell'art. 34, in merito alla comunicazione delle violazioni dei dati personali e dell'art. 5, riguardante i principi applicabili al trattamento, per quelle disposizioni che riguardano solamente le previsioni disposte dagli artt. da 12 a 22 del Reg. UE 2016/679.

⁵⁶ Il riferimento è alla "fast call" promossa dal Ministero <https://innovazione.gov.it/telemedicina-e-sistemi-di-monitoraggio-una-call-per-tecnologie-per-il-contrasto-alla-diffusione-del-covid-19/>

continuo, l'*alerting* ed il controllo tempestivo del livello di esposizione al rischio del contagio. Alcune di queste tecnologie sono misure di "sorveglianza attiva" ovvero di isolamento dei focolai del virus che avviene attraverso il tracciamento dei contatti dei soggetti positivi e la sottoposizione di essi ai *test* anche se trovati asintomatici⁵⁸. Diverse regioni italiane⁵⁹ hanno fin da subito scelto di utilizzare tali tecnologie, basate sul consenso⁶⁰ dei soggetti interessati, come ad esempio la regione Lombardia, interessata in modo particolare dal contagio del Coronavirus, con il supporto della Protezione Civile, ha sviluppato un sistema di monitoraggio della popolazione, implementando

⁵⁷ Per telemedicina si intende la «modalità di erogazione di servizi di assistenza sanitaria, tramite il ricorso a tecnologie innovative in situazioni in cui il professionista della salute e il paziente (o due professionisti) non si trovano nella stessa località». Tale definizione è fornita dalle linee di indirizzo in materia di telemedicina del Ministero della salute, che costituiscono l'allegato A dell'Intesa tra il Governo, le Regioni e le Province autonome di Trento e Bolzano, sottoscritto il 20 febbraio 2014. Per approfondire il tema della definizione di telemedicina, si veda *ex multis* A. L. TARASCO, *La telemedicina per lo sviluppo della sanità del Mezzogiorno: una introduzione giuridica*, Rivista giuridica del Mezzogiorno, fasc. n. 4, dicembre 2010; C. BOTRUGNO, *Un diritto per la telemedicina: analisi di un complesso normativo in formazione*, in *Politica del diritto*, fasc. n. 4/2014, p. 640; C. BOTRUGNO, *La diffusione della telemedicina nella pratica medica ordinaria: verso un'etica ad hoc*, in *Ragion pratica*, fasc. n. 1/2016; F. G. CUTTAIA, *Lo sviluppo della telemedicina e i profili di tutela della privacy*, in *Studi parlamentari e di politica costituzionale*, n. 201- 202, 3° e 4° trimestre 2018, p. 30 e ss.

⁵⁸ Sul punto si veda D. DE FALCO - M. L. MADDALENA, *op. cit.*, p. 3, G. FARES, *Covid-19 e diritti: i nodi da sciogliere*, in *Ius et Salus, Rivista di diritto sanitario e farmaceutico*, fasc. n. 1/2020 p. 9.

⁵⁹ Sul punto si veda quanto riportato dalla rivista online wired.it. R. ANGIUS – L. ZORLONI, *Coronavirus: Regione che vai, tecnologia che trovi*, in <https://www.wired.it/internet/web/2020/03/28/coronavirus-regioni-tracciamento-privacy/>

⁶⁰ La definizione di consenso è presente nel Reg. Ue 2016/679 all'art. 4, par.1, punto 11: "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*". Per approfondire il tema del consenso rilasciato per il trattamento dei dati personali, si vedano in particolare C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., p. 115 ss.; L. CHIEFFI, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., p. 235 ss.. Inoltre, il Gruppo di lavoro Articolo 29, WP 29, ha fornito ulteriori indicazioni sul tema, *nelle Linee guida sul consenso ai sensi del Regolamento (UE) 2016/679*, adottate il 28 novembre 2017 come modificate e adottate da ultimo il 10 aprile 2018, 17/it Wp 259 rev.01, analizzando nello specifico ogni elemento della definizione del consenso che lo rendono valido. Inoltre, come fa notare S. RODOTÀ, *Tecnologie e diritti*, Bologna, il Mulino, 1995, p. 81, il tradizionale consenso ha subito evoluzioni significative. Si passa infatti dalla tecnica dell'*implied consent* all'*informed consent*, ossia ad un consenso informato, validamente espresso sulla base delle informazioni fornite al soggetto interessato. Per un approfondimento sul tema del consenso informato, si veda dello stesso Autore, *Perché laico*, Roma-Bari, ed. Laterza, 2009 e *Il diritto di avere diritti*, *op. cit.*

l'app AllertaLom⁶¹. La app raccoglie dati per mappare il rischio del contagio, e permette di fare un *triage* a distanza attraverso le risposte ad un questionario⁶². La regione Lazio, invece, ha adottato una app⁶³ di telemedicina⁶⁴ con lo scopo di mettere in contatto con il proprio medico di base, i cittadini che presentano i sintomi del virus o sono stati in contatto con soggetti positivi al Covid-19, per avviare il protocollo per i casi sospetti.

Focalizzando l'attenzione sulla app di telemedicina adottata dalla Regione Lazio, possiamo affermare che essa è uno strumento di sanità digitale⁶⁵, concetto non nuovo nel nostro Paese. Già alla fine degli anni 90 si sviluppa l'idea di favorire «le tecniche

⁶¹ L'app AllertaLOM era già utilizzata, prima dell'emergenza Coronavirus, per le allerte di Protezione Civile. A seguito dello svilupparsi del Covid-19 è stato implementato al fine di gestire l'emergenza sanitaria, con la possibilità di individuare in anticipo l'emergere di eventuali nuovi focolai.

⁶² In merito alla app. AllertaLom la Regione Lombardia ha precisato che non si tratta di una app di telemedicina, ma che serve solo a conoscere le dinamiche di diffusione capillare del virus. <https://www.openinnovation.regione.lombardia.it/b/572/regioneaicittadiniunapppermonitorareladiffusedelcovid> La notizia è stata, inoltre, riportata da diverse testate giornalistiche. Di seguito se ne segnalano alcune <https://www.wired.it/scienza/medicina/2020/04/02/coronavirus-lombardia-cercacovid-allertalom/> ; <https://www.punto-informatico.it/lombardia-allertalom-cercacovid/> ; <https://www.ilfattoquotidiano.it/2020/04/01/coronavirus-regione-lombardia-prova-a-mappare-il-rischio-di-contagio-con-unapp-si-chiama-cercacovid-ecco-come-funziona/5756453/>

⁶³ Si tratta dell'applicazione chiamata LAZIODRCOVID (Lazio Doctor Covid) e si rivolge a tutti i cittadini che vogliono entrare in contatto con il proprio medico di famiglia da remoto, a chi manifesta sintomi legati al Covid19 (febbre, tosse, bruciore agli occhi), a chi è entrato in contatto stretto con persone positive al Covid19 e a chi è stato sottoposto a misure di sorveglianza attiva da parte della Asl. Così come indicato sul sito web della Regione, i dati inseriti nella app verranno rielaborati dal sistema e saranno messi a disposizione degli operatori sanitari. Nel caso di risposte indicative di rischio di contatto o malattia, l'utente verrà contattato per un approfondimento ed una televisita, e verrà inserito nel servizio di telesorveglianza. Invece, i pazienti risultati positivi al Covid-19 saranno telemonitorati, collegandosi ad alcuni dispositivi che verranno consegnati al paziente al momento della diagnosi. <http://www.regione.lazio.it/rl/coronavirus/scarica-app/>

⁶⁴ Il fine è quello di permette il monitoraggio dei pazienti a distanza e di prediligere «un approccio alla cura centrato sul paziente stesso» G. FARES, *Covid-19 e diritti: i nodi da sciogliere*, op. cit., p. 9.

⁶⁵ Come indicato dal documento della PRESIDENZA DEL CONSIGLIO DEI MINISTRI, *Strategia per la crescita digitale 2014-2020*, del 3 marzo 2015, versione del 21 giugno 2016, per sanità digitale si intende la forte interazione dei sistemi informativi sanitari, aziendali e ospedalieri, basati sull'utilizzo diffuso di tecnologie *cloud*, sull'applicazione di criteri per omogeneizzare e standardizzare la raccolta e il trattamento dei dati sanitari. L'obiettivo primario della sanità digitale è quello di garantire la continuità assistenziale. Consolidando i sistemi informativi territoriali su cui impiantare modelli organizzativi innovativi, si potrà essere in grado di erogare servizi ad assistiti e operatori anche a supporto delle attività socio-sanitarie territoriali, come agevolare la diagnostica, sostenere i percorsi di cura e gestire le cronicità. Sul punto si veda F. APERIO BELLA, *Tecnologie innovative nel settore salute tra scarsità delle risorse e differenziazione: alla ricerca di un equilibrio difficile*, in *federalismi.it*, fasc. n.2/2020, p. 249.

intelligenti di monitoraggio sanitario e di accesso telematico all'informazione ed all'assistenza medica»⁶⁶. Nel 2004 la Commissione europea ha adottato il primo piano d'azione per la sanità elettronica⁶⁷, o *e-health*, evidenziando i benefici per lo Stato, il mercato e gli stessi cittadini-utenti. Anche nel più recente «Piano d'azione Sanità elettronica 2012-2020 – Una sanità innovativa per il 21esimo secolo»⁶⁸, sono state evidenziate le peculiarità per i cittadini che avrebbero un'assistenza sanitaria più incentrata su di loro e quindi più mirata, più efficiente e più efficace⁶⁹. La sanità digitale o elettronica è fortemente legata al concetto di sanità mobile (*m-health*), ossia, la pratica della medicina supportata da *device* mobili, quali *smarthphone* e altri dispositivi senza fili che permettono al medico di monitorare il paziente a distanza⁷⁰. Le applicazioni di *m-health* permettono quindi di raccogliere un volume considerevole di dati relativi alla salute, consentendo di costituire la base per la prestazione di cure e la conduzione di attività di ricerca e permettendo ai pazienti di accedere più facilmente alle informazioni sulla propria salute⁷¹.

⁶⁶ Cfr. C. FILIPPI - S. MELCHIONNA, *op. cit.*, p. 484.

⁶⁷ COMMISSIONE EUROPEA (2012), Comunicazione della Commissione al Consiglio, al Parlamento Europeo, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Sanità elettronica – Migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica*, COM/2004/356, <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52004DC0356&qid=1585903034937&from=IT>

⁶⁸ COMMISSIONE EUROPEA (2012), Comunicazione della Commissione al Consiglio, al Parlamento Europeo, al Comitato economico e sociale europeo e al Comitato delle regioni. *Piano d'azione «Sanità elettronica» 2012-2020 – Una sanità innovativa per il 21esimo secolo*, COM/2012/0736, <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52012DC0736>

⁶⁹ G. VICARELLI, M. BRONZINI, *La sanità digitale: dimensioni di analisi e prospettive di ricerca*, in *Politiche Sociali*, fasc. n. 2, maggio-agosto 2018, pp. 150-151.

⁷⁰ COMMISSIONE EUROPEA, *Libro Verde sulla sanità mobile ("mHealth")*, COM/2014/ 219 final <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52014DC0219&rid=25> . Una definizione di *m-health* è fornita anche dal COMITATO NAZIONALE PER LA BIOETICA, *"Mobile-health" e applicazioni per la salute: aspetti bioetici*, del 28 maggio 2015, p. 5.

⁷¹ Per un approfondimento si veda R. M. COLANGELO, *App mediche e protezione dei dati personali. Alcuni spunti giuridici tra Gdpr, codice privacy novellato e chiarimenti del Garante*, in *Autonomie locali e servizi sociali*, fasc. n. 2/2019. L'autore oltre a soffermarsi sulle diverse peculiarità rappresentate dalla *m-health*, evidenzia anche alcuni aspetti critici legati non solo al continuo trattamento dei dati dovuto all'attività di *self tracking*, ma anche ad altri di carattere generale come ad esempio il rischio di aumento del *digital divide* tra quanti hanno uno strumento che garantisca la *m-health*, come lo *smartphone* e quanti non ne dispongono, anche in ragione di fattori anagrafici.

La telemedicina potrebbe allora rappresentare «una delle chiavi di volta per lo sviluppo e l'ammmodernamento della sanità italiana»⁷², poiché con essa è possibile trasmettere in modo sicuro le informazioni e i dati relativi alla salute, nelle diverse forme necessarie per la prevenzione, la diagnosi, il trattamento ed il successivo controllo dei pazienti⁷³. L'uso delle tecnologie a distanza, governate dall'intelligenza artificiale, di seguito anche AI, per la gestione del Covid-19, potrebbe essere una soluzione, oltre che di efficienza⁷⁴, anche di efficacia rispetto alla salvaguardia delle vite dei medici e di tutto il personale sanitario, i quali sono maggiormente esposti al contagio. Elaborare e programmare un sistema informatico in grado di somministrare delle cure ad un paziente non deve essere una visione marziana. Esperimenti di questo tipo si sono verificati a Whuan⁷⁵ ma anche in ospedali italiani, tra cui Circolo di Varese⁷⁶ e di Rimini⁷⁷. Al di fuori di questa emergenza, sono diverse le applicazioni di AI utilizzate nel campo dell'*healthcare*, tra cui quelle adottate per la terapia dei più piccoli, come a Bologna dove il robot Marino può comunicare con i pazienti più piccoli di oncologia aiutandoli ad esternare le proprie emozioni⁷⁸, oppure, Kaspar, il robot che aiuta i bambini affetti da autismo ad interagire con il prossimo. Inoltre, esempi di *m-health* sono forniti da una *start-up* spagnola che ritiene di essere riuscita a creare un

⁷² Cfr. A. L. TARASCO, *op. cit.*, p. 1390.

⁷³ Ministero della Salute, *Telemedicina. Linee di indirizzo nazionali*, del 20 febbraio 2014. http://www.salute.gov.it/imgs/C_17_pubblicazioni_2129_allegato.pdf

⁷⁴ Affidare la realizzazione di un'analisi genetica a tecnologie dotate di AI significa ridurre notevolmente i tempi di attesa della risposta normalmente previsti. Sul punto si veda M. FASAN, *op. cit.*, p. 680. Ciò, a parer di chi scrive, potrebbe assicurare una miglior tenuta in termini di resistenza del sistema sanitario e garantire una miglior gestione dell'emergenza sanitaria, soprattutto nella sua fase più critica e acuta.

⁷⁵ Coronavirus, a Wuhan c'è un reparto ospedaliero interamente gestito dai robot, in https://www.repubblica.it/tecnologia/2020/03/10/news/coronavirus_a_wuhan_c_e_un_reparto_ospedaliero_interamente_gestito_dai_robot-250838881/, Un ospedale pieno di robot per proteggere i medici dal coronavirus, in <https://www.lastampa.it/tecnologia/news/2020/03/12/news/un-ospedale-pieno-di-robot-per-proteggere-i-medici-dal-coronavirus-1.38581189>

⁷⁶ I sette robot in corsia che curano i pazienti affetti da Covid-19 (e fanno fronte alla carenza di medici e infermieri) <https://www.corriere.it/video-articoli/2020/04/01/i-sette-robot-corsia-che-curano-pazienti-affetti-covid19-far-fronte-carenza-medici-infermieri/b8c51084-7419-11ea-b181-d5820c4838fa.shtml>

⁷⁷ La notizia è stata riportata sul quotidiano online Ansa ed è consultabile al seguente link: https://www.ansa.it/emiliaromagna/notizie/2020/03/28/a-rimini-robot-visita-pazienti-coronavir_3dc4a895-e1a1-4737-982c-7076071f9da6.html

⁷⁸ Per leggere la notizia si può consultare il link di seguito: <http://www.noisiamopronti.it/2017/08/14/bologna-il-piccolo-robot-che-parla-con-i-bimbi-malati/>

modello di AI in grado di applicare modelli e metodi scientifici psicologici per migliorare le condizioni di vita dei pazienti affetti da patologie psichiatriche. Ancora, un'altra start-up francese cerca di migliorare la vita dei pazienti con il diabete di tipo I, personalizzando ed ottimizzando le dosi di insulina rispetto all'effettivo bisogno dell'individuo⁷⁹.

Queste tecnologie avanzate ed innovative offrono numerose peculiarità ma rappresentano anche dei potenziali rischi per la *privacy*, è perciò interessante comprendere come queste si potrebbero conciliare con il diritto alla protezione dei dati personali.

4. Considerazioni tecniche conclusive

Una delle soluzioni innovative e tecnologiche che la Task force è chiamata ad individuare ha ad oggetto la telemedicina e l'assistenza domiciliare dei pazienti, in virtù delle caratteristiche proprie che tali strumenti offrono, poiché permettendo l'assistenza sanitaria a distanza, si garantirebbe il più possibile la tenuta dei sistemi sanitari nazionali⁸⁰.

Ipotizzando come soluzione l'adozione di una app è possibile avanzare alcune considerazioni conclusive.

Trattandosi di strumenti e di misure invasive si assiste a forti limitazioni dei diritti fondamentali per i soggetti interessati⁸¹. È per questo motivo che assume particolare spessore il diritto all'autodeterminazione informativa⁸², ossia la possibilità che gli individui hanno di governare i propri dati personali nel modo più consapevole possibile. Affinché ciò avvenga devono quindi essere fornite delle essenziali

⁷⁹ Sul punto si veda Fondazione Leonardo Civiltà delle Macchine, *Statuto Etico e Giuridico dell'IA*, 2019, pp. 21-22.

⁸⁰ M. FASAN, *op. cit.*, p. 677.

⁸¹ Sul punto si veda G. FARES, *Covid-19 e diritti: i nodi da sciogliere*, *op. cit.*, p. 6.

⁸² «L'autodeterminazione nella vita e nel corpo rappresenta il punto più intenso e estremo della libertà esistenziale», S. RODOTÀ, *Il diritto di avere diritti*, *op. cit.*, p. 250. Sul principio di autodeterminazione informativa si veda, *ex multis*, L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, *op. cit.*, 2016; L. CALIFANO, *Il trattamento dei dati genetici: finalità di ricerca, esigenze di sicurezza e diritto alla protezione dei dati personali*, in *Cultura giuridica e diritto vivente*, vol. 4, 2017, p. 3; L. CALIFANO, *Il regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in L. CALIFANO - C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento Ue 2016/679*, *op. cit.*

informazioni a tali soggetti. In primo luogo, è necessario chiarire quali sono i soggetti legittimati al trattamento dei dati che vengono raccolti. In tal senso, la app Immuni, scelta per il *tracing*, può fornire una indicazione in merito, poiché, come si evince dall'informativa resa, ai sensi degli artt. 13 e 14 del Reg. UE 2016/679, il titolare del trattamento⁸³ potrebbe essere anche in questo caso, il Ministero della salute. Sarebbe necessario però fornire una indicazione più precisa dei soggetti che “*di default*” sono deputati al trattamento dei dati, ossia il personale medico e/o gli operatori sanitari. Il testo dell'art. 17-bis, co.1, della legge del 24 aprile 2020, n.27, non permette infatti, di delineare un numero limitato di soggetti deputati al trattamento⁸⁴, lasciando aperta la facoltà di trattare quei dati a innumerevoli individui coinvolti nella gestione dell'emergenza sanitaria.

Particolare attenzione merita la valutazione che il titolare del trattamento deve compiere per quanto riguarda le misure di sicurezza che devono essere adottate ai sensi dell'art. 32 del Reg. UE 2016/679⁸⁵. La app di telemedicina dovrebbe prevedere una password di accesso *ad hoc* e di *default* dovrebbero essere adottate tecniche di pseudonimizzazione⁸⁶ che garantirebbero ulteriore sicurezza ai dati trattati e conservati

⁸³ Il Reg. Ue 2016/679, definisce all'art. 4.7 il titolare del trattamento quale «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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri».

⁸⁴ La previsione dell'art. 17-bis, co.1 della legge n. 27 del 24 aprile 2020 è la seguente: “Fino al termine dello stato di emergenza deliberato dal Consiglio dei ministri in data 31 gennaio 2020 (...)i soggetti operanti nel Servizio nazionale della protezione civile, di cui agli articoli 4 e 13 del codice di cui al decreto legislativo 2 gennaio 2018, n. 1, e i soggetti attuatori di cui all'articolo 1 dell'ordinanza del Capo del Dipartimento della protezione civile n. 630 del 3 febbraio 2020, nonché gli uffici del Ministero della salute e dell'Istituto superiore di sanità, le strutture pubbliche e private che operano nell'ambito del Servizio sanitario nazionale e i soggetti deputati a monitorare e a garantire l'esecuzione delle misure disposte ai sensi dell'articolo 2 del decreto-legge 25 marzo 2020, n. 19, anche allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, possono effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali, anche relativi agli articoli 9 e 10 del regolamento (UE) 2016/679, che risultino necessari all'espletamento delle funzioni ad essi attribuite nell'ambito dell'emergenza determinata dal diffondersi del COVID-19.”.

⁸⁵ Si tratta delle «misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio» così come previsto dall'art. 32 del Reg. Ue 2016/679.

⁸⁶ Il Reg. Ue 2016/679, fornisce una definizione di pseudonimizzazione all'art. 4.5: “il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali

sulla app. Pur nel rispetto del principio di minimizzazione⁸⁷, i dati che inevitabilmente sono raccolti e trattati rientrano nelle categorie particolari di dati personali *ex art. 9* del Regolamento. Si tratterebbe infatti di dati relativi alla salute, senza poter escludere i dati genetici e i dati biometrici⁸⁸, oltre che informazioni e documenti di varia natura, come ad esempio la diagnostica per immagini, che nel caso del Covid-19 potrebbe essere fondamentale per lo studio della storia clinica del paziente.

Inoltre, l'uso della app di telemedicina dovrebbe essere volontario, così come indicato dal Garante⁸⁹ e dall'*European Data Protection Board*⁹⁰ per le app di tracciamento. A tal proposito, non si dovrebbe rendere obbligatorio il *download* ed il seguente uso della app., che rimarrebbe volontario, ma il trattamento dei dati effettuato potrebbe configurarsi necessario per lo svolgimento di un compito di interesse pubblico, ai sensi

informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile". Sul punto si veda anche G. D'ACQUISTO - M. NARDI, *op. cit.*, p. 38, definiscono la pseudonimizzazione «consiste nel sostituire un attributo, solitamente univoco, di un dato con un altro, ugualmente univoco e solitamente non immediatamente intellegibile». Attraverso questa tecnica, il processo di identificazione può essere più oneroso, ma è mantenuto inalterato il quadro di certezze per concatenare l'attribuzione del dato pseudonimo alla persona.

⁸⁷ Il Reg. Ue 2016/679, prevede il principio di minimizzazione all'art. 5, disponendo che i dati personali sono «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*».

⁸⁸ I dati genetici e biometrici sono definiti dal Reg. Ue 2016/679 rispettivamente all'art. 4.13 e all'art. 4.14. I «*dati genetici sono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione*», mentre i dati biometrici sono «*i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*».

⁸⁹ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Primi riscontri alle ipotesi avanzate all'interno del Gruppo di lavoro *data-driven* per l'emergenza COVID-19, 7 aprile 2020, Audizione informale, in videoconferenza, del Presidente del Garante per la protezione dei dati personali sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus, Commissione IX (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati (8 aprile 2020), Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19 - 29 aprile 2020, Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 - App Immuni - 1° giugno 2020. I documenti sono reperibili alla pagina web dedicata <https://www.garanteprivacy.it/temi/coronavirus> (ultima visita 6 giugno 2020).

⁹⁰ EUROPEAN DATA PROTECTION BOARD, *Linee-guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19*, Adottate il 21 aprile 2020, punto 29, pp. 7 e 8.

dell'art. 6, par. 1, lett. e), del Reg. UE 2016/679⁹¹. A supporto di ciò dovrebbe però intervenire un atto normativo *ad hoc*, che renderebbe lecito il trattamento dei dati. Diverso è il discorso del consenso che assume una duplice veste nelle app di telemedicina. Abbiamo infatti il «consenso informato⁹² al trattamento sanitario che favorisce la realizzazione congiunta del diritto alla tutela della salute e della libertà personale del paziente ed il consenso informato al trattamento dei dati personali che non risponde al fine di tutela della salute di chi lo presta, potendo essere piegato ad altri scopi»⁹³.

Una criticità può essere rilevata in merito alla *data retention*⁹⁴, ossia al tempo di conservazione dei dati. In tal senso, a parer di chi scrive, potrebbero essere adottate due diverse soluzioni: i dati trattati potrebbero essere conservati solo per il periodo necessario a ricevere l'assistenza sanitaria, oppure, in una seconda ipotesi, i dati potrebbero essere conservati per tutto il tempo di durata dello stato di emergenza⁹⁵, e

⁹¹ L'art. 6, par. 1, lett. e), del Reg. UE 2016/679 sancisce che “il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento”.

⁹² Sul consenso informato quale espressione della volontà di un soggetto a sottoporsi ad una prestazione sanitaria, si veda S. AZZINI, *Biobanche, consenso e fonti del diritto: un caso di eccezionale disordine?*, in C. CASONATO - C. PICIOCCHI - P. VERONESI (a cura di), *La disciplina delle biobanche a fini terapeutici e di ricerca*, Forum di biodiritto 2010, Università degli studi di Trento, 2012, p. 120. Come rilevato dall'autrice, il consenso informato è centrale nel rapporto medico-paziente. V. MARZOCCO, *Il consenso informato alla conservazione e all'utilizzo di materiale biologico umano. Persona e corpo tra relazione interrotta e nuovi scenari rappresentativi*, in C. CASONATO - C. PICIOCCHI - P. VERONESI (a cura di), *op. cit.*; M. MACILOTI, *Consenso informato e biobanche di ricerca*, in *La nuova giurisprudenza civile commentata*, n. 3, marzo 2009; M. MACILOTI - U. IZZO - G. PASCUIZZI - M. BARBARESCHI, *La disciplina giuridica delle biobanche*, in *Pathologica*, 2008, p. 95 ss.; E. MAESTRI, *Digibodies. Biobanche e consenso informato tra finzioni scientifiche e finzioni giuridiche*, in R. BRIGHI - S. ZULLO (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Roma, Aracne, 2015; R. PACIA, *Campione biologico e consenso informato nella ricerca genetica: il possibile ruolo delle biobanche*, in *www.juscivile.it*, n. 3, 2014, p. 85 ss. Ancora, sul tema del consenso al trattamento dei dati personali del minore, si veda F. NADDEO, *Il consenso al trattamento dei dati personali del minore*, in *Diritto dell'informazione e dell'informatica*, n. 1/2018.

⁹³ Cfr. G. FARES, *Covid-19 e diritti: i nodi da sciogliere*, *op. cit.*, p. 15.

⁹⁴ Per *data retention* si intende il periodo di conservazione dei dati raccolti. Come indicato dal considerando 39 del Reg. Ue 2016/679, il periodo di conservazione dei dati deve essere limitato al minimo necessario.

⁹⁵ Sul punto si veda G. BISCONTINI, M. E. COMBA, E. DEL PRATO, L. A. MAZZAROLLI, A. POGGI, G. VALDITARA, F. VARI, *Le tecnologie al servizio della tutela della vita e della salute e della democrazia. Una sfida possibile*, in *federalismi.it*, Osservatorio Emergenza Covid-19, Paper del 23 marzo 2020, p. 4.

successivamente cancellati, così come dovrebbe avvenire per la app. Immuni⁹⁶. A seguito dell'emergenza, inoltre, non sembrerebbe esclusa, in virtù di quanto previsto per il *tracing* dall'art. 6, co. 3 d.l. n. 28/2020, la possibilità di trattare i dati raccolti dalla app a fini di ricerca scientifica⁹⁷. Infatti, il Regolamento rende lecito il trattamento anche delle categorie particolari di dati personali a fini di ricerca scientifica, all'artt. 5, par. 1, lett. b) ed e), l'art. 9, paragrafo 2, lettera j), in combinato con le deroghe previste degli artt. 49 e 89⁹⁸. Nel caso dell'emergenza sanitaria risulterebbe necessario raccogliere numerose informazioni destinate ad alimentare «banche dati aperte per gli studi sul monitoraggio dei focolai e sulle dinamiche del fenomeno, postulando una necessaria cooperazione internazionale che potrebbe comportare trasferimenti di dati relativi alla salute»⁹⁹.

Ciò che risulta evidente al termine di queste considerazioni è che con la valutazione di impatto¹⁰⁰, strumento di *accountability*¹⁰¹, il titolare del trattamento può da subito avere

⁹⁶ Nel caso della app. Immuni, infatti, il d.l. del 30 aprile 2020, n. 28, all'art. 6, co.6, prevede che entro e non oltre il 31 dicembre del 2020 tutti i dati trattati devono essere cancellati o resi definitivamente anonimi.

⁹⁷ Si deve precisare che il Regolamento Ue 2016/679, prevede sì la possibilità di trattare i dati a fini di ricerca scientifica, ma a patto che essi siano anonimizzati. Inoltre, l'anonimizzazione è considerata un trattamento vero e proprio, quindi, deve essere indicato nell'informativa consegnata ai pazienti-utenti che al termine dello stato di emergenza, i dati potrebbero essere anonimizzati e utilizzati a fini di ricerca scientifica. Il Codice per la protezione dei dati personali, prevede all'art. 105 le modalità di trattamento dei dati a fini di ricerca di scientifica ed inoltre prevede all'articolo 106 l'adozione di Regole deontologiche per i trattamenti di dati a fini di ricerca scientifica. per un approfondimento sul tema L. CHIEFFI, *Ricerca scientifica e tutela della persona. Bioetica e garanzie costituzionali*, Napoli, Edizioni scientifiche italiane, 1993; L. SAPORITO, *La ricerca scientifica*, Padova, Cedam, 1993; E. LONGO, *I trattamenti nel settore dell'istruzione e a fini di ricerca (scientifica, storica, statistica)*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento Ue 2016/679*, op. cit.

⁹⁸ Per un approfondimento si veda D. POLETTI, *op. cit.*, p. 68.

⁹⁹ *Ivi*, p. 68.

¹⁰⁰ La valutazione d'impatto sulla protezione dei dati o *Data Protection Impact Assessment* (DPIA), è una procedura prevista dall'articolo 35 del Reg. Ue 2016/679 che analizza un trattamento di dati per valutarne in particolare i rischi, allo scopo di adottare misure idonee a fronteggiarli. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi. Per un approfondimento sul tema si veda, GRUPPO DI LAVORO ARTICOLO 29, *Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679*, adottate il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017, (17/it Wp 248 rev. 01, reperibili sul sito www.ec.europa.eu); GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4,*

quella visione complessiva del trattamento dei dati e del flusso degli stessi tanto da permettergli di valutare quali misure implementare affinché il trattamento avvenga nel pieno rispetto dei principi di *privacy by design e privacy by default*¹⁰².

In conclusione, si rileva che il diritto alla *privacy* non deve essere considerato un ostacolo o un limite per l'applicazione di tecnologie innovative nel campo della salute e tantomeno bisogna scegliere se utilizzare o meno tali tecnologie disponibili. Nella realtà sociale in cui viviamo, vale a dire una società di dati, un'era digitale, i dati personali sono da considerarsi un'estensione della persona. Invero, proprio come diceva il professor Rodotà, «la proiezione dell'umano oltre il corpo, non implica una sua dispersione, ma il suo occupare uno spazio più vasto»¹⁰³. Ciò è permesso dallo sviluppo delle tecnologie, le quali disperdono l'uomo in una miriade di frammenti, ma trovano proprio nell'uomo l'unico connettore, poiché gli stessi processi tecnologici in esso convergono. Per cui seppur il principio di autodeterminazione informativa sembrerebbe essere messo in crisi e sfuggire al controllo dell'uomo¹⁰⁴ data la sua identità digitale, la normativa vigente in materia di protezione dei dati personali fornisce tutti gli strumenti necessari affinché gli individui possano esercitare

del Regolamento (UE) n. 2016/679 - 11 ottobre 2018, reperibile sul sito www.garanteprivacy.it (doc. web n. 9058979).

¹⁰¹ Il principio di *accountability* è "l'obbligo per il titolare del trattamento di mettere in atto tutte le misure ritenute adeguate a garantire il rispetto di principi e obblighi dettati dal GDPR", L. GIACOMINI, C.A. TROVATO, C. ROSSI CHAUVENET, *Il registro delle attività di trattamento previsto dal GDPR: più di uno strumento di mera compliance*, in *Medialaws. Rivista di diritto dei media*, n. 3/2018. Per un approfondimento, *ex multis*, si veda L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, Editoriale Scientifica, 2016, p. 73, della stessa autrice, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, in L. CALIFANO – C. COLAPIETRO (a cura di), *op. cit.*, p. 34 e ss; S. CALZOLAIO, *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *Federalismi.it*, n. 24/2017.

¹⁰² Con l'espressione *privacy by design* si intende la protezione dei dati fin dalla progettazione. Ciò significa che a partire dal momento preparatorio e progettuale delle attività di trattamento di dati personali devono essere configurati strumenti e metodi che rispettino i principi di protezione dei dati, i requisiti del trattamento e la tutela dei diritti degli interessati. Invece, con l'espressione *by default* si intendono «le adeguate soluzioni tecniche e organizzative poste in essere dal titolare per garantire che, in base ad impostazioni predefinite (by default) e in corrispondenza di ogni specifica finalità del trattamento, questo si limiti ai soli dati necessari». Cfr. R. D'ORAZIO, *Protezione dei dati by default e by design*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *op. cit.*, p. 81-82. Si veda inoltre, COMITATO NAZIONALE DI BIOETICA, *op. cit.*, p. 11; S. CALZOLAIO, *op. cit.*, p. 631.

¹⁰³ Cfr. S. RODOTÀ, *Il diritto di avere diritti*, *op. cit.*, p. 366.

¹⁰⁴ Sul punto si veda S. RODOTÀ, *Il diritto di avere diritti*, *op. cit.*, p. 366 e ss.

pienamente tale principio.

dirittifondamentali.it