TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE E TUTELA DELLA SALUTE

LE SFIDE APERTE TRA PROTEZIONE, CIRCOLAZIONE E RIUTILIZZO DEI DATI

CARLO **BOTRUGNO**

&dq

Tecnologie dell'informazione e della comunicazione e tutela della salute: le sfide aperte tra protezione, circolazione e riutilizzo dei dati

Information and Communication Technologies for Health Care: Exploring Current Issues between Data Protection, Circulation and Re-Use

CARLO BOTRUGNO

Assegnista di Ricerca presso Dipartimento di Scienze Giuridiche, Università degli Studi di Firenze; Coordinatore della Research Unit on Everyday Bioethics and Ethics of Science.
E-mail: carlo.botrugno@gmail.com

ABSTRACT

Obiettivo di questo lavoro è analizzare le sfide indotte dalla diffusione dei servizi sanitari mediati dalle tecnologie dell'informazione e della comunicazione prendendo come punto di riferimento il Regolamento europeo concernente la protezione e la libera circolazione dei dati personali nell'area dell'Unione. Inoltre, ci si sofferma sulle principali problematiche etiche e giuridiche sollevate dall'adozione dei servizi sanitari digitali per favorire il contenimento del contagio da CoViD-19.

This article aims at assessing the main challenges posed by the spread of healthcare services mediated by the information and communication technologies taking as a reference the EU Regulation on protection and free circulation of data concerning natural persons. In addition, the main ethical and legal issues raised by the introduction of digital healthcare services to face the CoViD-19 pandemic are identified and analysed.

KEYWORDS

Tecnologie dell'informazione e della comunicazione, dati sanitari, privacy e protezione dei dati personali, libera circolazione dei dati, sanità digitale

Information and communication technologies, health data, privacy and data protection, free circulation of personal data, digital healthcare

ISSN 1825-0173

Tecnologie dell'informazione e della comunicazione e tutela della salute: le sfide aperte tra protezione, circolazione e riutilizzo dei dati

CARLO BOTRUGNO

1. *Introduzione*

L'entrata in vigore del nuovo Regolamento europeo per la protezione dei dati personali[1], meglio noto come *General Data Protection Regulation* (d'ora in avanti, RGPD o Regolamento) ha sancito la nascita di un nuovo impianto, pensato allo scopo di incrementare il livello di protezione fornito dalla normativa previgente, attuazione della Direttiva 95/46/CE[2], e quindi dare vita a uno *jus commune* europeo che garantisca maggiore uniformità e certezza in questa materia.

Negli ultimi vent'anni, invero, le esigenze di protezione della privacy individuale si sono moltiplicate, non solo a causa della progressiva diffusione di tecnologie e servizi che, in un modo o nell'altro, prevedono la raccolta di informazioni personali, ma anche in ragione di una loro crescente "aggressività" nei confronti di queste ultime. È lo stesso Regolamento a sottolineare che «la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati sanitari»[3], il che, peraltro, corrisponde alla «diffusa sensazione che i nostri dati personali siano costantemente a rischio» (COLAPIETRO 2018, 2)[4]. Invero, il clamore suscitato dal susseguirsi di violazioni della privacy, talvolta di tipo plurimo[5] ha reso evidente che le informazioni personali possono diventare fonte di profitto per chi è in grado di accedervi, controllarle ed eventualmente elaborarle attraverso i più svariati procedimenti di *data-mining* e *influencing*, per lo più basati su funzioni algoritmiche.

Com'è facilmente intuibile, nel più ampio contesto della protezione dei dati personali, l'ambito sanitario è fra quelli che spiccano per importanza dal momento che nella pratica medica si scambia e si condivide una serie ragguardevole di informazioni personali che non solo permet-

[1] Regolamento 2016/679/UE 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.

[2] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[3] Cfr. considerando n. 6 del RGPD.

[4] Nello stesso senso PIZZETTI 2018, 108.

[5] Tra i molti possibili esempi di violazione della privacy, si pensi allo scandalo suscitato dal caso *Cambridge Analytica*, società di consulenza britannica accusata di aver utilizzato procedimenti di elaborazione e *data-mining* per influenzare surrettiziamente le opinioni politiche degli utenti di Facebook in prossimità delle elezioni politiche statunitensi del 2016.

tono l'identificazione diretta dei pazienti ma altresì di accedere alle loro condizioni di salute. Questa condivisione e/o trasmissione può avvenire per il tramite di sistemi informatici complessi, oppure, più semplicemente, attraverso strumenti di comunicazione di uso comune come lo scambio di e-mail e di altri messaggi in forma scritta. Come noto, le informazioni riconducibili all'ambito della salute appartengono alla categoria dei cc.dd. dati sensibili – categorie di dati "particolari" nel RGPD –, insieme a ogni altra informazione da cui sia possibile evincere l'orientamento sessuale, l'origine razziale o etnica, le convinzioni religiose e filosofiche, le opinioni politiche, l'appartenenza sindacale degli individui. In questo contesto, non appare superfluo ricordare che un orientamento consolidato della Corte di Cassazione definisce evocativamente i dati sanitari come "sensibilissimi" o "supersensibili"[6]. Da ciò discende che gli stessi debbano essere oggetto di una "protezione rafforzata" dal momento che essi riguardano la parte più intima della persona nella sua corporeità e nelle sue convinzioni psicologiche più profonde.

D'altro canto, la diffusione delle nuove tecnologie in ambito sanitario fa sì che le violazioni dei dati personali possano divenire non solo macroscopiche in considerazione della portata degli interessi protetti – in un climax, diritto alla riservatezza, alla salute, all'integrità fisica, alla libertà e alla vita –, ma che le stesse possano anche assumere proporzioni abnormi, coinvolgendo contestualmente un elevato numero di individui.

Le esigenze di protezione della sfera individuale nell'ambito sanitario acquisiscono una portata specifica con riferimento all'utilizzo delle tecnologie dell'informazione e della comunicazione (d'ora in avanti TIC), le quali permettono di mettere in comunicazione pazienti e professionisti sanitari, o questi ultimi fra loro, in vista del raggiungimento di una serie di finalità che attengono alla diagnosi, prevenzione, monitoraggio, riabilitazione e trattamento di un numero sempre più vasto di patologie[7]. Peraltro, come si vedrà più ampiamente all'interno di questo lavoro, l'avvento della pandemia di CoViD-19 ha impresso un'accelerazione senza precedenti alla transizione digitale dei nostri sistemi sanitari, mostrando quanto la protezione dei dati personali sia il risultato di un bilanciamento complesso tra il godimento dei diritti fondamentali e le esigenze di tutela della salute individuale e collettiva.

Nel prosieguo, pertanto, ci si soffermerà sulle sfide indotte dalla diffusione dei servizi sanitari mediati dalle TIC, prendendo come punto di riferimento il nuovo impianto di protezione dei dati personali predisposto in sede comunitaria[8]. Dopo aver ripercorso brevemente l'evoluzione delle TIC in ambito sanitario (§ 2), ci si sofferma sinteticamente sul ruolo assunto dai dati sanitari all'interno della strategia europea di promozione delle TIC (§ 3). Successivamente, si analizzano gli elementi di maggiore novità introdotti dal RGPD (§ 4), soprattutto alla luce della loro incidenza sulle attività di erogazione dei servizi sanitari a distanza. A seguire, si fa il punto sulla disciplina nazionale, tra l'adeguamento del Codice in materia di protezione dei dati personali[9] e il contributo apportato dal Garante della privacy al tema della protezione dei dati sanitari raccolti tramite le TIC (§ 5). Segue un'analisi delle principali problematiche etiche e giuridiche sollevate dall'adozione di servizi tecnologicamente mediati per favorire il contenimento della pandemia (§ 6). Infine, si propone una riflessione critica che analizza le sfide aperte a livello eti-

[6] Cfr. Cass. Civ., Sez. VI, sentenza dell'11/01/2016, n. 222; Cass. Civ., Sez. I, sentenza. del 07/10 2014, n. 21107; Cass. Civ., Sez. I, sentenza del 01/08/2013, n. 18443.

[7] Organizzazione Mondiale della Sanità, *Report on the second global survey on e-health*, 2010, disponibile in: www.who.int/goe/publications/goe_telemedicine_2010.pdf (consultato il 24/08/2020).

[8] Esula, pertanto, dalle finalità di questo lavoro l'analisi relativa al trattamento dei dati sanitari in ambiti ulteriori rispetto a quelli ascrivibili alla tutela della salute (*e.g.* in ambito lavoristico, assicurativo, ecc.).

[9] Tale adeguamento è stato effettuato per mezzo del d.lgs. n. 101/2018, *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*. Il provvedimento è entrato in vigore in data 19 settembre 2018.

co e giuridico in un contesto, quale quello attuale, in cui l'intersezione tra dati sanitari e diffusione delle TIC assume un ruolo determinante nello sviluppo delle società contemporanee (§ 7).

2. *Dalla sanità elettronica alla telemedicina: varianti terminologiche ed evoluzione del settore*

Nelle ultime due decadi, si è assistito a una notevole proliferazione di espressioni e definizioni che hanno come denominatore comune l'utilizzo di TIC per il miglioramento dei processi di gestione in sanità o al fine di predisporre nuovi servizi e percorsi diagnostico-terapeutici di cui i pazienti possono beneficiare a distanza. Per le finalità di questo lavoro, è importante provare a fare chiarezza sulle caratteristiche intrinseche a questi servizi, soprattutto in considerazione del fatto che dalla loro qualificazione può dipendere l'applicabilità o meno di determinate disposizioni giuridiche (Botrugno 2018a, 132).

All'espressione "sanità elettronica", inizialmente ricorrente soprattutto nel panorama nazionale, si è progressivamente venuta ad affiancare la "salute digitale", insieme al più noto corrispettivo in lingua inglese *e-health* e, successivamente, alla *mobile health*. Sulla scorta degli orientamenti adottati in questa materia dalla Commissione europea[10]), l'*e-health* può essere intesa come una convergenza fra informatica medica, sanità pubblica ed economia, che si basa sulla raccolta di informazioni e sull'offerta di servizi sanitari per mezzo di internet e delle tecnologie correlate al suo utilizzo. Così intesa, pertanto, l'*e-health* include potenzialmente ogni utilizzo delle TIC che avvenga nell'ambito di un sistema sanitario, ovvero che coinvolga direttamente o indirettamente uno o più professionisti sanitari. La letteratura specializzata in questo settore ha poi messo in rilievo come il termine *e-health* sia atto a designare non solo uno sviluppo di tipo tecnico, ma anche «uno stato d'animo, un modo di pensare, un'attitudine, e uno sforzo proteso verso il raggiungimento di una connettività globale, finalizzati a migliorare l'assistenza sanitaria attraverso le tecnologie dell'informazione e della comunicazione» (Eysennbach 2001).

Pressoché contestualmente all'emersione dell'*e-health*, inizia ad affacciarsi sullo scenario delle TIC sanitarie anche la "telemedicina", un termine che, come facilmente intuibile a livello semantico, deriva dalla fusione di telematica e medicina (Botrugno 2018b, 13 ss). Anche la telemedicina ha progressivamente conosciuto una proliferazione di varianti terminologiche, molte delle quali di derivazione anglosassone – *telehealth*, *telehealthcare*, *telehomecare*, *remote care*, *virtual care*, ecc. – ognuna delle quali volta a designare una dimensione particolare d'intervento a distanza, con caratteristiche e modalità di funzionamento che, caso per caso, possono variare anche in misura significativa.

Rispetto alla più ampia sfera dell'*e-health*, tuttavia, il tratto distintivo della telemedicina risiede nel presupporre comunque una forma di interazione, in tempo reale o differito, tra il paziente e il professionista sanitario. Conformemente all'orientamento adottato in sede comunitaria[11], infatti, la telemedicina presuppone l'erogazione di una prestazione medica, ovvero di una *performance* di natura intellettuale, resa da un professionista abilitato all'esercizio della professione.

All'interno della telemedicina si suole poi annoverare una modalità di intervento più specifica, ovvero il monitoraggio remoto dei parametri vitali del paziente – anche noto come telemonitoraggio –, che può essere effettuato per mezzo di dispositivi indossabili, impiantabili e perfino ingeribili. Oggi, il telemonitoraggio rappresenta una delle aree più promettenti dell'intero panorama dei servizi a distanza e può essere effettuato dal paziente in via autonoma o in collabora-

[10] A mero titolo esemplificativo, si vedano i seguenti atti di orientamento della Commissione europea: Comunicazione 2004/356, *Sanità elettronica: migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica*; Comunicazione 2008/689, *Sulla telemedicina a beneficio dei pazienti, dei sistemi sanitari e delle società*; Comunicazione 2012/736, *Sanità elettronica 2012-2020 - Una sanità innovativa per il 21° secolo*.

[11] Commissione europea, Comunicazione 2008/689, cit., 20.

zione con un'istituzione sanitaria. Questa distinzione non è di poco conto poiché, se in quest'ultimo caso si resta senza dubbio nell'ambito della telemedicina, il primo ricomprende un'area complessa ed estremamente articolata, quella delle *health apps*, con cui si suole designare un insieme di servizi progettati per il funzionamento su dispositivi portatili di comune utilizzo come tablet e smartphone. Invero, sebbene l'utilizzo delle *health apps* consenta ai propri utilizzatori di perseguire finalità ascrivibili al mantenimento del benessere o alla tutela della propria salute in senso lato, è opportuno chiarire che, laddove tali servizi siano utilizzati in assenza di un qualsiasi coinvolgimento o apporto materiale da parte di un professionista sanitario, il loro funzionamento fuoriesce dall'ambito della telemedicina e da quello della stessa *e-health*, per rientrare in una dimensione che può essere definita più opportunamente in termini di *self-care* (BOTRUGNO 2016, 193; LUPTON 2013, 256). Sulle *health apps* si è espresso anche il Comitato Nazionale per la Bioetica (CNB), che ha dedicato un apposito parere alle implicazioni etiche derivanti dal loro crescente utilizzo[12]. Dopo aver salutato con favore la diffusione di nuove tecnologie che promettono di migliorare la qualità dell'assistenza sanitaria, il parere evidenzia i possibili rischi innescati dalla loro diffusione, fra cui non solo quelli afferenti alla tutela della privacy, ma anche quelli relativi alla possibilità di diagnosi e prescrizioni terapeutiche fatte in proprio (*self-made*) dai loro utilizzatori[13]. Tale sorta di timore, peraltro, trova una corrispondenza concreta in evidenze empiriche offerte da studi qualitativi di orientamento critico (LUPTON 2013; MORT et al. 2013, 799; MILLIGAN et al. 2011, 347), all'interno dei quali si sottolinea come il *digital engagement* dei pazienti si fondi sovente su strategie volte a trasferire una serie di incombenze dai professionisti sanitari ai pazienti, con l'obiettivo mediato di contenere i costi dell'assistenza pubblica.

3. *Il ruolo dei dati sanitari nella strategia europea di promozione delle TIC*

Nelle ultime due decadi, la Commissione europea ha profuso un impegno notevole al fine di stimolare l'adozione dei servizi sanitari mediati dalle TIC all'interno dei sistemi sanitari degli Stati membri, dapprima con l'*e-Health Action Plan*[14] e poi con la più ampia *Policy for Ageing Well With ICTs*, politiche sviluppate sotto l'egida del Mercato Unico Digitale. A questa ampia azione di promozione delle TIC[15] si ricollega l'adozione di una *Strategia europea dei dati*, che delinea un "approccio globale" il cui obiettivo finale è quello di «incrementare l'utilizzo e la domanda di dati e di prodotti e servizi basati sui dati in tutto il mercato unico»[16]. Nella visione adottata dalla Commissione europea, i dati sono intesi come

> «la linfa vitale dello sviluppo economico: sono la base di molti nuovi prodotti e servizi e generano guadagni in termini di produttività ed efficienza delle risorse in tutti i settori economici, rendendo possibili prodotti e servizi più personalizzati, un miglioramento del processo di elaborazione delle politiche e un potenziamento dei servizi pubblici»[17].

[12] Comitato Nazionale per la Bioetica,"*Mobile-health" e applicazioni per la salute: aspetti bioetici*, disponibile in: http://bioetica.governo.it/it/documenti/pareri-e-risposte/mobile-health-e-applicazioni-per-la-salute-aspetti-bioetici/ (consultato il 24/08/2020).

[13] Comitato Nazionale per la Bioetica,"*Mobile-health" e applicazioni per la salute: aspetti bioetici*, cit., 15 ss.

[14] Adottato nel 2004 attraverso la Comunicazione 2004/356, cit., e poi rinnovato per mezzo della Comunicazione 2012/736, cit.

[15] Recentemente rinnovata e ridenominata *Plasmare il futuro digitale dell'Europa*, disponibile in: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_it (consultato il 24/08/2020).

[16] Cfr. Commissione europea, Comunicazione 2020/66, *Una strategia europea per i dati*, 2.

[17] Commissione europea, *Plasmare il futuro digitale dell'Europa*, cit., 3.

Ciò rende evidente che la promozione di questa strategia si fonda su una matrice essenzialmente economica, così come desumibile, peraltro, dal richiamo ivi contenuto alla necessità di competere con attori globali all'avanguardia nel settore digitale quali Cina e Stati Uniti[18]. Invero, nonostante il riferimento enfatico all'essere umano quale "elemento centrale" di questa visione[19], l'obiettivo manifesto della Commissione europea è quello di

> «creare uno spazio unico europeo di dati – un autentico mercato unico di dati, aperto ai dati provenienti da tutto il mondo – nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore»[20].

Per quanto riguarda la valenza assunta dai dati nell'ambito sanitario, la Commissione si era già espressa con la Comunicazione 2018/233, «relativa alla trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana»[21]. Dopo aver introdotto il contesto dei sistemi sanitari degli Stati membri – con le relative sfide, fra cui invecchiamento della popolazione, multimorbilità, scarsità di personale sanitario, incremento delle patologie non trasmissibili e riemergere di quelle trasmissibili – la Commissione snocciola i benefici ottenibili grazie alla digitalizzazione dei sistemi sanitari, fra cui la possibilità di «accrescere il benessere di milioni di cittadini e cambiare radicalmente il modo in cui i servizi sanitari e assistenziali vengono forniti ai pazienti». Più in particolare, lo sviluppo dei servizi sanitari digitali consentirebbe di migliorare la continuità assistenziale, promuovere la salute e il benessere anche sul posto di lavoro e, più in generale, «sostenere la riforma dei sistemi sanitari e la loro transizione verso nuovi modelli di assistenza, basati sui bisogni delle persone, e consentire un passaggio da sistemi incentrati sugli ospedali a strutture assistenziali integrate e maggiormente basate sulle comunità»[22]. All'interno di questa visione, la Commissione riconosce che i dati sanitari rappresentano un "elemento chiave" per dare avvio alla rivoluzione digitale, e quindi ridisegnare il funzionamento dei sistemi sanitari e, al contempo, ampliarne l'accessibilità.

La Comunicazione 2018/233 della Commissione europea chiarisce altresì come il raggiungimento di tali obiettivi sia stato sinora frenato dall'assenza di un'effettiva interoperabilità dei dati sanitari e dalla frammentazione del mercato, fattori che «rappresentano un ostacolo ad un approccio integrato alla prevenzione delle malattie e ad una cura e assistenza meglio adattate alle esigenze dei cittadini»[23]. A questo proposito, non appare superfluo ricordare che l'interoperabilità dei dati sanitari – il cui ottenimento è divenuto un obiettivo fondamentale nella Strategia europea dei dati –, rappresentava già un pilastro della Direttiva 2011/24/UE[24] sull'assistenza sanitaria transfrontaliera a beneficio dei cittadini dei paesi membri, per il cui raggiungimento quest'ultima aveva istituito un'apposita *eHealth Network*, che riunisce oggi i paesi membri più la Norvegia in qualità di osservatore e opera sotto la supervisione della stessa Commissione europea. Nel contesto attuale, le attività di condivisione e scambio dei dati sanitari a livello europeo sono limitate alla cooperazione volontaria fra paesi membri, i quali si avvalgono a tal fine di una *eHealth Digital Service Infrastructure*. Tuttavia, sino a questo momento tale cooperazione è rima-

[18] Commissione europea, *Plasmare il futuro digitale dell'Europa*, cit., 4.
[19] *Ibid*.
[20] *Ibid*.
[21] Commissione europea, Comunicazione 2018/233 relativa alla trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana.
[22] Commissione europea, Comunicazione 2018/233, cit., 1.
[23] Commissione europea, Comunicazione 2018/233, cit., 2.
[24] Direttiva 2011/24/UE del 9 marzo 2011 concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera.

sta circoscritta allo scambio dei fascicoli sanitari dei pazienti e delle prescrizioni in formato telematico. È per questo motivo che la Commissione europea ha assunto un impegno concreto volto all'adozione di standard europei per la qualità, affidabilità e sicurezza dei dati sanitari e per l'adozione di un formato europeo che renda possibile la standardizzazione delle cartelle cliniche elettroniche e quindi lo scambio[25].

4. *Tra protezione e circolazione: dalla privacy alla concezione dinamica della tutela dei dati personali*

L'Unione europea ha ridisegnato il proprio impianto di protezione dei dati personali attraverso l'emanazione del RGPD, che all'art. 1, rubricato "Oggetto e finalità", oltre ad annunciare «norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali», prevede anche «norme relative alla libera circolazione di tali dati». Il paragrafo 3 dello stesso articolo rafforza l'enfasi sulla libera circolazione dei dati personali all'interno dell'Unione, sottolineando come questa non possa essere «limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali». Come messo adeguatamente in rilievo a questo proposito, il Regolamento «disciplina temi che nulla hanno a che fare con la riservatezza in senso stretto, ma che attengono invece al regime di circolazione delle informazioni, in parte propri di altri settori e materie, quali il mercato della concorrenza sulle informazioni e l'accesso alle informazioni» (Finocchiaro 2018, 896).

Sin dal suo *incipit*, pertanto, il RGPD rende evidente il binomio indissolubile tra protezione dei dati personali e libera circolazione degli stessi nello spazio europeo, segno di "distacco" da parte del legislatore europeo «dalla concezione sostanzialmente statica del diritto al rispetto della vita privata, in cui era sufficiente una tutela eminentemente negativa, consistente nel potere di escludere le interferenze altrui» (Colapietro 2018, 4). Come messo in rilievo dalla dottrina, infatti, l'idea di protezione esclusivamente rivolta alla "persona fisica" è divenuta vetusta all'interno delle società contemporanee, il funzionamento delle quali ha reso invece necessaria l'adozione di una concezione "dinamica" di protezione dei dati, quindi, la necessità di apprestare una tutela che «segue i dati nel momento della loro circolazione» (Colapietro 2018, 4). A ciò corrisponde il passaggio da un "modello unidirezionale", in cui il flusso di dati avveniva principalmente dall'interessato al titolare del trattamento, a uno di "condivisione e cogestione" dei dati e delle informazioni i quali appaiono «destinati fin dall'origine ad una circolazione globale» (Finocchiaro 2017, 1).

D'altra parte, la transizione dall'*habeas corpus* all'*habeas data* (Colapietro 2018, 14), ovvero dall'idea della privacy in quanto protezione della riservatezza della persona a una concezione plurivoca di protezione delle informazioni personali che formano il contenuto dei dati, è stata suggellata dalla c.d. costituzionalizzazione del diritto alla protezione dei dati personali e, più precisamente, dalla scelta di prevedere un omonimo diritto accanto al più classico diritto alla vita privata e familiare (rispettivamente, artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea). Secondo alcuni, infatti, questa scelta avrebbe

> «contribuito a trasformare l'approccio delle istituzioni, in questa materia, da una configurazione prevalentemente *market-driven* a una *fundamental rights-oriented*. La direttiva infatti risentiva ancora di una visione in larga parte mercantilistica, improntata a garantire la libera circolazione dei dati personali, considerati nella loro peculiare natura di asset economico e non ancora in una prospettiva legata alla tutela dei diritti fondamentali» (Bassini 2016, 588).

[25] A questo proposito cfr. la Raccomandazione (UE) 2019/243 della Commissione, del 6 febbraio 2019, relativa a un formato europeo di scambio delle cartelle cliniche elettroniche.

All'interno di quest'analisi, un ulteriore elemento da considerare è costituito dalla nuova definizione di "dato personale" adottata all'interno del RGPD, una definizione molto ampia – e secondo alcuni, talmente ampia da risultare potenzialmente onnicomprensiva, con il rischio di vanificare, *in limine*, la stessa tutela predisposta dal nuovo impianto normativo (PURTOVA 2018). In base a tale nuova definizione offerta dall'art. 4 del Regolamento, infatti, «qualsiasi informazione riguardante una persona fisica identificata o identificabile» rappresenta un dato personale. Più in particolare, la persona fisica – definita anche come "interessato" – è considerata identificabile nel momento in cui essa possa 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» (RGPD, art. 4).

Se, per un verso, l'ampiezza di tale definizione potrebbe ascriversi alla volontà di prevedere una categoria elastica, quindi in grado di ricomprendere nuove fattispecie che dovessero sorgere in futuro a seguito dell'evoluzione tecnologica, per un altro, alcuni hanno sottolineato che questa scelta deve essere interpretata come il segno del recepimento di alcuni orientamenti emersi in seno alla dottrina statunitense in materia, per effetto dei quali l'ampiezza (o vaghezza) definitoria è da ricondurre al superamento della dicotomia tra dato personale e dato anonimo, a cui si affiancano una serie di misure preventive volte all'attenuazione del rischio di violazione della privacy (COLAPIETRO 2018, 15). Per le finalità di questo lavoro, vale la pena sottolineare che tali orientamenti muoverebbero dalla presa d'atto del fallimento dei procedimenti di anonimizzazione e, in particolare, dalla consapevolezza per cui la distinzione tra dato personale e dato anonimo non sia più adeguata alla luce delle esigenze confliggenti di protezione dei dati stessi e circolazione di questi ultimi (DUCATO 2016, 164).

A questo proposito, va detto che, sebbene non siano mancati in dottrina i riferimenti alla "doppia natura" dei dati personali così come protetti all'interno del Regolamento – ovvero come bene economico e, al contempo, oggetto di un diritto fondamentale (FINOCCHIARO 2018, 896) – alcuni hanno espresso posizioni maggiormente critiche rispetto all'ammodernamento dell'impianto di protezione dei dati operato dal Regolamento. Nello specifico, esso è stato considerato come

> «una retrocessione sul terreno della protezione della persona, poiché reitera forme di salvaguardia dell'individuo per lo più di matrice individuale (consenso, diritti degli interessati, risarcimento del danno etc.) ma, nonostante l'evoluzione dei trattamenti dei dati personali, non percorre in maniera adeguata la via della difesa dei diritti individuali della persona sul piano pubblico e addirittura trascura il versante della tutela collettiva» (PIRAINO 2017, 405).

Altri ancora hanno ritenuto "deludente" il tenore della nuova normativa di protezione dei dati personali, soprattutto con riferimento al bilanciamento compiuto tra diritti fondamentali ed esigenze di mercato, il quale sembrerebbe

> «avvalorare un'accezione sempre più spersonalizzata di dati personali con un approccio lontano dalla sensibilità di chi sottolinea il valore giuridico della persona nella sua unitarietà e complessità. In altre parole, il termine dato personale sembra impoverirsi fino a rinnegare il suo potenziale rappresentativo per ridursi a qualcosa di algido e sterile, in sintonia con l'entusiasmo per le enormi potenzialità dei Big Data, che consentono di ricostruire informazioni preziose anche da frammenti di dati apparentemente privi di specifici elementi identificativi» (THIENE 2017, 410).

4.1. *Ambito di applicazione del RGPD e principi applicabili al trattamento*

La delimitazione dell'ambito di applicazione del Regolamento è da annoverarsi fra le novità di questa disciplina che ne sancisce un notevole ampliamento rispetto a quello offerto dalla Direttiva 95/46/CE. In questo contesto, il legislatore europeo dimostra di aver recepito i più recenti orientamenti della Corte di Giustizia[26] che ha dimostrato un "singolare attivismo" in questa materia (BASSINI 2016, 587)[27]. Per effetto dell'art. 3, il Regolamento si applica ad ogni attività posta in essere da «un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione»[28]. Al ricorrere di determinate condizioni, tuttavia, il RGPD si applica anche al trattamento effettuato dal titolare o dal responsabile che non siano stabiliti all'interno dell'Unione[29], il che comporta l'applicabilità della disciplina europea anche a quei trattamenti effettuati al di fuori dell'Unione europea, a condizione che i servizi collegati a tali trattamenti siano offerti a interessati che si trovano al suo interno[30].

Per quanto concerne l'ambito di applicazione materiale del Regolamento, esso ricomprende il «trattamento interamente o parzialmente automatizzato di dati personali e [il] trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi»[31]. Il Regolamento stabilisce i principi applicabili al trattamento, ovvero: liceità, correttezza e trasparenza[32]; limitazione delle finalità (affinché i dati siano raccolti per finalità delimitate, esplicite e legittime)[33]; minimizzazione dei dati (in modo che siano raccolte esclusivamente quelle informazioni necessarie a soddisfare le finalità previste)[34]; esattezza dei dati[35] e limitazione della loro conservazione per un lasso temporale non superiore a quello necessario[36]; integrità e riservatezza dei dati[37]. All'interno di questi principi, un rilievo particolare è assunto dalla liceità, che sussiste solo laddove l'interessato abbia espresso il proprio consenso al trattamento oppure nel caso in cui il trattamento appaia necessario al raggiungimento di una delle finalità tassativamente stabilite[38].

Prescrizioni più stringenti valgono per le categorie particolari di dati (già dati sensibili) che, ai sensi della disciplina in esame, includono non solo ogni dato idoneo a rivelare informazioni

[26] A questo proposito, si vedano, in particolare, le seguenti sentenze della Corte europea di giustizia: Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González; Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a. Per un approfondimento in materia cfr. FINOCCHIARO 2015.

[27] Sul tema cfr. anche POLLICINO 2014. Per un approfondimento sul ruolo assunto sulla nozione dello stabilimento all'interno del RGPD si veda estesamente STANZIONE 2016.

[28] RGPD, art. 3.

[29] RGPD, art. 3.

[30] Come sottolineato da COLAPIETRO 2018, 9, per stabilire caso per caso l'applicabilità territoriale del regolamento vengono in soccorso i considerando del Regolamento, e in particolare, i nn. 23 e 24. Inoltre, un rilievo centrale assume a questo proposito la nozione di "stabilimento" espressamente richiamata all'interno della giurisprudenza della Corte di Giustizia.

[31] RGPD, art. 1.

[32] RGPD, art. 5.1, lett. a.

[33] RGPD, art. 5.1, lett. b.

[34] RGPD, art. 5.1, lett c.

[35] RGPD, art. 5.1, lett. d.

[36] RGPD, art. 5.1, lett. e.

[37] RGPD, art. 5.1, lett. f.

[38] In base al dettato dell'art. 6, invero, affinché il trattamento dei dati sia considerato come lecito, è necessario che l'interessato abbia espresso il proprio consenso allo stesso, oppure che il trattamento sia necessario per raggiungere una delle seguenti finalità: *i*) esecuzione di un contratto di cui l'interessato è parte o di misure precontrattuali adottate su sua richiesta; *ii*) adempimento di un obbligo legale gravante in capo al titolare del trattamento; *iii*) salvaguardia di interessi vitali dell'interessato o di altra persona fisica; *iv*) esecuzione di un compito di interesse pubblico o relativo all'esercizio di poteri pubblici attribuiti al titolare del trattamento; *v*) perseguimento di un legittimo interesse detenuto dal titolare del trattamento o da terzi, fatto salvo il caso in cui debba darsi prevalenza agli interessi, ai diritti o alle libertà fondamentali della persona fisica a cui i dati pertengono.

come origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche e appartenenza sindacale, ma anche i dati genetici, i dati biometrici e i dati relativi alla salute, alla vita e all'orientamento sessuale degli individui interessati[39]. Alla regola generale che vieta il trattamento di tali dati[40] segue una serie di eccezioni dallo spettro potenzialmente molto ampio. In primo luogo, tali categorie di dati possono essere trattati ogni volta in cui vi sia un consenso esplicito da parte dell'interessato[41] o nel caso in cui sia stato egli stesso a renderli pubblici[42]. Inoltre, il trattamento di tali dati è consentito laddove ciò sia necessario per il perseguimento di finalità più specifiche, tra cui: assolvere agli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza e protezione sociale[43]; tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso[44]; espletare le attività proprie di una fondazione, associazione o di altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali[45]; accertare, esercitare o difendere un diritto in sede giudiziaria[46]; soddisfare esigenze di carattere pubblico[47]; perseguire finalità che rientrano nell'ambito della medicina preventiva o della medicina del lavoro[48]; soddisfare esigenze di interesse pubblico attinenti al settore della sanità pubblica[49]; perseguire finalità di interesse pubblico relative all'archiviazione, alla ricerca scientifica, o in ambito storico e statistico[50]. Com'è evidente da tale serie di casi, un ruolo fondamentale è qui assunto dalla nozione di interesse pubblico, dalla cui definizione dipende lo spazio di discrezionalità esercitabile dagli Stati membri, i quali possono eventualmente calibrare tale nozione in base alla volontà di allargare o restringere il novero delle finalità reputate meritevoli di interesse.

In sintesi, alla luce della disciplina offerta dal RGPD, è possibile affermare che il trattamento dei dati personali deve essere lecito e limitato alle finalità specifiche assunte dal trattamento stesso. I dati raccolti devono essere esatti e le forme di archiviazione devono essere tali da facilitare il loro trattamento, cancellazione e rettifica senza ritardo. Inoltre, gli stessi devono essere conservati per il periodo di tempo necessario al raggiungimento delle finalità per le quali erano stati raccolti. I dati devono essere trattati in modo che gli stessi siano protetti da eventuali utilizzi non autorizzati o illeciti, e devono essere salvaguardati con adeguati accorgimenti tecnici e organizzativi per evitare che possano andare persi, distrutti, o accidentalmente danneggiati.

4.2. Accountability *e principio di precauzione: la nuova visione della protezione dei dati personali*

Come sottolineato in precedenza, l'adozione di una definizione potenzialmente onnicomprensiva di dato personale sembra accompagnarsi a una – pur non manifesta – presa d'atto delle difficoltà di garantire una completa anonimizzazione dei dati nell'era digitale. A ciò fa da *pendant* il sorgere di una nuova visione del sistema di protezione dei dati stessi, ispirata ai principi di pre-

[39] RGPD, art. 9. Per un approfondimento sulle categorie particolari di dati si veda Granieri 2017.
[40] RGPD, art. 9.
[41] RGPD, art. 9.
[42] RGPD, art. 9.2, lett. e.
[43] RGPD, art. 9.2, lett. b.
[44] RGPD, art. 9.2, lett. c.
[45] RGPD, art. 9.2, lett. d. In questo caso devono comunque essere adottate determinate garanzie tra cui, che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con tale ente.
[46] RGPD, art. 9.2, lett. f.
[47] RGPD, art. 9.2, lett. g.
[48] RGPD, art. 9.2, lett. h.
[49] RGPD, art. 9.2, lett. i.
[50] RGPD, art. 9.2, lett. l.

cauzione e di prevenzione dei rischi per i diritti e per le libertà delle persone interessate (STANZIONE 2016, 1261). All'interno del Regolamento tale visione assume le forme di un'*accountability* – un dovere di dare conto – attribuito al titolare del trattamento, in particolare dall'art. 32, il quale assume il fine di stimolare «l'adozione di comportamenti proattivi e di misure idonee a dimostrare ed assicurare la corretta applicazione della disciplina europea, in una prospettiva di tutela preventiva, basata su diversi istituti che si iscrivono in una prospettiva di carattere responsabilizzante» (COLAPIETRO 2018, 27)[51].

Tra questi ultimi rientrano sicuramente i principi della *privacy by design* e *privacy by default*[52], ma soprattutto, per le finalità proprie di questo lavoro, la valutazione d'impatto preventiva, da effettuarsi nel caso di trattamento di alcune categorie di dati, fra cui quelli raccolti e/o elaborati per mezzo delle "nuove tecnologie"[53]. Al di là di quest'ipotesi specifica, il RGPD assegna al titolare del trattamento l'onere di effettuare tale valutazione in considerazione della natura dei dati raccolti, del loro oggetto, del contesto e delle finalità del trattamento[54]. Nondimeno, all'interno di questa cornice di discrezionalità riconosciuta al titolare del trattamento, il RGPD prevede anche che tale valutazione debba comunque effettuarsi nel caso di trattamenti automatizzati che coinvolgono aspetti personali degli interessati su cui possano fondarsi «decisioni che hanno effetti giuridici» o altrimenti in grado di incidere significativamente sulla loro sfera personale. Inoltre, la valutazione d'impatto è espressamente richiesta anche nel caso di trattamento su larga scala di dati sensibili e di dati relativi a reati e/o a condanne penali, e nel caso di «sorveglianza sistematica su larga scala di una zona accessibile al pubblico»[55]. In questo contesto, il Regolamento prescrive l'adozione di procedimenti di pseudonimizzazione e cifratura dei dati in oggetto, a cui corrispondono altrettanti certificati di autenticità e meccanismi per l'autenticazione dei soggetti abilitati all'accesso. Inoltre, appare degno di nota che esso suggerisca anche l'adozione di iniziative volte alla formazione e alla sensibilizzazione del personale coinvolto nelle attività di trattamento[56], eventualmente attraverso la definizione di appositi codici di condotta che assumono il fine di contribuire alla sua corretta applicazione[57].

Da diverso punto di vista, il RGPD cerca anche di rafforzare le condizioni che sottostanno all'ottenimento del consenso presso gli interessati, prescrivendo che la relativa richiesta sia «presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro»[58].

Infine, all'interno della nuova concezione di protezione dei dati adottata dal RGPD deve annoverarsi il rinnovato ruolo attribuito alle Autorità nazionali di controllo, soprattutto per quanto concerne il controllo su alcuni spazi di "flessibilità" contenuti all'interno del nuovo impianto normativo (PIZZETTI 2018, 108). In particolare, il ruolo delle Autorità diviene preminente in una serie di casi, tra cui, *in primis*, nell'ambito della valutazione d'impatto preventiva dianzi richiamata[59], soprattutto laddove il rischio di nocumento ai diritti e alle libertà dei singoli appaia elevato, caso in cui il titolare deve obbligatoriamente consultare l'Autorità[60]. Inoltre, alle Autorità

[51] Sul punto si veda anche FINOCCHIARO 2017; TOMMASI 2019; LUCCHINI GUASTALLA 2018.
[52] RGPD, art. 25.
[53] RGPD, art. 35.1.
[54] RGPD, art. 35.1.
[55] RGPD, art. 35.3
[56] RGPD, art. 39.
[57] RGPD, art. 40.
[58] RGPD, art. 7.2.
[59] E più precisamente, per «redige[re] e rende[re] pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati» (RGPD, art. 35, co. 4), ed eventualmente anche per «redige[re] e rende[re] pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto» (RGPD, art. 35.5).
[60] RGPD, art. 36.1.

di controllo spettano ulteriori compiti di consulenza (al Parlamento, al Governo e a tutti gli organismi e/o le istituzioni coinvolti/e dall'applicazione del Regolamento), di vigilanza sull'applicazione del Regolamento e di promozione della consapevolezza del pubblico riguardo «ai rischi, alle norme alle garanzie e ai diritti in relazione ai trattamenti»[61]. Infine, alle Autorità di controllo sono attribuiti compiti rilevanti nell'ambito dell'istituzione dei meccanismi di certificazione della protezione dei dati[62] e dei summenzionati codici di condotta.

In virtù di quanto precede, pertanto, è possibile convergere con l'analisi di chi ha sottolineato che, in parallelo all'adozione della nuova concezione di protezione dei dati da parte del Regolamento, anche il ruolo stesso delle Autorità di controllo sia stato ridisegnato in senso "dinamico", dal che discende che la tutela della protezione dei dati personali non possa più essere intesa esclusivamente in quanto «diritto fondamentale dei cittadini ma anche come un valore sociale di diritto pubblico europeo» (PIZZETTI 2018, 109). Da un punto di vista parzialmente differente, è stato evidenziato che, in uno scenario sempre più marcatamente ispirato all'interconnessione globale, gli spazi d'azione (e d'interpretazione) del diritto nazionale restano significativi, circostanza che pone le Autorità di controllo dinanzi al compito di adeguarsi al fine «di seguire costantemente i processi tecnologici; di valutarne le conseguenze sull'uso dei dati personali; di assicurare una costante informazione sulle conseguenze che le nuove tecnologie, e i trattamenti che comportano, possono presentare per tutta la comunità di riferimento» (PIZZETTI 2018,110). In questo senso, pertanto, è possibile affermare che la protezione dei dati, benché ancorata alla tutela di un diritto individuale, debba essere più correttamente intesa nella sua dimensione di interesse pubblico, e quindi «presidiata non solo a tutela dell'interessato e a sua richiesta ma anche in via generale e preventiva» (PIZZETTI 2018, 111)[63].

4.3. *L'incidenza del RGPD sulle attività di erogazione dei servizi sanitari a distanza*

L'assenza di una trattazione specifica dei dati sanitari all'interno del RGPD, se da un lato può essere letta come una volontà di non differenziarne la protezione da quella relativa alle ulteriori "categorie particolari" di dati personali, sorprende tuttavia alla luce degli ingenti sforzi condotti negli ultimi anni dalle istituzioni europee per stimolare la diffusione dei servizi mediati da TIC all'interno degli Stati membri[64]. Dall'analisi del Regolamento si evince che la nozione di dato sanitario ricomprende tutti i dati «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»[65]. A ciò si deve tuttavia aggiungere quanto espresso nella parte introduttiva dello stesso Regolamento dove, in linea con l'ampia definizione di dato personale a cui si è fatto cenno in precedenza, si suggerisce un'altrettanto ampia accezione di dato sanitario. Essa, infatti, include:

> «tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla

[61] RGPD, art 57.1, lett. b.
[62] RGPD, art. 42
[63] Sul nuovo ruolo delle autorità si veda anche CUFFARO 2018. Per un approfondimento sugli aspetti relativi ai procedimenti attivabili a seguito di violazione della normativa sulla protezione dei dati personali, invece, si rinvia all'analisi di MARIOTTINI 2016, 908 ss.
[64] Si veda sinteticamente *supra*, § 3.
[65] RGPD, art. 4.14.

> in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro»[66].

All'assenza di disposizioni specificamente rivolte alla protezione dei dati sanitari, corrisponde, peraltro, la mancanza di qualsivoglia riferimento all'utilizzo dei servizi mediati dalle TIC in ambito sanitario. Tuttavia, l'esame attento del testo del Regolamento consente di identificare alcuni elementi la cui analisi può essere di interesse per le finalità proprie di questo lavoro, soprattutto tenuto conto degli sviluppi più recenti delle TIC in sanità e, in particolare, della già richiamata proliferazione di app per la salute (*supra*, § 2). A questo proposito, pertanto, occorre menzionare, in primo luogo, il concetto di "profilazione", definito come

> «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica»[67].

Per espresso disposto del Regolamento, infatti, l'interessato ha il diritto di «non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»[68]. Questa sorta di "diritto di opposizione" può interessare le TIC in sanità dal momento che, come già anticipato, nella pratica medica si va diffondendo il ricorso a servizi e dispositivi tecnologici che integrano funzioni di *data-mining* per ottenere un'indicazione utilizzabile non solo a fini collettivo-statistici, ma anche nell'ambito del processo diagnostico e/o terapeutico inerente al singolo paziente[69]. Tuttavia, dal momento che obiettivo precipuo del Regolamento non è porre al vaglio i processi di digitalizzazione dell'assistenza sanitaria[70], ma apprestare un'adeguata tutela dei dati che attraverso quelli vengono trattati, si prevede la possibilità di acconsentire alla profilazione, per esempio, nell'esecuzione di un contratto di cui il soggetto interessato è parte, oppure nel caso di perseguimento di un interesse pubblico afferente all'ambito della sanità pubblica[71].

Un'altra disposizione del RGPD che può incidere direttamente sulle attività di erogazione dei servizi sanitari a distanza è quella relativa alle forme del consenso informato. Ai sensi della nuova disciplina, il titolare del trattamento dei dati non è obbligato a documentare per iscritto l'apposizione del consenso, né la forma scritta è richiesta in via esclusiva a tal fine[72]. Sebbene la forma scritta svolga una funzione innegabile di chiarificazione e agevoli la dimostrazione della

[66] RGPD, art. 4.14, considerando n. 35.
[67] RGPD, art. 4.4.
[68] RGPD, art. 22.1.
[69] Tra gli esempi più noti in questo ambito vi è l'elaboratore elettronico IBM Watson, ma non bisogna dimenticare la miriade di app per dispositivi mobili che offrono agli utenti elaborazioni di dati ottenute tramite algoritmi, le quali sono presentate come il risultato di un'autentica *medical expertise*, anche per via dell'utilizzo di interfaccia grafiche di facile utilizzo e di ispirazione "antropomorfa".
[70] Per una disamina più ampia delle implicazioni etiche, giuridiche e sociali derivanti dall'incedere dei processi di digitalizzazione dell'assistenza sanitaria sia consentito rinviare a BOTRUGNO 2020b.
[71] RGPD, art. 22.
[72] RGPD, in particolare, art. 7.2.

sua inequivocabilità – requisito introdotto per la prima volta dal RGPD stesso –, è evidente che la possibilità di digitalizzarne l'apposizione possa favorire notevolmente la diffusione dei servizi a distanza (non solo quelli sanitari).

Una menzione particolare merita il nuovo ruolo assunto dal Responsabile della protezione dei dati (RPD), che alla luce del nuovo impianto normativo è chiamato a svolgere funzioni di natura trasversale che «intersecano le questioni di cybersicurezza con gli aspetti di *compliance* sul piano giuridico» (PEDRAZZI 2019, 181) e che sono da ricondurre a un ruolo di supervisore «che mantenga il controllo del rispetto della normativa in materia e funga da punto di contatto con l'autorità di controllo, nonché nei confronti degli interessati che intendano esercitare i propri diritti» (PEDRAZZI 2019, 181).

Come chiarito dal Garante nazionale a integrazione delle apposite Linee Guida adottate dal Gruppo di Lavoro ex art. 29[73], la designazione di un RPD è obbligatoria per le «società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione». Questa figura deve operare in regime di «indipendenza organizzativa ed operativa» in modo da garantire trasparenza del proprio operato, soprattutto alla luce della necessità di evitare il conflitto di interessi, una questione rispetto alla quale le autorità di controllo di alcuni paesi membri dell'Unione si sono già pronunciate[74].

Da diverso punto di vista, deve essere evidenziato che il RGPD rimanda espressamente alla revisione di alcuni atti normativi il cui ambito di applicazione può influire sulla disciplina della protezione dei dati personali[75], circostanza che può investire l'oggetto di questo lavoro, soprattutto con riferimento alla Direttiva 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche[76], anche nota come Direttiva *ePrivacy*. Infatti, sebbene tale Direttiva non includa esplicitamente l'ambito sanitario nel proprio ambito di applicazione[77], alcune previsioni possono interessare i servizi mediati dalle TIC, soprattutto laddove si tratti di servizi offerti per il tramite di *health apps*. La Direttiva 2002/58/CE, da una parte, impone ai fornitori di servizi di adottare misure tecniche e organizzative tali da assicurare la sicurezza delle comunicazioni elettroniche[78]; dall'altra attribuisce alle competenti autorità degli Stati membri l'onere di garantire la riservatezza delle stesse[79]. In accordo con la revisione intermedia dell'attuazione della strategia per il Mercato Unico Digitale[80] la Commissione europea ha dato seguito all'esigenza sopra menzionata, presentando una proposta di Regolamento[81] destinata a sostituire la Direttiva 2002/58/CE. La proposta di Regolamento è intesa come *lex specialis* rispetto al RGPD, il che implica che per ogni aspetto non espressamente disciplinato dal primo si debba fare riferimento al secondo. In questo senso, sebbene i principi su cui si reggeva la Direttiva

[73] Si vedano Faq sul Responsabile della Protezione dei Dati in ambito privato adottate in aggiunta a quelle adottate dal Gruppo Art. 29, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793 (consultato il 23/08/2020).

[74] In particolare PEDRAZZI 2019 riporta un caso di incompatibilità allo svolgimento delle funzioni di RPD deciso dall'autorità di controllo della regione tedesca della Bavaria, e il caso dell'autorità spagnola, la prima ad aver introdotto un meccanismo di certificazione per il ruolo di RPD. Quest'ultimo tuttavia, è stato ritenuto inadeguato dal Garante italiano.

[75] RGDP, considerando introduttivo n. 173.

[76] 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.

[77] La Direttiva 2002/58/CE si applica infatti «al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nella Comunità» (art. 3.1).

[78] Direttiva 2002/58/CE. In materia di sicurezza delle comunicazioni elettroniche, si veda anche la Direttiva 2016/1148/UE, anche nota con l'acronimo "NIS", e avente per oggetto la sicurezza dei sistemi informativi.

[79] Direttiva 2002/58/CE, art. 5.

[80] Commissione europea, Comunicazione 2017/228, *Costruire un'economia dei dati europea*.

[81] Commissione europea, *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la Direttiva 2002/58/CE*, COM/2017/010.

2002/58/CE siano ritenuti ancora validi[82], la Commissione ha manifestato la necessità di adeguarne le disposizioni agli sviluppi tecnologici più recenti. Ad avviso della Commissione, infatti

> «I consumatori e le imprese si sono affidati sempre più ai nuovi servizi basati su internet intesi a consentire le comunicazioni interpersonali, quali il voice-over-IP, la messaggistica istantanea e i servizi di posta elettronica basati sulla rete anziché fruire dei servizi di comunicazione tradizionali. Questi servizi di comunicazione over-the-top ("OTT") non sono di norma soggetti all'attuale quadro di riferimento dell'Unione per le comunicazioni elettroniche, compresa la direttiva sulla vita privata elettronica. Ne consegue che la direttiva non è al passo con gli sviluppi tecnologici, il che si traduce in una lacuna nella tutela delle comunicazioni effettuate mediante i nuovi servizi»[83].

Su questa materia, tuttavia, è intervenuto di recente l'*European Data Protection Board* (EDPB) con un apposito parere finalizzato a chiarire se e in che misura il RGPD e la Direttiva *ePrivacy* si sovrappongono o, piuttosto, si integrano[84]. In particolare, l'EDPB ha richiamato l'attenzione sul fatto che già all'interno del RGPD – in particolare, all'art. 95 e al considerando n. 173 –, si conferma che il rapporto tra le due discipline è rispettivamente quello che sussiste tra *lex generalis* e *lex specialis*[85]. Ciò si evince, peraltro, dallo stesso art. 95 richiamato dal parere dell'EDPB, secondo cui il RGPD

> «non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE».

5. *La disciplina nazionale tra adeguamento del Codice in materia di protezione dei dati personali e contributo del Garante*

Il d.lgs. n. 101/2018 ha modificato il d.lgs. n. 196/2003, meglio noto come Codice in materia di protezione dei dati personali, al fine di renderlo conforme alle prescrizioni contenute all'interno del nuovo impianto normativo predisposto in sede comunitaria. Tale modifica, peraltro, ha portato alla soppressione di molte delle precedenti disposizioni del Codice, dal momento che il nuovo asse portante della disciplina in materia di protezione dei dati personali è ora costituito dal Regolamento stesso. Tuttavia, contravvenendo in parte alla propria natura di fonte normativa direttamente applicabile all'interno degli Stati membri, il Regolamento, da una parte, ha richiesto ai legislatori nazionali una serie di interventi attuativi per favorire l'adozione di una disciplina di dettaglio in alcuni settori mentre, dall'altra, ha contemplato alcuni interventi facoltativi, il tenore dei quali, evidentemente, non può avere per effetto di derogare la normativa contenuta al suo interno[86].

[82] Si veda a questo proposito il rapporto della Commissione europea *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, disponibile in: https://ec.europa.eu/digital-single-market/en/news/evaluation-and-review-directive-200258-privacy-and-electronic-communication-sector (consultato il 24/08/2020).

[83] Commissione europea, *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche*, cit.

[84] EDPB, *Opinion n. 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*.

[85] EDPB, *Opinion n. 5/2019*, 12.

[86] Sul punto si veda COLAPIETRO 2018, 28, il quale si sofferma sul più generale rapporto di stretta implicazione che sussiste tra il RGPD e il Codice per la protezione dei dati personali così come novellato dal d.lgs. n. 101/2018. Tale rapporto, peraltro, diventa anche di tipo funzionale nella misura in cui il RGPD assume il ruolo di parametro di

Come visto *supra* (§ 4), il Regolamento prevede un divieto generale di trattamento delle categorie particolari di dati personali, a cui fa seguito una serie di eccezioni, fra cui spiccano quelle giustificate dai motivi di "interesse pubblico", nozione che, tuttavia, non è ulteriormente determinata. Attraverso il d.lgs. n. 101/2018, il legislatore italiano scioglie ogni dubbio e definisce rilevante l'interesse pubblico «relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri». Fra questi rientrano:

> «t) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano; u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica; v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale»[87].

Da diverso punto di vista, il Regolamento attribuisce agli Stati membri la facoltà di mantenere o introdurre «ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute»[88]. È in quest'ottica che va inquadrato il dettato del d.lgs. n. 101/2018, volto a garantire che il trattamento dei dati riconducibili a tali categorie avvenga previa emanazione di "misure di garanzia" adottate da parte del Garante per la protezione dei dati personali. Tali misure devono essere formulate tenuto conto:

> «a) delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali; b) dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure; c) dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea»[89].

Le misure di garanzia devono essere adottate per ciascuna delle tre categorie di dati menzionate e commisurate alle finalità specifiche del trattamento. L'adozione delle stesse può inoltre ricomprendere, da una parte, la definizione di ulteriori condizioni volte ad assicurare la legittimità del trattamento dei dati sensibili e, dall'altra, quella di misure di sicurezza, tra cui le «tecniche di cifratura e di pseudonimizzazione, le misure di minimizzazione, le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a garantire i diritti degli interessati»[90].

A differenza del RGPD, che, come già messo in evidenza, non prevede disposizioni specificamente rivolte alla protezione dei dati sanitari, nella Parte II[91], il Codice per la protezione dei dati personali ospita ora un Titolo V specificamente dedicato al «Trattamento di dati personali

legittimità per l'interpretazione delle disposizioni del Codice.

[87] Cfr. d.lgs. n. 101/2018, art. 2-sexies, co. 2. Si rammenta, inoltre, che ai casi già menzionati vanno aggiunti quelli ulteriori in cui l'ammissibilità del trattamento sia prevista «dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato» (D.lgs. n. 101/2018, art. 2-sexies, co. 1).

[88] RGPD, art. 9.4.

[89] Cfr. d.lgs. n. 101/2018, art. 2-septies, co. 1-2.

[90] D.lgs. n. 101/2018, art. 2-septies, co. 5.

[91] Il Titolo V del Codice in materia di protezione dei dati personali comprende gli artt. da 75 a 94, ed è rubricato «Disposizioni specifiche per i trattamenti necessari per adempiere ad un obbligo legale o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri nonché disposizioni per i trattamenti di cui al Capo IX del Regolamento».

in ambito sanitario», che fornisce indicazioni di dettaglio sui doveri incombenti in capo ai professionisti sanitari affinché sia garantito l'adempimento degli obblighi informativi inerenti alla raccolta e al successivo trattamento dei dati personali. In particolare, le forme attraverso cui tali obblighi sono espletati devono essere tali da evidenziare in maniera analitica l'eventualità di «rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato»[92]. Il Codice procede poi a specificare alcune situazioni nell'ambito delle quali si ritiene che il trattamento dei dati presenti di per sé siffatto genere di rischi. Per le finalità proprie di questo lavoro, è opportuno ricordare che fra tali situazioni vi sono: il trattamento dei dati effettuato per il tramite di telemedicina (o teleassistenza); quello relativo alla prestazione di servizi o alla fornitura di beni effettuato tramite una rete di comunicazione elettronica; quello necessario ai fini dell'implementazione del fascicolo sanitario elettronico[93], dei sistemi di sorveglianza sanitaria e dei registri istituiti al fine di «registrare e caratterizzare tutti i casi di rischio per la salute, di una particolare malattia o di una condizione di salute rilevante in una popolazione definita»[94].

In questo contesto, un apporto fondamentale per far luce sui dubbi interpretativi sollevati a seguito dell'emanazione del RGPD è stato offerto dal Garante, a cui, peraltro, il legislatore nazionale, per il tramite del d.lgs. n. 101/2018[95], aveva affidato il compito di adottare misure di garanzia *ad hoc* e di promuovere l'adozione di regole deontologiche nell'ambito dei trattamenti aventi ad oggetto dati sanitari. A questo proposito, il Garante ha ritenuto opportuno «fornire alcuni chiarimenti sull'applicazione della disciplina di protezione dei dati in ambito sanitario»[96]. Nello specifico, il Garante ha ribadito che al divieto di trattare le cc.dd. categorie particolari di dati personali ex art. 9 del Regolamento seguono una serie di eccezioni, tra cui, per quanto concerne i dati sanitari: motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri[97]; motivi di interesse pubblico nel settore della sanità pubblica[98]; finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari e sociali[99]. Da ciò discende che «Gli eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari, richiedono, quindi, anche se effettuati da professionisti della sanità, una distinta base giuridica da individuarsi, eventualmente, nel consenso dell'interessato o in un altro presupposto di liceità»[100]. All'interno di questa categoria di trattamenti, il Garante annovera: i trattamenti relativi all'utilizzo di app mediche che non siano riconducibili alla telemedicina e quelli ai cui dati possano avere accesso soggetti sui quali non incombe l'onere del segreto professionale; i trattamenti rivolti alla fidelizzazione della clientela; i trattamenti effettuati in ambito sanitario da soggetti privati per finalità promozionali e/o commerciali; i trattamenti effettuati da professionisti sanitari per finalità commerciali o eletto-

[92] Titolo V del Codice in materia di protezione dei dati personali, art. 78.5.

[93] Cfr. art. 12 d.l. n. 179/2012, convertito, con modificazioni, dalla l. n. 221/2012.

[94] Art. 12 d.l. n. 179/2012. Qui il riferimento è ai «registri di mortalità, di tumori e di altre patologie, di trattamenti costituiti da trapianti di cellule e tessuti e trattamenti a base di medicinali per terapie avanzate o prodotti di ingegneria tessutale e di impianti protesici».

[95] In particolare, artt. 2-septies e 2-quater. Ma si vedano anche gli artt. 20 e 21 dello stesso decreto che affidano al Garante il compito di verificare la compatibilità delle prescrizioni contenute nelle autorizzazioni generali sul trattamento dei dati sensibili al RGPD, compito che il Garante ha evaso con il provvedimento del 13 dicembre 2018 (n. 9068972).

[96] Cfr. il documento redatto dal Garante, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, n. 9091942 del 7 marzo 2019.

[97] RGPD, art. 2, lett. g.

[98] RGPD, art 9.2, lett. i.

[99] RGPD, art. 9.2 lett. h e art. 9.3. Rispetto a quest'ultima categoria di dati, in particolare, il Garante segnala che «Diversamente dal passato, quindi, il professionista sanitario, soggetto al segreto professionale, non deve più richiedere il consenso del paziente per i trattamenti necessari alla prestazione sanitaria richiesta dall'interessato», cfr. punto 1 dei *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito* sanitario, cit.

[100] RGPD, art. 9.2 lett. h e art. 9.3.

rali; i trattamenti effettuati attraverso il Fascicolo sanitario elettronico (FSE) di cui al d.l. n. 179/2012, nell'ambito del quale è richiesta l'acquisizione del consenso dell'interessato[101].

Il Garante interviene anche in relazione ai trattamenti effettuati tramite il "dossier sanitario", il quale si distingue nettamente dal FSE. Se infatti quest'ultimo è costituito da «l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito»[102], il primo, invece, è composto da «l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, messi in condivisione logica a vantaggio dei professionisti sanitari che presso lo stesso titolare del trattamento lo assistono»[103]. A questo proposito, il Garante ricorda come il consenso per l'inclusione dei dati personali all'interno del dossier fosse già richiesto dalle linee guida emanate dalla stessa autorità di controllo nel 2009, quindi anteriormente all'emanazione del RGPD[104]. Tuttavia, il Garante stesso si riserva di «individuare, nell'ambito delle misure di garanzia da adottarsi sulla base dell'art. 2-septies del Codice, i trattamenti che, ai sensi dell'art. 9, par. 2, lett. h), possono essere effettuati senza il consenso dell'interessato»[105].

In questa sede deve essere anche ricordato che il Garante ha apportato un contributo fondamentale anche in sede di accertamento delle violazioni della privacy dei pazienti, soprattutto per quanto concerne le modalità di archiviazione elettronica dei dati sanitari[106]. In questo contesto è emerso come spesso le misure di sicurezza adottate dalle istituzioni sanitarie interessate dall'attività di accertamento fossero inadeguate al fine di prevenire l'accesso a tali dati da parte di soggetti che, pur lavorando nella stessa azienda, non avevano diritto di accedervi. Come già messo in luce dalla stessa Autorità, infatti, i rischi principali riscontrati nel corso dell'attività ispettiva condotta in quest'ambito sono da ricondurre alla circostanza per cui

> «nella maggior parte dei dossier sanitari esaminati gli stessi sono stati sviluppati in modo non strutturale e organizzato, bensì partendo da alcune iniziative estemporanee di informatizzazione delle cartelle cliniche di reparto o di ambulatorio e, quindi, senza tener conto del fatto che si andava predisponendo un sistema informativo in grado di gestire potenzialmente l'intera storia clinica di un individuo. Ciò ha determinato la realizzazione di sistemi in cui la mancanza di certezza sull'autenticità delle informazioni presenti, la possibilità che le stesse siano accessibili e modificabili da parte di soggetti non legittimati o siano persino diffuse, la non disponibilità delle stesse costituiscono rischi reali per lo più non considerati dalle strutture sanitarie almeno nelle prime fasi di realizzazione dei dossier»[107].

6. *La tempesta perfetta: la diffusione del CoViD-19 e la strategia (digitale) per il contenimento del contagio*

Come noto, la diffusione del CoViD-19 a livello globale ha avuto un impatto devastante sulla salute e sulla vita di moltissime persone, rendendo necessaria l'adozione di misure straordinarie per il contenimento del contagio tra la popolazione che, a loro volta, si sono tradotte in una re-

[101] Cfr. art. 12, co. 5, nonché art. 79 del Codice novellato. Per un'analisi più ampia relativa a FSE e dossier sanitario si veda CALIFANO 2015.

[102] Cfr. art. 12, d.l. n. 179/2012, cit.

[103] Cfr. le *Linee guida in materia di dossier sanitario*, *Allegato A alla deliberazione del Garante del 4 giugno 2015*, 6.

[104] Si veda la deliberazione del Garante del 4 giugno 2015, a cui le *Linee guida in materia di dossier sanitario* sono allegate.

[105] Cfr. il documento del Garante *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, cit.

[106] Si vedano i seguenti provvedimenti del Garante: n. 468 del 23 ottobre 2014, *Dossier sanitario elettronico e privacy dei pazienti*; n. 340 del 3 luglio 2014, *Trattamento di dati sanitari tramite il dossier sanitario aziendale*; n. 3 del 10 gennaio 2013, *Dossier sanitario e trattamento dei dati personali dei pazienti*; n. 610 del 18 dicembre 2014, *Illiceità nel trattamento di dati personali e sensibili presso una struttura ospedaliera*.

[107] *Linee guida in materia di dossier sanitario*, cit., p. 4.

strizione senza precedenti dei diritti e delle libertà individuali. All'imposizione di tali misure – utilizzo di dispositivi di protezione, distanziamento sociale e isolamento domiciliare – si è affiancata una notevole accelerazione dei processi di digitalizzazione, unica alternativa al prolungato periodo di chiusura di servizi e attività economiche ritenuti "non essenziali" disposto durante il c.d. *lockdown* della scorsa primavera.

Dall'inizio della pandemia ad oggi, sono stati riportati numerosi esempi di utilizzo di nuove tecnologie finalizzate al contenimento del contagio e, in particolare al controllo dell'osservanza delle disposizioni adottate in sede di decretazione d'emergenza al fine di proteggere la popolazione. Tra tali tecnologie vi sono: *termoscanner* all'ingresso di supermercati, farmacie, aeroporti e stazioni ferroviarie; braccialetti biometrici e droni, utilizzati da alcune forze di polizia per controllare gli individui sottoposti all'obbligo di quarantena; applicazioni per dispositivi mobili volte al "tracciamento di prossimità" – più comunemente noto come *contact tracing* –, il cui obiettivo è generare un sistema di allerta rivolto congiuntamente alle autorità sanitarie e a quegli utenti entrati "in contatto" con una persona con positività al virus. Lo sviluppo e la successiva adozione di queste applicazioni ha sollevato un grande dibattito tanto a livello nazionale quanto nel più ampio contesto europeo, data la molteplicità di questioni di carattere etico e giuridico sollevate dal loro utilizzo[108]. Fra queste, un ruolo preponderante è stato assunto dalla tutela della privacy individuale, il cui livello di vulnerabilità dipende in concreto dalle configurazioni tecniche previste per il funzionamento di tali applicazioni, oltreché dal più ampio contesto normativo all'interno del quale le stesse sono destinate ad operare[109].

Come già evidenziato in precedenza, fermo restando il rispetto dei principi generali applicabili al trattamento dei dati personali, il RGPD ne consente la raccolta e il trattamento da parte delle autorità pubbliche anche a prescindere dal consenso dell'interessato, in particolare allorché ciò sia necessario per fare fronte a «gravi minacce per la salute a carattere transfrontaliero»[110] quale, per esempio, quella attualmente rappresentata dalla diffusione del CoViD-19. Per quanto concerne il contesto europeo, la sperimentazione e l'adozione di queste applicazioni sono state seguite con attenzione dall'EDPB, il quale è intervenuto con una serie di documenti che si prefiggevano di guidarne lo sviluppo in piena conformità alle previsioni del RGPD e a quelle contenute nei principi fondamentali dei trattati d'integrazione europea, fra cui, in particolare, la Carta Europea dei diritti fondamentali. In questo contesto, l'EDPB ha rimarcato che

> «La messa a punto delle app deve avvenire secondo criteri di responsabilizzazione, documentando attraverso una valutazione di impatto sulla protezione dei dati tutti i meccanismi messi in atto alla luce dei principi di privacy *by design* e *by default*; inoltre, il codice sorgente dovrebbe essere reso pubblico così da permettere la più ampia valutazione possibile da parte della comunità scientifica»[111].

L'EDPB, inoltre, ha raccomandato che l'adozione delle applicazioni di tracciamento avvenisse su base volontaria, ritenendo quest'ultima non solo più confacente ai valori dell'architettura giuridica

[108] Per un approfondimento del dibattito si rinvia ai contributi ospitati all'interno del Simposio "Privacy e Contact Tracing" organizzato dalla rivista MediaLaws, disponibili in: https://www.dimt.it/news/simposio-medialaws-privacy-contact-tracing/ (consultato il 24/08/2020), e in particolare agli scritti di POLLICINO 2020 e PLUTINO 2020. Si vedano inoltre GADOTTI 2020 e MICOZZI 2020.

[109] Un'interessante iniziativa è quella del *Covid Tracking Project*, che riporta un elenco di tutte le app per *contact tracing* adottate nel mondo, con una valutazione relativa al livello di protezione della privacy individuale. Disponibile in: https://docs.google.com/spreadsheets/d/1ATalASO8KtZMx_zJREoOvFhonmB-sAqJ1-CjVRSCOw/edit#gid=0 (consultato il 24/08/2020).

[110] RGPD, art. 9.2, lett. i.

[111] EDPB, *Lettera della Presidente alla Commissione europea sul Progetto di linee-guida in materia di app per il contrasto della pandemia dovuta al Covid-19*, (14/04/2020), disponibile in: https://www.osservatoriosullefonti.it/emergenza-covid-19/autorita-di-regolazione/european-data-protection-board-edpb/3002-emcovid-edpb1 (consultato il 24/08/2020).

europea, ma anche per stimolare l'assunzione di "responsabilità" da parte della popolazione nel contrasto alla pandemia[112]. L'EDPB si è espressa anche in merito all'opportunità di utilizzare i dati di localizzazione dei dispositivi mobili degli utenti raccolti presso i fornitori dei servizi di telecomunicazioni, evidenziando come, in linea di principio, la Direttiva *ePrivacy*[113] consenta agli Stati membri di introdurre misure legislative di carattere eccezionale volte alla salvaguardia della sicurezza pubblica[114]. Tuttavia, come parimenti evidenziato dallo stesso EDPB

> «Tale legislazione eccezionale è possibile solo se costituisce una misura necessaria, adeguata e proporzionata all'interno di una società democratica. Tali misure devono essere conformi alla Carta dei diritti fondamentali e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Inoltre, esse sono soggette al controllo giurisdizionale della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo»[115].

In particolare, la Direttiva *ePrivacy* prevede che i dati relativi alla localizzazione dei dispositivi mobili – che devono essere distinti dai dati del "traffico" telefonico avvenuto per il loro tramite – possono essere trasmessi dai fornitori dei servizi di telecomunicazioni alle autorità (o a terzi) solo previa loro sottoposizione a procedimento di anonimizzazione o laddove la stessa trasmissione sia stata autorizzata dagli interessati[116]. In un secondo momento, tuttavia, l'EDPB sembra mutare orientamento con riferimento all'opportunità e alla necessità di utilizzare i dati di localizzazione dei dispositivi mobili. Invero, nella Lettera inviata alla Commissione europea in data 14 aprile 2020 si afferma che la localizzazione dei dispositivi mobili non è necessaria per il funzionamento delle app di *contact tracing* poiché il loro obiettivo primario

> «non è seguire gli spostamenti individuali o imporre il rispetto di specifiche prescrizioni, bensì individuare eventi (il contatto con soggetti positivi) che hanno natura probabilistica e che possono anche non verificarsi per la maggioranza degli utenti, soprattutto nella fase post-emergenziale. Raccogliere dati sugli spostamenti di una persona durante il funzionamento di un'app di tracciamento dei contatti configurerebbe una violazione del principio di minimizzazione dei dati, oltre a comportare gravi rischi in termini di sicurezza e privacy»[117].

Infine, l'EDPB ha ricordato che l'uso di app di *contact tracing* deve essere interrotta, e con essa anche l'archiviazione dei dati raccolti per il loro tramite, nel momento in cui la trasmissione del virus cessa di rappresentare un pericolo per la salute pubblica.

Per quanto riguarda il nostro paese, il 23 marzo scorso, in pieno contesto emergenziale, il Governo, in collaborazione con l'Istituto Superiore della Sanità e l'Organizzazione Mondiale della Sanità, ha adottato una "Fast Call" volta a identificare «tecnologie e strategie basate sulle tecnologie per il "monitoraggio attivo" del rischio di contagio»[118]. La Call ha condotto – pur a seguito di

[112] EDPB, *Lettera della Presidente alla Commissione europea europea sul Progetto di linee-guida in materia di app per il contrasto della pandemia dovuta al Covid-19*, (14/04/2020), cit.

[113] Cfr. art. 15 Direttiva 2002/58/CE.

[114] EDPB, *Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19* (19/03/2020), disponibile in: https://www.osservatoriosullefonti.it/emergenza-covid-19/autorita-di-regolazione/european-data-protection-board-edpb/ 2841-emcovid-edpb (consultato il 24/08/2020).

[115] EDPB, *Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19* (19/03/2020), cit.

[116] Cfr. art. 9 Direttiva 2002/58/CE.

[117] EDPB, *Lettera della Presidente alla Commissione europea sul Progetto di linee-guida in materia di app per il contrasto della pandemia dovuta al Covid-19* (14/04/2020), cit.

[118] La Call intitolata "Telemedicina e Data Analysis" era anche rivolta a identificare soluzioni e tecnologie relative ad app di telemedicina e assistenza domiciliare dei pazienti affetti da CoViD-19. Per un'analisi delle iniziative di promozione della telemedicina nel corso dell'emergenza sanitaria sia consentito rinviare a BOTRUGNO 2020a.

ritardi e polemiche[119] – all'adozione dell'applicazione di tracciamento denominata "Immuni". La sua adozione su tutto il territorio nazionale è stata preceduta da un periodo di sperimentazione che ha coinvolto quattro regioni italiane e, infine, suggellata dall'autorizzazione del Garante per la protezione dei dati personali[120], il quale ha ritenuto che il trattamento effettuato nell'ambito della stessa fosse proporzionato «essendo state previste misure volte a garantire in misura sufficiente il rispetto dei diritti e le libertà degli interessati, che attenuano i rischi che potrebbero derivare da trattamento»[121]. Lo stesso Garante, tuttavia, ha posto particolare enfasi sui doveri informativi a beneficio degli utenti dell'applicazione, doveri che avrebbero dovuto includere indicazioni relative alla non completa affidabilità delle rilevazioni effettuate per il suo tramite:

> «Sulla base della valutazione d'impatto trasmessa dal Ministero, tenuto conto della complessità del sistema di allerta e del numero dei soggetti potenzialmente coinvolti, il Garante ha comunque ritenuto di dare una serie di misure volte a rafforzare la sicurezza dei dati delle persone che scaricheranno la app. [...] In particolare, l'Autorità ha chiesto che gli utenti siano informati adeguatamente in ordine al funzionamento dell'algoritmo di calcolo utilizzato per la valutazione del rischio di esposizione al contagio. E dovranno essere portati a conoscenza del fatto che il sistema potrebbe generare notifiche di esposizione che non sempre riflettono un'effettiva condizione di rischio. Gli utenti dovranno avere inoltre la possibilità di disattivare temporaneamente l'app attraverso una funzione facilmente accessibile nella schermata principale»[122].

Ulteriori cautele sono state previste dal Garante al fine di impedire che i dati raccolti attraverso l'applicazione di tracciamento potessero essere riutilizzati per finalità non previste dalla norma che ne aveva sancito l'utilizzo, e quindi per garantire la trasparenza e la sicurezza del trattamento effettuato «a fini statistico-epidemiologici», evitando, nello specifico, «ogni forma di riassociazione a soggetti identificabili e adottando idonee misure di sicurezza e tecniche di anonimizzazione»[123]. Infine, il Garante ha raccomandato la definizione di «misure tecniche e organizzative per mitigare i rischi derivanti da falsi positivi»[124], raccomandazione che rimanda a una serie di profili critici relativi al funzionamento di questo strumento, evidenziati anche all'interno della Relazione *ad hoc* pubblicata dal Copasir in data 16 maggio 2020[125].

7. *Conclusioni. Circolazione, riutilizzo e vulnerabilità: le sfide aperte nella protezione dei dati*

Come evidenziato all'interno di questo lavoro – in particolare, *supra*, § 4 – l'emanazione del RGPD ha suggellato il legame indissolubile tra la protezione dei dati personali e la loro "libera"

[119] Polemiche e ritardi sono stati riscontrati anche in altri paesi europei, tra cui il Regno Unito, dove l'adozione dell'app di tracciamento è stata fortemente contestata proprio sotto il profilo del rispetto della privacy (si veda quanto riportato dai media britannici, https://www.theguardian.com/technology/2020/may/05/uk-racing-to-improve-contact-tracing-apps-privacy-safeguards; https://www.theguardian.com/commentisfree/2020/apr/25/contact-apps-wont-end-lockdown- but-they-might-kill-off-democracy, consultati il 24/08/2020). Simili preoccupazioni sono state espresse in Francia (https://www.lesechos.fr/tech-medias/hightech/coronavirus-les-risques-des-applis-de-tracage-pour-la-vie-privee-1197871, consultato il 24/08/2020).

[120] Parere del 1° giugno 2020, disponibile in: https://www.garanteprivacy.it/home/docweb/-/docweb-display/ docweb/9356588 (consultato il 24/08/2020).

[121] Parere del 1° giugno 2020, cit.

[122] Parere del 1° giugno 2020, cit.

[123] Parere del 1° giugno 2020, cit.

[124] Parere del 1° giugno 2020, cit.

[125] Cfr. *Relazione sui profili di sicurezza del sistema di allerta Covid-19 previsto dall'articolo 6 del decreto-legge n. 28 del 30 aprile 2020*, disponibile in: http://documenti.camera.it/_dati/leg18/lavori/documentiparlamentari/IndiceETesti/034/ 002/INTERO.pdf (consultato il 24/08/2020).

circolazione nello spazio europeo. L'importanza di tale legame, peraltro, è confermata dalla Comunicazione della Commissione europea 2018/232, evocativamente intitolata *Verso uno spazio comune europeo dei dati* la quale rimanda alla creazione di «un'area digitale senza soluzione di continuità, la cui scala consenta lo sviluppo di nuovi prodotti e servizi basati sui dati»[126]. Com'è evidente dal tenore della stessa Comunicazione – «I dati sono la materia prima del mercato unico digitale»[127] –, così come dagli orientamenti espressi all'interno di ulteriori atti adottati in questo settore[128] il perseguimento di uno spazio comune europeo dei dati è legato alla volontà di sfruttare i "vantaggi socioeconomici" offerti dal loro utilizzo. Con riferimento più specifico all'ambito sanitario, ivi si legge che all'Unione europea spetta il compito di «stimolare l'innovazione nelle soluzioni sanitarie, quali telemedicina e applicazioni mobili per la salute, come indicato nella revisione intermedia del mercato unico digitale e in piena conformità alla legislazione sulla protezione dei dati»[129]. In questo contesto, la Commissione europea ha identificato tre aree strategiche da sviluppare:

> «i) accesso sicuro dei cittadini ai dati sanitari e condivisione degli stessi; ii) dati migliori per la promozione della ricerca, la prevenzione delle malattie e l'assistenza sanitaria personalizzata; iii) strumenti digitali per dare maggiori poteri e autonomia ai cittadini e per un'assistenza incentrata sulla persona»[130].

La volontà di creare uno spazio comune europeo dei dati va letta congiuntamente all'emanazione del Regolamento 2018/1807/UE sulla libera circolazione dei dati non personali nell'area dell'Unione, il quale si prefigge un obiettivo ambizioso, ovvero l'introduzione di una "quinta libertà" di circolazione, che si affianca pertanto a quelle relative a merci, servizi, capitali, e persone, che rappresentano un pilastro fondamentale nell'intero processo di integrazione europea. Per consentire il perseguimento di quest'obiettivo, il Regolamento ha imposto l'eliminazione degli obblighi di localizzazione «a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità»[131]. In questo modo, si aspira a creare un mercato unico europeo per i servizi di archiviazione (*hosting*) e gli altri servizi di trattamento dei dati, sfruttando così le enormi opportunità di crescita legate all'economia dei dati[132], che secondo una stima recente si attestano in un valore superiore ai 106 miliardi per il 2020[133]. Il Regolamento, inoltre, prevede che le autorità competenti mantengano la facoltà di «chiedere od ottenere l'accesso a dati ai fini dell'esercizio delle loro funzioni ufficiali conformemente al diritto dell'Unione o nazionale. L'accesso ai dati da parte delle autorità competenti non può essere rifiutato per il fatto che i dati sono trattati in un altro Stato membro»[134].

[126] Commissione Europea, Comunicazione 2018/232, *Verso uno spazio comune europeo dei dati*, 1.
[127] Commissione Europea, Comunicazione 2018/232, *Verso uno spazio comune europeo dei dati*, 2.
[128] *Ex multis*, cfr. Commissione europea, Comunicazione 2017/228, cit.
[129] Commissione Europea, Comunicazione 2018/232, cit., 1.
[130] Commissione Europea, Comunicazione 2018/232, 4.
[131] Cfr. art. 4.1 del Regolamento 2018/1807/UE del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.
[132] All'interno della già menzionata Comunicazione della Commissione europea 2017/228, 2, si legge che «Il valore dell'economia dei dati nell'UE è stato stimato a 257 miliardi di euro nel 2014, pari all'1,85% del PIL dell'UE, passati a 272 miliardi di euro nel 2015, ossia all'1,87% del PIL dell'UE (per un incremento annuo del 5,6%). La stessa stima prevede che, istituendo per tempo un assetto programmatico e giuridico per l'economia dei dati, il suo valore potrà raggiungere i 643 miliardi di euro nel 2020, pari al 3,17% del PIL complessivo dell'UE».
[133] Tale stima, contenuta all'interno della proposta di Regolamento sulla libera circolazione dei dati non personali (COM/2017/0495) è ricavata dalla relazione *IDC and Open Evidence, European Data Market*, nella versione finale del febbraio 2017 (SMART 2013/0063). Cfr. anche *Free Flow of Non-Personal Data Factsheet*, disponibile in: https://ec.europa.eu/digital-single-market/en/news/free-flow-non-personal-data (consultato il 24/08/2020).
[134] Commissione europea, *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, cit., art. 5.

Sebbene sulla carta la protezione dei dati personali e la libera circolazione di quelli non personali appaiano nettamente distinguibili, all'atto pratico le interferenze tra l'una e l'altra possono essere plurime. Non appare superfluo ricordare che la categoria dei dati non personali ricomprende tanto le informazioni impersonali per natura e che, in quanto tali quindi, non consentono l'identificazione dei soggetti presso le quali sono state raccolte, tanto le informazioni personali che sono state sottoposte a un procedimento di anonimizzazione o spersonalizzazione in un momento successivo a quello della loro raccolta. Considerata la loro intrinseca natura, tuttavia, il trattamento dei dati sanitari consente nella maggior parte dei casi l'identificabilità del soggetto interessato, dal che discende che la libera circolazione dei dati sanitari interessi per lo più le informazioni personali sottoposte a procedimento di anonimizzazione. A quest'ultimo proposito, tuttavia, come già ricordato *supra* (§ 4), i procedimenti di anonimizzazione restano comunque soggetti alle notevoli possibilità di *reverse engineering* offerte dalle nuove tecnologie, il che si traduce in un rischio per le informazioni personali.

Alla libera circolazione dei dati (sanitari e non) si lega indissolubilmente il loro riutilizzo, il quale è affrontato dal RGPD al considerando n. 50. Secondo quest'ultimo, il riutilizzo «dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali». In particolare, a proposito dell'ottenimento del consenso, ivi si precisa che, per esempio, il riutilizzo di dati previamente raccolti per finalità di «archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile». Per stabilire se le finalità perseguite nell'ambito del riutilizzo dei dati siano legittime in virtù di una loro compatibilità con quelle originarie, sempre al considerando n. 50, si attribuisce al titolare l'onere di verificare "ogni nesso" intercorrente tra le une e le altre, così come, più in generale, di tenere conto

> «del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto».

Nell'ambito del riutilizzo dei dati, una posizione preminente è assunta dalla ricerca biomedica, soprattutto in considerazione del fatto che la diffusione delle TIC in ambito sanitario favorisce la creazione di grandi archivi di informazioni, concepiti anche al fine di un loro riutilizzo in forma aggregata, ovvero, come dianzi accennato, previo procedimento di anonimizzazione. Come è stato adeguatamente sottolineato, questa possibilità ha rivoluzionato il paradigma della ricerca quantitativa nel settore delle scienze della salute:

> «I Big Data stanno profondamente modificando la metodologia di ricerca, e con essa la gamma di applicazioni pubbliche e private dei nuovi approfondimenti raccolti con il loro utilizzo. Le fonti di Big Data potenzialmente preziose per i ricercatori medici comprendono cartelle cliniche elettroniche e fascicoli sanitari elettronici, dati di studi clinici aggregati, dati amministrativi di assistenza sanitaria, e dati genomici e altri -omics, ma sono sempre più integrate ed integrabili con dati raccolti da applicazioni utilizzate per altre finalità e con dati ambientali sempre più ampi e granulari» (Comandé 2019, 18).

Tuttavia, si è parimenti messo in evidenza come lo strumento dell'anonimizzazione, inteso quale punto di equilibrio ideale tra la tutela della privacy e il riutilizzo delle informazioni personali, possa, *in limine*, frustrare entrambe le esigenze dal momento che, da una parte, non garantisce in assoluto dal rischio di re-identificazione, mentre dall'altra può avere per effetto quello di atte-

nuare o limitare fortemente il potenziale dei dati stessi, almeno nella misura in cui un numero cospicuo di informazioni (personali) sono oscurate o rimosse:

> «la capacità dell'anonimato di offrire reale tutela è sempre più messa in discussione specialmente di fronte alle tecnologie di *data mining*. Del resto, per essere un minimo efficace, il processo di anonimizzazione dovrebbe eliminare un numero eccessivo di dati, normalmente vitali per i nuovi approcci alla ricerca, senza al contempo eliminare i rischi di discriminazione per gruppi che sono stati evidenziati in letteratura» (COMANDÉ 2019, 189).

In questo contesto, pertanto, una sfida aperta nell'ambito della protezione dei dati, in particolar modo quelli sanitari, è rappresentata dalla stessa dicotomia "dato personale" *vs* "dato anonimo", che all'atto pratico si rivela molto meno lineare di quanto possa apparire all'interno delle disposizioni del RGPD. Sempre nell'ambito della ricerca scientifica, un'ulteriore insidia sorge in relazione all'apposizione del consenso dell'interessato per il riutilizzo dei propri dati personali. A questo proposito, il considerando n. 33 del RGPD mette opportunamente in rilievo come non sempre sia possibile identificare

> «la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista».

La possibilità di prevedere un «consenso ampio e modulare» (COMANDÉ 2019, 190) per il riutilizzo dei dati per finalità di ricerca, sebbene, *ictu oculi*, sembri contravvenire il tenore dei principi generali del Regolamento, che invece richiede un consenso esplicito per finalità parimenti esplicite, pur tuttavia può essere legittimato dallo stesso, a condizione che siano rispettati i requisiti previsti all'art. 9.2, lett. j[135].

Da diversa prospettiva, una sfida ulteriore per la protezione dei dati sanitari è quella relativa alla loro estrema vulnerabilità, connotazione che deriva direttamente dalla loro intrinseca appetibilità, soprattutto per coloro che sono in grado di processarli e trarne profitto. Come sottolineato in apertura di questo lavoro, infatti, i processi di digitalizzazione della sanità e la promozione di servizi tecnologicamente mediati espongono inevitabilmente le informazioni veicolate per il loro tramite al rischio di accessi non autorizzati e altre forme di abuso dei dati. L'allarme sulla vulnerabilità dei dati relativi alla salute è stato lanciato da voci autorevoli, tra cui il *Journal of American Medical Association*, che in un editoriale (LIU et al. 2015) ha rimarcato come, stante l'evoluzione dei processi di digitalizzazione in sanità, gli episodi di violazione della privacy individuale sono destinati ad aumentare. Questa previsione, peraltro, trova già riscontro in alcune stime che riportano incrementi costanti delle violazioni della privacy in ambito sanitario nel triennio 2015-2017[136]. Un aspetto peculiare evidenziato all'interno di queste ultime analisi è quello che concerne l'adozione di atteggiamenti ritenuti inadeguati da parte dei professionisti sanitari che hanno diritto di accesso ai dati dei pazienti. Errori e superficialità da parte di questi ultimi, invero, sembrano sempre assumere un ruolo preponderante nell'accresciuta vulnerabilità della privacy dei pazienti:

[135] Per un approfondimento sul punto si rinvia a COMANDÉ 2019. Per una prospettiva comparatistica si veda invece AMRAN 2019.

[136] Cfr. il *2018 Data Breach Investigation Report*, disponibile in: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf (consultato il 24/08/2020).

> «L'errore umano è fra i fattori principali che contribuiscono a questo rischio. Inoltre, i professionisti spesso abusano della loro posizione per accedere ai dati personali dei pazienti, sebbene in circa il 13% dei casi, tale accesso sia effettuato per divertimento o curiosità – come il caso in cui il paziente sia un personaggio pubblico»[137].

Il "fattore umano", peraltro, assume una rilevanza fondamentale con riferimento alla diffusione delle TIC, oggi utilizzate in misura crescente non solo per l'archiviazione dei dati sanitari e per l'erogazione di servizi a distanza, ma anche per l'elaborazione di diagnosi e prescrizioni terapeutiche in forma automatica o semi-automatica. Non è un caso che il funzionamento dei sistemi sanitari – e, per certi versi, la stessa conoscenza medica – si fondi in maniera sempre più consistente su processi di quantificazione numerica, una tendenza che alcuni hanno ridefinito in termini di *datafication* della salute (Wallenburg, Bal 2018; Lun 2018). Le implicazioni di questa tendenza restano in larga parte da esplorare e riguardano elementi fondamentali che vanno dall'organizzazione dei sistemi sanitari alla garanzia dei diritti fondamentali, passando per l'influenza che l'elaborazione dei *big data* sta assumendo sulla stessa epistemologia medica (Botrugno 2020b).

In questo contesto, pertanto, sembra possibile affermare che l'idea della protezione dei dati personali è messa a dura prova dall'emersione di molteplici spinte volte a raccogliere, archiviare, elaborare e riutilizzare i dati (sanitari e non), a cui si correlano numerose possibilità di sfruttamento economico, il tutto in un contesto di crescente penetrazione delle nuove tecnologie all'interno dei sistemi sanitari odierni. Basti ricordare che la stessa Unione europea ha sposato una visione all'interno della quale i dati sono considerati il volano dello sviluppo economico dei prossimi decenni, nonché un fattore chiave per poter reggere il confronto economico e geopolitico con le altre potenze globali.

Pertanto, è possibile concludere che, per effetto dei processi di digitalizzazione che interessano le società contemporanee – e i sistemi sanitari in particolare –, la privacy dell'individuo, lungi dall'essere realmente "privativa", ovvero, esclusiva della persona a cui le informazioni stesse pertengono, va sempre più connotandosi alla stregua di una serie controllata di accessi e restrizioni per finalità e secondo modalità ritenute socialmente legittime. Questa transizione è resa evidente anche dalla progressiva emersione del diritto di opposizione (il c.d. *opting out*) anche al di là della figura consacrata all'art. 21 del RGPD – la quale riconosce a determinate condizioni, il diritto dell'interessato di opporsi al trattamento di dati che lo riguardano. Nel più ristretto ambito sanitario, invero, la figura dell'*opt-out* si è consolidata quale possibilità concessa all'utente del sistema sanitario di negare il proprio consenso alla creazione di fascicoli elettronici in cui sarebbero affluiti tutti i propri dati. È in caso in particolare dei servizi sanitari nazionali di Regno Unito e Australia che, in forme diverse, hanno imposto una *deadline* ai propri utenti per l'esercizio di quest'opposizione. In questo contesto, pertanto, l'*opting-out* si sta configurando alla stregua di una forma di resistenza contro i processi di digitalizzazione in sanità, una sorta di "diritto di uscita" (Botrugno 2020b, 75 ss.) che rappresenta il rovescio della medaglia, d'ispirazione garantista, di società e sistemi sanitari ormai manifestamente votati a fagocitare il maggior numero possibile di informazioni personali.

[137] *2018 Data Breach Investigation Report*, cit., 2, traduzione dall'originale in inglese.

Riferimenti Bibliografici

AMRAM D. 2019. *L'Ulisse "accountable". Ricerca e protezione dei dati personali concernenti la salute: il tentativo di armonizzazione al livello europeo "post" GDPR e le interpretazioni offerte dai sistemi irlandese, belga, spagnolo e italiano*, in «Rivista italiana di medicina legale e del diritto in campo sanitario», 1, 2019, 209 ss.

BASSINI M. 2016. *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in «Quaderni Costituzionali», 3, 2016, 587 ss.

BOTRUGNO C. 2016. *La diffusione della telemedicina nella pratica medica ordinaria: verso un'etica ad hoc*, in «Ragion Pratica», 46, 2016, 185 ss.

BOTRUGNO C. 2018a. *Telemedicine in Daily Practice: Addressing Legal Challenges while Waiting for an EU Regulatory Framework*, in «Health Policy and Technology», 7, 2018, 131 ss.

BOTRUGNO C. 2018b. *Telemedicina e trasformazione dei sistemi sanitari. Un'indagine di bioetica*, Aracne.

BOTRUGNO C. 2020a. *Telemedicina ed emergenza sanitaria: un grande rimpianto per il nostro paese*, in «Biolaw Journal», 1 (numero speciale), 2020, 691 ss.

BOTRUGNO C. 2020b. *La nuova geografia del diritto alla salute. Innovazione tecnologica, relazioni spaziali e forme di sapere*, IF Press.

CALIFANO L. 2015. *Fascicolo sanitario elettronico (Fse) e dossier sanitario. Il contributo del Garante privacy al bilanciamento tra diritto alla salute e diritto alla protezione dei dati personali*, in «Sanità pubblica e privata», 3, 2015, 7 ss.

COLAPIETRO C. 2018. *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in «Federalismi.it», 22, 2018, 1 ss.

COMANDÉ G. 2019. *Ricerca in sanità e data protection un puzzle... risolvibile*, in «Rivista Italiana di Medicina Legale», 1, 2019, 187 ss.

CUFFARO V. 2018. *Il diritto europeo sul trattamento dei dati personali*, in «Contratto e Impresa», 3, 2018, 1098 ss.

DUCATO R. 2016. *La crisi della definizione di dato personale nell'era web 3.0*, in CORTESE F., TOMASI M. (eds.), *Le definizioni nel diritto*, Quaderni della facoltà di giurisprudenza, 164 ss.

EYSENNBACH G. 2001. *What Is e-Health?*, in «Journal of Medical Internet Research», 3, 2, 2001, 1 ss.

FINOCCHIARO G. 2015. *La giurisprudenza della corte di giustizia in materia di dati personali da Google Spain a Scherms*, in «Diritto dell'informazione e dell'informatica», 31, 4/5, 2015, 779 ss.

FINOCCHIARO G. 2017. *Introduzione al Regolamento europeo sulla protezione dei dati personali*, in «Le nuove leggi civili commentate», 1, 2017, 1 ss.

FINOCCHIARO G. 2018. *Riflessioni sul poliedrico Regolamento europeo sulla privacy*, in «Quaderni Costituzionali», 4, 2018, 895 ss.

GADOTTI A. 2020. *Privacy e contact tracing: cosa può andare storto? Ecco i rischi concreti*, in «Agenda Digitale». Disponibile in: https://www.agendadigitale.eu/sicurezza/privacy/privacy-e-contact-tracing-cosa-puo-andare-storto-unanalisi-dei-rischi-concreti/.(consultato l'11/01/2021).

GRANIERI M. 2017. *Il trattamento di categorie particolari di dati personali nel reg. Ue 2016/679*, in «Le nuove leggi civili commentate», 1, 2017, 165 ss.

LIU V., MUSEN A., CHOU T. 2015. *Data Breaches of Protected Health Information in the United States*, in «Journal of American Medical Association», 313, 14, 2015, 1471 ss.

LUCCHINI GUASTALLA E. 2018. *Il nuovo Regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in «Contratto e Impresa», 1, 2018, 106 ss.

LUN K. 2018. *The Datafication of Everything - Even Toilets*, in «Yearbook of Medical Informatics», 27, 1, 2018, 234 ss.

LUPTON D. 2013. *The Digitally Engaged Patient: Self-Monitoring and Self-Care in the Digital Era*, in «Social Theory and Health», 11, 2013, 256 ss.

MARIOTTINI C.M. 2016. *Il pacchetto di riforma della Commissione Europea in materia di protezione dei dati personali*, in «Rivista di diritto internazionale privato e processuale», 3, 2016, 905, ss.

MICOZZI P. 2020. *Le tecnologie, la protezione dei dati e l'emergenza coronavirus: rapporto tra il possibile e il legalmente consentito*, in «Biolaw Journal», 1 (numero speciale), 2020, 623 ss.

MILLIGAN C., ROBERTS C., MORT M. 2011. *Telecare and Older People: Who Cares Where?*, in «Social Science & Medicine», 72, 3, 2011, 347 ss.

MORT M., ROBERTS C., CALLÉN B. 2013. *Ageing with Telecare: Care or Coercion in Austerity?*, in «Sociology of Health and Illness», 35, 6, 2013, 799 ss.

PEDRAZZI G. 2019. *Il ruolo del responsabile della protezione dei dati (DPO) nel settore sanitario*, in «Rivista Italiana di Medicina Legale», 1, 2019, 179 ss.

PIRAINO F. 2017. *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in «Le nuove leggi civili commentate», 2, 2017, 369 ss.

PIZZETTI F. 2018. *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni*, in «Media Laws», 1, 2018, 103 ss.

PLUTINO M. 2020. *Immuni. Un'app rassicurante in punto di tutela di diritti ma a forte rischio di esternalità negative*, in «Agenda Digitale». Disponibile in: http://www.medialaws.eu/immuni-unapp-rassicurante-in-punto-di-tutela-di-diritti-ma-a-forte-rischio-di-esternalita-negative/ (consultato il 24/08/2020).

POLLICINO O. 2014. *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in «Federalismi.it», 3, 2014, 1 ss.

POLLICINO O. 2020. *Fighting Covid-19 and Protecting Privacy. A Proposal in the Light of the Roots of European Constitutional Law*, in «Media Laws», disponibile in: http://www.medialaws.eu/fighting-covid-19-and-protecting-privacy-a-proposal-in-the-light-of-the-roots-of-european-constitutional-law/ (consultato il 24/08/2020).

PURTOVA N. 2018. *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, in «Law, Innovation and Technology», 10, 1, 2018, 40 ss.

STANZIONE M.G. 2016. *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in «Europa e Diritto Privato», 4, 2016, 1249 ss.

THIENE A. 2017. *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo*, in «Le nuove leggi civili commentate», 2, 2017, 410 ss.

TOMMASI C. 2019. *La nuova disciplina europea sulla protezione dei dati personali*, in «Studium Iuris», 1, 2019, 6 ss.

WALLENBURG I., BAL R. 2018. *The Gaming Healthcare Practitioner: How Practices of Datafication and Gamification Reconfigure Care*, in «Health Informatics Journal», 25, 3, 2018, 549 ss.