RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2023
DOI: 10.32091/RIID0109
Articolo sottoposto a peer review

Tra *dataveillance* e *cybersecurity*: il *digital phenotyping* alla prova del regolamento UE 2016/679

Carlo Botrugno

Le società contemporanee si affidano in misura crescente alle opportunità create dalle tecnologie che rendono possibile la produzione, raccolta, elaborazione e riutilizzo di enormi dataset per ricavare inferenze spendibili negli ambiti più disparati. Fra questi vi è anche quello medico-sanitario, che ha visto un'accelerazione inusitata dei processi di digitalizzazione in coincidenza con l'avvento della pandemia di COVID-19. Tali processi hanno contribuito al consolidamento di quella che può essere definita come *informational medicine*, ovvero un paradigma che si basa in misura progressivamente crescente sulla raccolta e l'analisi di dati tratti dal corpo umano. In questo contesto va inquadrata l'emersione del *digital phenotyping*, ovvero la quantificazione di caratteristiche fenotipiche umane attraverso l'analisi dei dati offerti dai dispositivi digitali. Come evidenziato dalla letteratura specializzata in materia, il *digital phenotyping* può rivoluzionare il processo diagnostico-terapeutico, soprattutto nell'ambito della salute mentale, garantendo maggiore accuratezza e tempestività d'intervento. Tuttavia, l'emersione di questa innovativa dimensione rischia di sfumare i confini tra prevenzione e sorveglianza, rappresentando una minaccia concreta non solo per la sfera personale, ma anche, più in generale, sul piano della cybersecurity. All'interno di questo lavoro si descrivono in maniera più dettagliata i rischi che possono derivare dalla diffusione del *digital phenotyping* attraverso un raffronto costante tra i riscontri offerti dalla letteratura e il contesto giuridico di riferimento, tra cui, in particolare, la disciplina offerta dal Regolamento UE 2016/679.

Fenotipo digitale – Privacy – Protezione dei dati – Sorveglianza dei dati – Cybersicurezza – RGPD

Sommario: *1. Introduzione – 2. Le TIC e i dati sanitari nella* Digital Strategy *dell'Unione europea – 3. Tra protezione e circolazione: la tutela "dinamica" dei dati personali nel Regolamento Ue n. 679/2016 – 4. Le criticità derivanti dalla definizione di "dato personale" e di "dato sanitario" – 5. L'incrocio tra TIC e dati sanitari nell'emergenza pandemica – 6. Profilazione e consenso: il GDPR alla prova del* digital phenotyping *– 7. Conclusioni: il* digital phenotyping *tra* cybersecurity *e* dataveillance

1. Introduzione

Le società contemporanee si affidano in misura crescente alle opportunità create dalle tecnologie che rendono possibile la produzione, raccolta, elaborazione e riutilizzo di enormi dataset per ricavare inferenze che siano spendibili negli ambiti più disparati. Fra questi vi è anche quello medico-sanitario, che ha visto un'accelerazione inusitata dei processi di digitalizzazione in coincidenza con l'avvento della pandemia di COVID-19. Tali processi hanno contribuito al consolidamento di quella che può essere definita come *informational medicine*, ovvero un paradigma che si basa in misura sempre minore sul contatto fisico tra medico e paziente e, più in generale, sulle facoltà sensoriali di quest'ultimo, per prediligere la raccolta e l'analisi di dati

C. Botrugno è ricercatore a tempo determinato presso il Dipartimento di Scienze Giuridiche dell'Università di Firenze e coordinatore della *Research Unit on Everyday Bioethics and Ethics of Science* presso il Centro di ricerca inter-universitario *L'Altro Diritto*.

tratti dal corpo umano[1]. I dati, pertanto, non solo rappresentano la "materia grezza" di cui l'*informational medicine* si nutre, ma altresì il risultato finale dell'utilizzo su larga scala dei servizi sanitari mediati dalle tecnologie dell'informazione e della comunicazione (TIC), servizi che oggi 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[2].

Il rapporto di reciproca implicazione che intercorre tra la diffusione delle TIC e la crescente rilevanza dei dati in ambito sanitario è testimoniato dall'emersione di un fenomeno che ha preso il nome di *digital phenotyping* – talvolta conosciuto anche come *person sensing*[3] –, che può essere inteso come «*a field that enables the intelligent systems to sense and mine mental health states, support smart decisions, maximize the treatment outcomes and facilitate prevention and surveillance based on the ubiquitous "digital footprints" from multiple data sources, e.g. ubiquitous sensors, social media and healthcare systems*»[4]. Il *digital phenotyping* fa leva sulla raccolta e analisi di dati derivanti da comportamentali umani di tipo passivo o attivo da cui possano essere ricavati stati cognitivi, emotivi, sociali e altri fattori che possono assumere rilevanza nel benessere della persona. Tra i dati di tipo passivo vanno incluse tutte le "tracce" derivanti dai dati di localizzazione e del *mobility tracking*, mentre al secondo vanno ascritti tutti quei dati che scaturiscono da attività in cui l'utente partecipa in maniera attiva alla loro produzione (come per esempio i questionari online, le risposte a *queries* o *feedback* sull'esperienza di un determinato servizio, forniti attraverso qualsiasi strumento digitale). Non solo il *digital phenotyping* può avvalersi della convergenza di entrambe le tipologie di dati appena descritte, ma bisogna considerare che il suo sviluppo prende avvio dalla diffusione dei c.d. *enriched data*, ovvero una fusione tra dati ricavati da sensori portatili, social media e servizi sanitari che permettono di estrarre un flusso informativo in maniera continua e non invasiva. Il concetto di flusso può essere utile a facilitare la comprensione della dinamica processuale su cui si basa il *digital phenotyping*, il quale, come è stato rimarcato, è «*less focused on bringing surveys to subjects but instead attempts to capture, with minimal interference, different aspects of the ways in which the subjects interact with the surrounding world. As smartphone technology evolves, it will likely be possible to capture more and more details about these interactions*»[5]. In altre parole, la costruzione di "fenotipi digitali" consiste nella quantificazione continua di caratteristiche fenotipiche umane ricorrendo ai dati offerti dai dispositivi digitali, tra cui soprattutto smartphone e sensori indossabili[6]. L'integrazione di varie tecniche di intelligenza artificiale, tra cui *natural language processing* e *image processing*, consente di elaborare categorie eterogenee di dati, che possono essere suddivise in 4 categorie: dati fisici (e.g., dati tratti dal contesto, tratti comportamentali, dati acustici, espressioni facciali); dati digitali (e.g., immagini, dati tratti dal testo, *electronic health records* e *personal health records*); dati biologici (e.g., dati genetici, dati relativi all'attività cerebrale, *markers* biologici); dati dell'attività social (e.g., interazione online e offline, commenti, *like*)[7].

Fra le aree maggiormente interessate dallo sviluppo del *digital phenotyping* vi è quella della salute mentale. Non è un caso che alcuni abbiano messo in evidenza come il *digital phenotyping* possa rivoluzionare il processo diagnostico oggi praticato nell'ambito della salute mentale – che si basa in larga parte su strumenti di valutazione soggettiva come la somministrazione di questionari –, per fargli assumere i caratteri di una misurazione analitica di tipo oggettivo[8]. Più nello specifico, è stato sottolineato come il *digital phenotyping* potrebbe trovare una larga applicazione nell'ambito della diagnosi e trattamento della salute mentale dei più giovani. Ciò non si deve solo al rapporto privilegiato che questi ultimi hanno con l'uso delle nuove tecnologie, ma anche al fatto che, in molti casi, la prima comparsa di sintomi di disagio mentale avviene proprio in età adolescenziale[9]. In questo contesto, il *digital phenotyping* garantirebbe "oggettività e tempestività", diventando uno strumento fondamentale per incrementare l'efficacia del percorso diagnostico-terapeutico, nonché per assicurare un migliore benessere e una migliore qualità di vita a coloro che soffrono di problemi di salute mentale.

Sebbene non si possa dire che questa dimensione abbia già trovato larga applicazione nella pratica di routine[10], è innegabile che l'enorme quantità di dati che oggi viene raccolta attraverso l'uso di sensori portatili e indossabili (o persino ingeribili) e dispositivi mobili possa rivoluzionare completamente la stessa nozione di assistenza sanitaria per come è intesa oggi, rendendo possibili forme di tutela che possono dispiegarsi lungo un *continuum* che rischia di sfumare i confini convenzionali tra prevenzione e sorveglianza. In questo contesto, appare opportuno analizzare il fenomeno del *digital phenotyping* alla luce delle possibili ripercussioni innescate da questa pervasiva convergenza di informazioni di natura eterogenea, le quali, come appare evidente, riguardano la privacy individuale e la protezione dei dati personali, entrambe in rapporto di stretta correlazione tanto con la garanzia di ulteriori prerogative fondamentali dell'individuo, quanto con quel fascio di interessi pubblici

che attengono alla *cybersecurity*. Nel prosieguo di questo lavoro, pertanto, si descrivono in maniera più dettagliata i rischi principali che possono derivare dalla diffusione del *digital phenotyping* attraverso un raffronto costante tra i riscontri offerti dalla letteratura e il contesto giuridico di riferimento, ovvero, in primo luogo, il Regolamento dell'Unione europea 679/2016 per la protezione dei dati personali concernenti le persone fisiche (d'ora in avanti, brevemente, GDPR o Regolamento), nonché il Codice per la protezione dei dati personali che risulta dalla trasposizione del nuovo impianto di protezione nell'ordinamento giuridico italiano. Per inquadrare al meglio la materia, inoltre, si richiama brevemente la *Digital Strategy* adottata dall'Ue, che si snoda tra sostegno all'implementazione delle TIC in ambito sanitario e crescente consapevolezza del *leading role* assunto dai dati sanitari – e non solo – per la crescita economica dell'area comune (paragrafo 2). Segue un sintetico *excursus* sul nuovo impianto di protezione dei dati personali predisposto dal Regolamento (paragrafo 3), e sulle difficoltà che circondano la definizione di dato personale (paragrafo 4), nonché, più specificamente quelle relative al dato sanitario. Successivamente, si richiamano sinteticamente i tentativi di intensificare le pratiche di sorveglianza sanitaria divenute necessarie al fine di contrastare l'emergenza pandemica (paragrafo 5). Dopodiché, si analizza la legittimità del *digital phenotyping* alla luce del nuovo impianto predisposto dal Regolamento (paragrafo 6), per poi concludere soffermandosi sui rischi di questo fenomeno all'intersezione tra tutela dei diritti fondamentali e *cybersecurity*.

2. Le TIC e i dati sanitari nella *Digital Strategy* dell'Unione europea

A partire dai primi anni 2000, la Commissione europea ha avviato un percorso volto a sostenere gli Stati membri nel processo di introduzione dei servizi sanitari mediati dalle TIC all'interno dei rispettivi sistemi sanitari. La prima tappa di questo percorso può farsi coincidere con l'emanazione dell'*e-Health Action Plan* del 2004[11] che negli anni successivi confluisce nella più ampia *Policy for Ageing Well With ICTs*, sviluppata sotto l'egida del Mercato Unico Digitale, per poi approdare nella più recente e onnicomprensiva *Digital Strategy for EU*[12]. Quest'ultima comprende espressamente una "Strategia europea dei dati" che traccia 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»[13]. All'interno di quest'ultima, i dati rappresentano "la linfa vitale dello sviluppo economico". Essi costituiscono, infatti, «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»[14]. Più nello specifico, l'obiettivo perseguito dall'Unione europea in questo contesto è quello della creazione di uno spazio unico europeo di dati ovvero «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»[15].

Con riferimento più specifico all'ambito sanitario, la Commissione europea si era già espressa attraverso la Comunicazione n. 233/2018, 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". In questo contesto, infatti, la Commissione aveva evidenziato a più riprese i vantaggi derivanti dalla digitalizzazione dell'assistenza, 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»[16]. Nella prospettiva della Commissione europea, il potenziale delle TIC in ambito sanitario diviene ancora più evidente se si considera che i sistemi sanitari dei paesi industrializzati si trovano a far fronte a molteplici fattori di sfida tra cui l'invecchiamento della popolazione, l'incremento delle condizioni di comorbidità, la scarsità di personale sanitario, l'incremento delle patologie non trasmissibili e il riemergere di quelle infettive. In questo contesto, la penetrazione dei servizi sanitari digitali nella pratica di routine permetterebbe di promuovere la continuità assistenziale, migliorare le condizioni di salute e il benessere globale della popolazione, anche sul posto di lavoro, ma anche di «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»[17].

Da quanto precede, pertanto, appare evidente come i dati sanitari rappresentino il fulcro di un processo che è inteso non solo a migliorare accessibilità ed efficienza dei sistemi sanitari, ma anche ad alimentare la più ampia trasformazione digitale della società europea. Nell'analisi offerta dalla Commissione all'interno della Comunicazione n. 233/2018, tuttavia, emerge chiaramente come la frammentazione del mercato dei servizi in questo settore, unita ai problemi relativi

all'interoperabilità dei dati sanitari, abbia reso impossibile giungere all'obiettivo di un "approccio integrato" alla prevenzione delle patologie e alla predisposizione della migliore risposta possibile per la popolazione degli Stati membri dell'Ue[18]. Da tale consapevolezza prende avvio la necessità di creare uno "Spazio europeo dei dati sanitari", che ha preso le forme di una proposta di Regolamento[19] che predispone «disposizioni, norme e prassi comuni, infrastrutture e un quadro di governance per l'uso primario e secondario dei dati sanitari elettronici»[20] e che si prefigge obiettivi ambiziosi, ovvero «a) rafforza[re] i diritti delle persone fisiche in relazione alla disponibilità e al controllo dei loro dati sanitari elettronici; b) stabili[re] norme per l'immissione sul mercato, la messa a disposizione sul mercato o la messa in servizio di sistemi di cartelle cliniche elettroniche nell'Unione; c) stabili[re] norme e meccanismi a sostegno dell'uso secondario dei dati sanitari elettronici; d) istitui[re] un'infrastruttura transfrontaliera obbligatoria che rende possibile l'uso primario dei dati sanitari elettronici in tutta l'Unione; e) istitui[re] un'infrastruttura transfrontaliera obbligatoria per l'uso secondario dei dati sanitari elettronici»[21].

3. Tra protezione e circolazione: la tutela "dinamica" dei dati personali nel Regolamento Ue n. 679/2016

Il nuovo impianto di protezione dei dati concernenti le persone fisiche si apre all'art. 1 con le norme relative alla "protezione delle persone fisiche con riguardo al trattamento dei dati personali", che affiancano quelle relative alla "libera circolazione" degli stessi. L'esigenza della libera circolazione dei dati è immediatamente ribadita al paragrafo 3 dello stesso articolo, là dove si mette in rilievo come quest'ultima non possa essere «limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali». La letteratura più attenta, infatti, ha sottolineato come la disciplina offerta dalle disposizioni del GDPR tratta «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»[22]. In altre parole, sin dall'avvio, il Regolamento rende esplicita la connessione tra protezione e libera circolazione dei dati personali nello spazio dell'Ue, rivelando un netto cambio di direzione rispetto alla concezione che ispirava la normativa previgente, di carattere sostanzialmente "statico". Si trattava, in altre parole, di «una tutela eminentemente negativa, consistente nel potere di escludere le interferenze altrui»[23] che corrispondeva a un flusso di dati di tipo "unidirezionale", ovvero in gran parte alimentato dalla persona fisica e recepito dal titolare del trattamento. Oggi, quel modello è stato ampiamente superato da forme di condivisione e co-gestione dei dati e delle informazioni che appaiono «destinati fin dall'origine ad una circolazione globale»[24], il che appare ancora più evidente laddove si consideri la crescente importanza assunta dai processi di digitalizzazione per il funzionamento delle società contemporanee. Tali esigenze, pertanto, hanno condotto alla necessità di ridisegnare la tutela dei dati in senso "dinamico", predisponendo un regime di protezione che, come efficacemente sostenuto, «segue i dati nel momento della loro circolazione»[25].

Per quanto concerne la delimitazione dell'ambito territoriale del GDPR, il legislatore europeo ha fatto propri alcuni orientamenti della Corte di giustizia[26] che hanno portato a una progressiva estensione dell'applicazione della disciplina europea[27], con l'effetto finale di influenzare anche il contesto giuridico extraeuropeo, in particolare quello statunitense[28]. Il GDPR trova applicazione, infatti, per ogni attività posta in essere da «un titolare del trattamento o [da] un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione»[29]. Ad alcune condizioni, tuttavia, il Regolamento trova applicazione anche a quei trattamenti effettuati dal titolare o dal responsabile che non siano stabiliti all'interno dell'Unione[30], a condizione che i servizi collegati agli stessi siano offerti a persone fisiche che si trovano al suo interno[31]. Con riferimento all'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»[32].

Il trattamento dei dati personali deve fondarsi sui seguenti principi: liceità, correttezza e trasparenza[33]; limitazione delle finalità, affinché i dati siano raccolti per finalità delimitate, esplicite e legittime[34]; minimizzazione, in modo che siano raccolti solo i dati necessari per il raggiungimento delle finalità previste[35]; esattezza dei dati[36]; limitazione della loro conservazione per un lasso temporale non superiore a quello strettamente necessario[37]; infine, integrità e riservatezza dei dati[38]. Vale la pena specificare che, in base al dettato dell'art. 6, 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 debba darsi prevalenza agli interessi, ai diritti o alle libertà fondamentali della persona fisica a cui i dati pertengono.

Come noto, nell'ambito sanitario si scambia e si condivide una mole enorme di dati che non solo rendono possibile l'identificazione diretta dei rispettivi titolari – il che rappresenta il presupposto di base per l'applicazione del GDPR –, ma che possono inoltre rivelare informazioni che la Corte di Cassazione aveva già ricondotto alla categoria dei dati "sensibilissimi" o "supersensibili"[39], poiché considerati espressione della parte più intima dell'individuo nella sua corporeità e nelle sue convinzioni psicologiche più profonde. Il GDPR prevede una protezione rafforzata per tutti quei dati che siano idonei a rivelare informazioni come l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, ma anche i dati genetici, i dati biometrici, e i dati relativi alla salute o alla vita sessuale e all'orientamento sessuale delle persone, ora definiti "categorie particolari di dati" (art. 9)[40]. Tuttavia, per quanto il Regolamento esordisca con un divieto generale di trattare tali categorie di dati[41], fa subito seguire una serie di eccezioni dallo spettro potenzialmente molto ampio. Il trattamento di questi dati è legittimo, in primo luogo, in presenza di un consenso esplicito da parte dell'interessato[42], oppure nel caso in cui gli stessi siano stati resi pubblici dal primo[43]. A ciò vanno aggiunte una serie di situazioni in cui il trattamento di tali dati è considerato lecito a prescindere dal consenso dell'interessato, ovvero nel caso in cui ciò appaia giustificato da una delle finalità che il legislatore europeo ha ritenuto meritevoli di tutela dal punto di vista dell'"interesse pubblico"[44]. È evidente, pertanto, come dall'ampiezza di questa nozione dipenda la discrezionalità esercitabile dagli Stati membri nel modulare la scelta della base giuridica per il trattamento delle categorie di dati particolari a prescindere al consenso degli interessati[45].

4. Le criticità derivanti dalla definizione di "dato personale" e di "dato sanitario"

Il GDPR ha introdotto una definizione di "dato personale" piuttosto ampia, che ricomprende «qualsiasi informazione riguardante una persona fisica identificata o identificabile»[46]. Una persona fisica è considerata "identificabile" laddove 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»[47]. Se, da una parte, la scelta di una definizione così ampia potrebbe essere stata dettata dall'intenzione di introdurre una categoria capace di assorbire le nuove tipologie di dati che dovessero emergere in futuro, dall'altra, questa definizione potrebbe rappresentare il recepimento da parte del legislatore europeo di quegli orientamenti che prendono atto delle notevoli difficoltà – se non dell'impossibilità *tout court* – di una completa anonimizzazione dei dati personali, quindi del superamento della classica contrapposizione tra dato personale e dato anonimo[48], che avrebbe portato alla scelta di introdurre misure preventive volte all'attenuazione del rischio di violazione della privacy in quelle che possono essere considerate "zone d'ombra", ovvero di difficile distinzione tra dato personale e dato non personale. Sempre a proposito dell'ampiezza della definizione, è stato evidenziato come essa rischia di apparire eccessivamente vaga e generica[49] con l'effetto di frustrare, *in limine*, le finalità di tutela che il nuovo impianto di protezione si prefigge di perseguire. Da una prospettiva parzialmente diversa, altri autori considerano "deludente" la disciplina offerta dal GDPR, soprattutto per quanto concerne il bilanciamento tra diritti fondamentali ed esigenze di mercato, che 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»[50].

Le criticità che circondano la definizione della categoria di dato personale si affiancano a quelle relative alla sottocategoria dei "dati personali relativi alla salute", che 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»[51]. Nell'analizzare tale definizione è necessario tenere conto di quanto espresso nella parte introduttiva del Regolamento, in particolare al considerando n. 35, secondo il quale per dati personali relativi alla

salute si intendono «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 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».

Come già anticipato, i dati personali relativi alla salute sono oggetto della protezione rafforzata prevista anche per le "categorie particolari" di dati (ex. art. 9). In questo contesto, tuttavia, sorprende la scelta del legislatore europeo di non prevedere una disciplina differenziata o, perlomeno, l'introduzione di cautele aggiuntive per quanto concerne i dati sanitari raccolti nell'ambito dei servizi sanitari mediati dalle TIC. Tale scelta stride con gli sforzi profusi dalla Commissione europea negli ultimi vent'anni per dare impulso alla diffusione dei servizi digitali nei sistemi sanitari degli Stati membri[52], ma soprattutto rischia di porre l'interprete dinanzi a dubbi applicativi, soprattutto allorché si consideri la crescente penetrazione di questi servizi all'interno della pratica di routine. Per contro, il legislatore italiano ha optato per una scelta diversa e – nella "forzosa trasposizione" della fonte di rango primario – ha introdotto nella parte II del Codice per la protezione dei dati personali un Titolo V appositamente rivolto al "Trattamento di dati personali in ambito sanitario"[53]. Al suo interno, si trovano indicazioni di dettaglio rispetto ai doveri incombenti sui professionisti sanitari affinché sia garantito l'adempimento degli obblighi informativi relativi alla raccolta e al successivo trattamento dei dati personali. Più nello specifico, si prevede che le forme attraverso cui tali obblighi sono espletati siano tali da identificare eventuali rischi «per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato»[54]. Il Codice procede, inoltre, a definire alcune situazioni nell'ambito delle quali il trattamento dei dati sanitari sia intrinsecamente foriero di rischi. Tra queste vi è l'erogazione di servizi di telemedicina e teleassistenza, l'erogazione di servizi che forniscono beni o servizi attraverso una rete di comunicazione telematica, di quelli i cui dati raccolti confluiscono nel fascicolo sanitario elettronico[55], nonché 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»[56].

Per le finalità proprie di questo lavoro, preme sottolineare che le esigenze di protezione della sfera individuale in ambito sanitario assumono una portata specifica con riferimento all'utilizzo delle TIC, la cui diffusione, come già anticipato, ha visto un'accelerazione decisiva in coincidenza con l'avvento della pandemia di COVID-19, che ha portato alla luce in maniera inequivoca come la protezione dei dati – sanitari e non solo – rappresenti il risultato di un "bilanciamento complesso" tra la tutela della salute pubblica e il godimento dei diritti fondamentali dell'individuo.

5. L'incrocio tra TIC e dati sanitari nell'emergenza pandemica

È noto che la nefasta diffusione del virus Sars-CoV-2 su scala globale abbia impresso un'accelerazione inimmaginabile allo sviluppo e diffusione di tecnologie e servizi che raccolgono e processano dati personali relativi alle condizioni di salute della popolazione. Nel contesto europeo, il dibattito relativo all'uso di questi ultimi è stato in larga parte monopolizzato dallo sviluppo e adozione delle *apps* per il "tracciamento di prossimità" – più comunemente noto come *contact tracing* –, la cui diffusione ha rappresentato un grande "banco di prova" per la tenuta complessiva dell'impianto predisposto dal GDPR a pochi anni dalla sua entrata in vigore. Va detto che, in concreto, il livello di esposizione della privacy individuale nell'utilizzo di tali servizi è apparso strettamente correlato alle configurazioni tecniche adottate dai service provider, oltreché dal più ampio contesto normativo all'interno del quale le stesse erano destinate ad operare. Per quanto riguarda il quadro europeo, non vi era dubbio sul fatto che, fermo restando il rispetto dei principi generali applicabili al trattamento dei dati personali, il GDPR consentisse la raccolta e il trattamento dei dati personali relativi alla salute da parte delle autorità pubbliche, anche a prescindere dal consenso dell'interessato, allorché ciò fosse necessario, tra l'altro, per far fronte a «gravi minacce per la salute a carattere transfrontaliero»[57] qual era, in effetti, quella rappresentata dalla diffusione del COVID-19 su scala globale.

La progressiva adozione di questi servizi da parte dei Paesi dell'Unione europea è stata monitorata

con attenzione dallo *European Data Protection Board* (EDPB), che è intervenuto con una serie di documenti volti a garantire che questa forma di innovazione risultasse conforme all'impianto predisposto dal Regolamento, oltreché ai principi fondamentali del funzionamento dell'Unione e, in particolare, a quelli enunciati all'interno della Carta europea dei diritti fondamentali. Più nello specifico, l'EDPB ha avuto l'opportunità di sottolineare come lo sviluppo delle applicazioni di *contact tracing* avrebbe dovuto seguire "criteri di responsabilizzazione", da perseguire attraverso la documentazione relativa alla valutazione di impatto condotta per la protezione dei dati, nonché di «tutti i meccanismi messi in atto alla luce dei principi di privacy by design e by default»[58]. Inoltre, l'EDPB ha sottolineato come il codice sorgente avrebbe dovuto «essere reso pubblico così da permettere la più ampia valutazione possibile da parte della comunità scientifica»[59]. L'EDPB, inoltre, si è prodigato per raccomandare che l'adozione delle applicazioni di *contact tracing* avvenisse su base volontaria, ritenendo tale scelta maggiormente in linea con i valori fondamentali dell'impianto giuridico dell'Unione, oltreché stimolo all'assunzione di responsabilità da parte della popolazione[60]. Nello stesso frangente, l'EDPB si è espresso anche sull'utilizzo dei dati di localizzazione dei dispositivi mobili degli utenti raccolti dai provider dei servizi di telecomunicazioni, sottolineando come la Direttiva ePrivacy[61] consentisse l'introduzione di misure legislative di carattere eccezionale finalizzate alla salvaguardia della sicurezza pubblica[62]. Cionondimeno, lo stesso EDPB ha rimarcato che tali misure di carattere eccezionale potevano considerarsi legittime solo laddove fossero apparse necessarie, adeguate e proporzionate rispetto alle finalità perseguite e comunque in linea con il rispetto dei valori proprie della democrazia. In particolare, ricordava l'EDPB, tali misure dovevano «essere conformi alla Carta dei diritti fondamentali e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali» restando comunque soggette «al controllo giurisdizionale della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo»[63]. In seno all'EDPB, tuttavia, sembra esservi stato un mutamento d'orientamento rispetto a questa possibilità, come si evinceva dalla Lettera inviata alla Commissione europea il 14 aprile 2020, dove si sosteneva che il funzionamento delle applicazioni di *contact tracing* potesse prescindere dalla localizzazione dei dispositivi mobili degli utenti, e che il loro obiettivo primario non fosse di «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»[64].

6. Profilazione e consenso: il GDPR alla prova del *digital phenotyping*

Il *digital phenotyping* incarna appieno l'ambiguità del termine "controllo", poiché assorbe tanto una dimensione di "vigilanza sanitaria" che può svilupparsi in stretta connessione con l'esigenza della prevenzione nell'ambito della sanità pubblica, tanto quella della c.d. *dataveillance* o del "controllo sociale attraverso i dati", che rappresenta ormai un punto di riferimento ineludibile nella più ampia riflessione relativa ai processi di digitalizzazione all'interno delle società contemporanee[65]. Più in particolare, l'avvento del *digital phenotyping* sembra portare alla luce l'esistenza di un nuovo spazio "extracorporale" all'interno del quale la patologia – quindi i suoi segni – possono essere captati[66]. In questo spazio, la convenzionale struttura triadica segno-sintomo-malattia appare ridefinita a vantaggio della nozione di "rischio", ovvero di una mera "eventualità". Infatti, il *digital phenotyping* rimanda alla malattia non tanto nelle sue manifestazioni concrete e attuali, quanto in quelle future ed eventuali. L'aggiunta dell'elemento temporale contribuisce a ridefinire la spazializzazione della malattia e introduce nell'analisi la categoria delle abitudini e degli stili di vita, in quanto *trait d'union* tra situazione attuale e sviluppi futuri. In altre parole, il target principale del *digital phenotyping* non è tanto la "malattia comprovata", già accertata, quanto, piuttosto, la condizione semi- o pre-patologica. Il controllo-vigilanza rivolto alle persone che rientrano in questa categoria si dispiega dunque in uno spazio virtuale e temporalmente non delimitato, che prende di mira le abitudini e gli stili di vita e lo colloca in una dimensione diacronica specifica, che si può far coincidere con l'apparizione delle prime manifestazioni considerate espressione del sintomo patologico.

Come già anticipato nell'apertura di questa riflessione, i dati prodotti, raccolti e poi elaborati nell'ambito del *digital phenotyping* sono "solitamente" prodotti in contesti extra-sanitari, o comunque non immediatamente riconducibili all'ambiente sanitario. Inoltre, spesso questi dati consistono in "tracce" o frammenti di informazioni, tanto che la loro riconduzione alle categorie predisposte dal Regolamento 2016/679 appare tutt'altro che pacifica[67]. Da un pun-

to di vista parzialmente differente, la convergenza di dati dalla natura estremamente eterogenea pone non pochi problemi anche in termini di affidabilità. Affinché possano essere utilizzati per trarne un'inferenza, tali dati necessitano comunque di un lavoro di selezione, filtraggio e "pulitura", processi che potrebbero compromettere anche in maniera significativa la loro capacità euristica. In questo contesto, può essere utile soffermarsi brevemente su alcuni dubbi interpretativi che possono emergere *ictu oculi* nel tentativo di analizzare la legittimità del *digital phenotyping* alla luce dell'impianto normativo delineato dal GDPR.

In primo luogo, appare opportuno richiamare quelle disposizioni relative alla raccolta del consenso dell'interessato per il trattamento dei propri dati e, in particolare, l'art. 7 del Regolamento, a norma del quale, diversamente da quanto accadeva con la Direttiva previgente, il titolare del trattamento non è più obbligato a documentare per iscritto l'apposizione del consenso da parte dell'interessato. Ne consegue una notevole agevolazione nella raccolta del consenso dell'interessato, soprattutto per quanto concerne i servizi mediati dalle TIC[68], il che si ripercuote inevitabilmente anche sulla raccolta di quelle "tracce" che convergono nell'ambito dei servizi di *digital phenotyping*. Da diverso punto di vista, appare evidente che tali servizi si servano di un'attività di profilazione di dati personali e non, con l'obiettivo finale di ricavare una serie di inferenze spendibili in ambito sanitario, tanto a livello preventivo-diagnostico, quando per perseguire finalità di tipo terapeutico. Questo tipo di attività sembra poter trovare spazio all'interno del concetto di profilazione introdotto dal Regolamento, che lo intende 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»[69]. In questo contesto, inoltre, appare opportuno richiamare quella disposizione del GDPR (art. 22)[70] che prevede che nessuno possa 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». Come emerge già dalla rubrica dell'art. 22, infatti, il "trattamento automatizzato" non coincide necessariamente con la profilazione, poiché il primo può ricomprendere la seconda. La profilazione, infatti, consiste in un trattamento automatizzato rivolto a perseguire una delle finalità previste dall'art. 4, comma 4. Ciò premesso, va preso atto che l'art. 22, comma 1, introduce un "diritto di opposizione" che, almeno sul piano astratto, può rappresentare un argine alla diffusione del *digital phenotyping*, almeno nella misura in cui quest'ultimo prevede il ricorso a funzioni di *data-mining* per processare una serie di tracce digitali la cui elaborazione finale non è pensata per un suo utilizzo in forma aggregata – e.g., per restare in ambito sanitario, sul piano statistico-epidemiologico –, ma, invece, è destinata a innescare o ad alimentare un processo diagnostico e/o terapeutico rivolto al singolo individuo. Per converso, la possibilità della persona fisica di opporsi alla profilazione da *digital phenotyping* deve trovare contemperamento nella necessità di perseguire finalità riconducili alla nozione di "interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri"[71]. In questo caso, il trattamento deve essere «proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato»[72].

Un ulteriore elemento da considerare a questo proposito è offerto dall'attività del Garante, a cui, peraltro, il legislatore nazionale aveva assegnato il compito di definire misure di garanzia *ad hoc* e di sostenere l'adozione di regole deontologiche nell'ambito dei trattamenti aventi ad oggetto dati sanitari[73]. Per le finalità proprie di questo lavoro, può essere utile ricordare che il Garante si è già espresso per fornire alcuni "chiarimenti" in questa materia[74], ribadendo che al divieto generale di trattare le cc.dd. categorie particolari di dati personali *ex* art. 9 del GDPR fanno eccezione quei trattamenti effettuati per il perseguimento di motivi: (i) di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri[75]; (ii) di interesse pubblico nel settore della sanità pubblica[76]; (iii) di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari e sociali[77]. Il Garante ha quindi ricordato che ogni eventuale trattamento di dati relativo all'ambito sanitario che fuoriesca da una delle fattispecie menzionate, seppur effettuato da professionisti sanitari, richiede una diversa base giuridica «da individuarsi, eventualmente, nel consenso dell'interessato o in un altro presupposto di liceità»[78]. Fra queste ultime, il Garante include espressamente: (i) i trattamenti relativi all'utilizzo di app mediche, con eccezione di quelle riconducibili alla telemedicina, e di quelli ai cui dati possano avere accesso soggetti diversi dai professionisti (sanitari e non) sui quali incombe l'onere del segreto professionale; (ii) i trattamenti rivolti alla fidelizzazione della clientela; (iii) i trattamenti effettuati in ambito sanitario da sogget-

ti privati per finalità promozionali e/o commerciali; (iv) i trattamenti effettuati da professionisti sanitari per finalità commerciali o elettorali; (v) i trattamenti effettuati attraverso il Fascicolo sanitario elettronico (FSE) di cui al d.l. 18 ottobre 2012 n. 179, nell'ambito del quale è richiesta l'acquisizione del consenso dell'interessato[79]. Se, da una parte, l'elenco predisposto dal Garante non deve intendersi come esaustivo, ragion per cui anche la profilazione da *digital phenotyping* potrebbe essere annoverata tra i casi in cui la base giuridica della raccolta è il consenso dell'interessato, dall'altra va detto che un'interpretazione particolarmente ampia della categoria dei "motivi di interesse pubblico" potrebbe conferire legittimità al *digital phenotyping* in assenza di siffatto consenso. Per rafforzare la plausibilità di quest'ultimo cammino interpretativo, va anche considerato che nel *digital phenotyping* effettuato in ambito sanitario la finalità perseguita appare intrinsecamente riconducibile all'ambito terapeutico, il che la rende più agevolmente inquadrabile nel novero dei motivi di interesse pubblico. Per converso, l'obiezione più immediata che questa interpretazione potrebbe sollevare è relativa alla necessaria sussistenza del carattere di proporzionalità tra trattamento dei dati e finalità perseguite, il che impedirebbe che qualsivoglia persona fisica possa essere sottoposta alla profilazione da *digital phenotyping* a mero scopo "preventivo", scongiurando quindi il pericolo di una *dataveillance* generalizzata a danno della popolazione. Se questo è vero, non va sottaciuto parimenti che tale nesso di proporzionalità potrebbe invece essere considerato sussistente laddove l'attività di profilazione fosse rivolta non a una platea indistinta, ma piuttosto a determinate categorie di persone, e.g., gruppi sociali considerati "a rischio" e che, quindi, appare necessario tutelare. Come messo in luce dalla letteratura in materia[80], tuttavia, questa attività di *targeting* rischia di creare abusi e distorsioni che scaturiscono dalla traslazione, consapevole o meno, di *bias* cognitivi e discriminazioni all'interno dei codici algoritmici che presiedono alle operazioni di *data-mining*. A ciò va aggiunto che gli algoritmi sviluppati dalle società commerciali sono generalmente protetti dai diritti di proprietà intellettuale, il che contribuisce alla loro opacità, quindi alla possibilità che le inferenze scaturite dal loro utilizzo amplifichino distorsioni esistenti o ne creino di nuove[81].

7. Conclusioni: il *digital phenotyping* tra *cybersecurity* e *dataveillance*

Nelle ultime due decadi, la tutela della privacy individuale e la protezione dei dati – ora chiaramente distinte nella nuova disciplina offerta dal GDPR[82] – sono state messe a dura prova dalla diffusione su larga scala di tecnologie e servizi che non solo raccolgono e trattano un numero sempre maggiore di informazioni personali, ma lo fanno ricorrendo a modelli che risultano sempre più pervasivi nei confronti della sfera individuale. Anche nell'ambito sanitario è possibile riscontrare una connotazione "aggressiva" nel funzionamento dei servizi mediati dalle TIC, come testimoniato, peraltro, dallo stesso GDPR, laddove sottolinea che «la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati sanitari»[83]. A questo proposito, vale la pena richiamare quanto enfatizzato all'interno del Code of Ethics adottato dall'International Medical Informatics Association[84], secondo il quale, i dati sanitari «*not only reveal much that is private and that should be kept confidential but, more importantly, function as the basis of decisions that have profound welfare implications for their subjects*». Questo tipo di preoccupazione, d'altronde, si riflette nei riscontri offerti dalla letteratura più attenta in questo settore, che mette in rilievo come i processi di innovazione tecnologica legati all'espansione delle TIC – non solo in ambito sanitario –, abbiano innescato la «diffusa sensazione che i nostri dati personali siano costantemente a rischio»[85].

Come si è mostrato nel corso di questo lavoro, l'emersione del *digital phenotyping* rappresenta un importante banco di prova per la tenuta complessiva del GDPR, poiché, seppur sotto l'egida della tutela della salute, che è declinata in un'accezione proattivo-preventiva, tale fenomeno rischia di produrre zone d'ombra nella protezione dei dati personali, generando quelli che alcuni hanno definito come *shadow health records*[86]. Come si è visto, infatti, il *digital phenotyping* prende avvio dalla convergenza tra dati di natura eterogenea, che possono includere tanto dati relativi alla salute, quanto dati non personali, e persino informazioni di difficile riconducibilità al concetto di dato personale, la cui aggregazione nel fenotipo digitale può comunque rivelare importanti informazioni pertinenti all'individuo, che possono essere utilizzate per finalità completamente diverse da quelle per cui erano state raccolte. Può apparire superfluo sottolineare come tutto ciò si traduca in una notevole esposizione dell'utente di tali servizi non solo al rischio di violazione della propria sfera intima, ma anche alla compromissione di ulteriori prerogative fondamentali ricollegate alla protezione dei dati personali. Tale constatazione assume una connotazione peculiare proprio in considerazione del bacino di utenza primario dei servizi di *digital phenotyping* che, almeno per il momento, si rivolge principalmente alle persone affette da disturbi di tipo mentale. Le perso-

ne che appartengono a questa categoria, infatti, sono considerate intrinsecamente vulnerabili dal momento che sperimentano livelli di compressione della propria autonomia decisionale che possono essere significativi, il che li porta a essere più facilmente esposti a influenze indebite e condizionamenti esterni che possono avere come effetto finale quello di modificare le loro visioni, preferenze e credenze, quindi anche influenzare l'adozione – o la mancata adozione – di determinate scelte e decisioni.

La portata delle minacce alla sicurezza degli utenti di tali servizi può essere più facilmente compresa laddove si considerino i profili relativi all'integrità dei dati raccolti e processati nell'ambito dei servizi di *digital phenotyping*. In questo ambito, infatti, l'integrità dei dati può venire in rilievo non solo sul piano della tutela della sfera intima, ma anche dal punto di vista dell'incolumità della persona. La possibilità di manipolare, modificare, sabotare, distruggere o sostituire i dati raccolti e veicolati per il tramite dei servizi di *digital phenotyping* rappresenta una minaccia concreta non solo per la salute della persona, ma per la sua stessa esistenza. Si pensi al caso dei dispositivi impiantabili o indossabili, soprattutto laddove essi incorporino una funzione di tipo attivo o che, comunque, integrino una qualche azione destinata a influenzare il comportamento dell'utente come effetto dell'interazione con il dispositivo – come può essere nel caso di un servizio che personalizza la posologia di un farmaco in base alla rilevazione di determinati parametri o, più semplicemente, come avviene nel caso delle applicazioni che offrono il promemoria della terapia farmacologica –.

È evidente, pertanto, come l'emersione del *digital phenotyping* si innesti su un terreno che appare centrale rispetto a tutta l'architettura adottata dall'Unione europea in materia di *cybersecurity*, protezione, circolazione e riutilizzo dei dati personali e non personali e, non ultimo, con riguardo all'ambiziosa proposta di creazione dello spazio europeo dei dati sanitari a cui si è fatto cenno in precedenza. Non è un caso, invero, che la Direttiva UE 2022/2555, relativa a "Misure per un livello comune elevato di cybersicurezza nell'Unione" (nota anche come "NIS 2") abbia inserito il settore sanitario tra quelli "ad alta criticità", e dopo aver superato la distinzione tra fornitori di servizi digitali e operatori di servizi essenziali propri della previgente Direttiva UE 2016/1148, ritenuta ormai obsoleta in ragione della complessità delle esigenze di protezione attuali, abbia espressamente incluso tanto i soggetti fornitori di servizi sanitari quanto i provider di servizi digitali nel novero dei soggetti che devono sottostare alle più stringenti e ora maggiormente dettagliate misure in materia di gestione dei rischi di cybersicurezza e ai relativi obblighi di segnalazione previsti dall'art. 21 della stessa[87].

Per proteggere gli utenti dal rischio di intrusioni indesiderate, alcuni hanno sottolineato l'opportunità di adottare linee guida che stabiliscano quali tipologie di dati possano essere legittimamente raccolte e per quali finalità possano essere utilizzate. Più in particolare, fra le soluzioni suggerite vi è quella di «*to draw a line between data that are free of semantic content, such as physiologic measures or keystroke patterns, versus data that include semantic content, such as text or speech. However, there is growing awareness that data labeled as content-free still may be used to draw inferences that reveal personal information. This points to a need for further empirical research to help discern ethically significant distinctions that can be made between these types of data*»[88].

Come si è accennato in precedenza, il *digital phenotyping* sembra doversi collocare nel limine tra quella che può essere considerata l'erogazione di un servizio o prestazione di cura – che quindi non necessita del consenso al trattamento dei dati da parte dell'interessato – e un'attività riconducibile a una dimensione di intervento "accessoria" – che, come ricordato dal Garante, non potrebbe considerarsi fra quelle volte al perseguimento di motivi di interesse pubblico e, pertanto, richiederebbe il consenso dell'interessato perché possa essere considerata legittima. Ovviamente la collocazione del *digital phenotyping* da una parte o dall'altra di questo discrimine non può essere eseguita *a priori*, ovvero non può prescindere da quelle che sono le configurazioni concrete del servizio (i.e., natura giuridica del soggetto che lo eroga, finalità perseguite, coinvolgimento di soggetti terzi per l'esecuzione delle attività, ecc.). Per esempio, l'utilizzo di tracce digitali da parte di un'istituzione riconducibile al sistema sanitario pubblico per intercettare e prevenire un tentativo di suicidio da parte di un soggetto "a rischio" pone implicazioni molto diverse da quelle che possono scaturire da un servizio di natura commerciale che analizza quelle stesse tracce per un *targeting* volto a offrire attività di *counseling* per il benessere dell'utente. Peraltro, non è possibile escludere che le finalità pubbliche perseguibili attraverso il *digital phenotyping* possano in futuro intrecciarsi alla finalità di lucro propria delle società commerciali, come avviene oggi con l'erogazione di tutti i servizi in regime di convenzione tra settore pubblico e settore privato. Tuttavia, pur limitandoci al perseguimento di finalità di interesse pubblico, ovvero considerare appena quei servizi di *digital phenotyping* posti in essere nell'ambito di attività di prevenzione della sanità pubblica, gli interrogativi e i dubbi interpretativi innescati dallo sviluppo di questa dimensione di inter-

vento restano comunque di notevole rilievo. Date le finalità intrinseche del *digital phenotyping* e, in particolare, il suo legame privilegiato con la salute mentale, è possibile prevedere che i risultati dell'attività di *data mining* prodotti da questi servizi possano in futuro rappresentare il presupposto per l'attivazione di attività che si collocano al crocevia tra la tutela della salute e la protezione della libertà personale, quale può essere l'intervento di operatori sanitari e forze dell'ordine che effettuano un trattamento sanitario obbligatorio a "beneficio" di persone che, dall'analisi del fenotipo digitale, mostrano di poter attentare alla propria incolumità (ad esempio, ponendo in essere condotte suicidarie) o a quella di terzi. In questo contesto, i motivi di interesse pubblico, combinati con la finalità della medicina preventiva, potrebbero essere sufficienti a garantire quel carattere di "necessarietà" – oltreché di urgenza – che rappresenta, come ricordato dal Garante, il requisito imprescindibile per giustificare la raccolta dei dati a prescindere dalla raccolta del consenso dell'interessato – tanto più che, in questo contesto, tale consenso assumerebbe scarso valore dato il trattamento sanitario obbligatorio presuppone uno stato di alterazione tale da comprometterne l'autonomia e la capacità decisionale di chi lo subisce –. In questo contesto, appare evidente come la predizione automatica di "tendenze comportamentali" possa portare ad abusi e violazioni di diritti fondamentali. Paradossalmente, come sottolineato da alcuni autori proprio con riferimento all'utilizzo del fenotipo digitale per prevenire la tendenza al suicidio[89], il rischio è che esso possa indurre una stigmatizzazione a danno dei gruppi sociali vulnerabili che incrementa il disagio e la condizione di malessere vissuta dagli stessi, con l'effetto paradossale di aumentare la possibilità di atti lesivi o autolesivi.

Lo scenario appena delineato rende evidente come l'integrazione di inferenze generate in maniera automatica all'interno del processo decisionale di tipo diagnostico-terapeutico sollevi la questione della loro "genuinità", ovvero della mancata validazione delle tracce (digitali) da parte del personale medico che possiede capacità ed esperienza tali da poter decidere se le manifestazioni di un determinato paziente siano effettivamente tali da destare preoccupazione da un punto di vista clinico e giustificare l'intervento (eventualmente coatto) oppure no. Il "fattore umano", invero, assume una rilevanza fondamentale con riferimento alla diffusione delle TIC che, al di là del *digital phenotyping* che si trova ancora in una fase embrionale, sono già ampiamente utilizzate 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[90], una tendenza che alcuni hanno ridefinito in termini di *datafication* della salute[91], le cui implicazioni restano in larga parte inesplorate, sebbene coinvolgano 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 trasformazione dell'epistemologia medica[92].

Note

[1] D. Lupton, *The digitally engaged patient: self-monitoring and selfcare in the digital era*, in "Social Theory and Health", 2013, n. 11, pp. 256-270.

[2] C. Botrugno, *Information technologies in healthcare: Enhancing or dehumanising doctor-patient interaction?*, in "Health", vol. 25, 2021, n. 4, pp. 475-493; World Health Organization, *Telemedicine: opportunities and developments in Member States: report on the second global survey on eHealth*, 2010.

[3] D.C. Mohr, M. Zhang, S.M. Schueller, *Personal Sensing: Understanding Mental Health Using Ubiquitous Sensors and Machine Learning*, in "Annual Review of Clinical Psychology", vol. 13, 2017, n. 8, pp. 23-47.

[4] Y. Liang, X. Zheng, D.D. Zeng, *A survey on big data-driven digital phenotyping of mental health*, in "Information Fusion", vol. 52, 2019, pp. 290-307, in particolare p. 291.

[5] J.-P. Onnella, S.L. Rauch, *Harnessing Smartphone-Based Digital Phenotyping to Enhance Behavioral and Mental Health*, in "Neuropsychopharmacology", vol. 41, 2016, n. 7, pp. 1691-1696, in particolare p. 1693.

[6] Y. Liang, X. Zheng, D.D. Zeng, *A survey*, cit., p. 290.

[7] *Ivi*, p. 293.

[8] K. Huckvale, S. Venkatesh, H. Christensen, *Toward clinical digital phenotyping: a timely opportunity to consider purpose, quality, and safety*, in "NPJ Digital Medicine", vol. 2, 2019, pp. 1-11.

[9] *Ibidem*.

[10] *Ivi*, p. 3.

[11] Adottato attraverso la COM(2004) 356, *Sanità elettronica - Migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica*, del 30 aprile 2004, e poi rinnovato per mezzo della COM(2012) 736, *Sanità elettronica 2012-2020 - Una sanità innovativa per il 21º secolo*, del 6 dicembre 2012.

[12] Cfr. Commissione europea, *Plasmare il futuro digitale dell'Europa*.

[13] Commissione europea, COM(2020) 66, *Una strategia europea per i dati*, del 19 febbraio 2020, p. 2.

[14] *Ivi*, pp. 3-4. La promozione di questa strategia si fonda su una matrice essenzialmente economica, così come si può evincere dai richiami espressi alla necessità di competere con attori globali all'avanguardia nel settore digitale quali Cina e Stati Uniti.

[15] *Ibidem*.

[16] Commissione europea, COM(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, del 25 aprile 2018.

[17] *Ibidem*.

[18] *Ivi*, p. 2. A questo proposito, non appare superfluo ricordare che l'interoperabilità dei dati – assurto a obiettivo fondamentale nella Strategia europea dei dati –, rappresentava già un pilastro della Direttiva 2011/24/UE 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, tale cooperazione è 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. A questo proposito si consultino le Raccomandazioni adottate dalla Commissione europea nel 2019 relative a un formato europeo di scambio delle cartelle cliniche elettroniche (UE) 2019/243, del 6 febbraio 2019.

[19] Proposta di Regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari (COM(2022) 197 final), del 3 maggio 2022.

[20] *Ivi*, art. 1, co. 1.

[21] *Ivi*, art. 1, co. 2.

[22] G. Finocchiaro, *Riflessioni sul poliedrico Regolamento europeo sulla privacy*, in "Quaderni Costituzionali", 2018, n. 4, pp. 895-897, in particolare p. 896.

[23] C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in "Federalismi.it", 2018, n. 22, pp. 1-34.

[24] G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati personali*, in "Le Nuove leggi civili commentate", 2017, n. 1, pp. 1-18, in particolare p. 1.

[25] *Ibidem*.

[26] A questo proposito, si vedano, in particolare, i casi *Google Spain SL*, *Schrems* e *Digital Rights Ireland Ltd.*

[27] Cfr. M. Bassini, *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in "Quaderni Costituzionali", 2016, n. 3, pp. 587-589, in particolare p. 587.

[28] N. Martinez-Martin, T.R. Insel, P. Dagum et al., *Data mining for health: staking out the ethical territory of digital phenotyping*, in "NPJ Digital Medicine", 2018, n. 1.

[29] *Ivi*, art. 3.

[30] *Ibidem*.

[31] Come sottolineato da C. Colapietro, *I principi ispiratori*, cit., p. 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 nella giurisprudenza della Corte di giustizia.

[32] Art. 1, GDPR.

[33] *Ivi*, art. 5.1, lett. a.

[34] *Ivi*, lett. b.

[35] *Ivi*, lett. c.

[36] *Ivi*, lett. d.

[37] *Ivi*, lett. e.

[38] *Ivi*, lett. f.

[39] Si veda, *ex multis*, Cass. civ., sez. VI, sent. dell'11 gennaio 2016, n. 222; sez. I, sent. del 7 ottobre 2014, n. 21107; sez. I, sent. 1 agosto 2013, n. 18443; sent. 8 luglio 2005, n. 14390.

[40] Art. 9, GDPR.

[41] *Ibidem*.

[42] *Ibidem*.

[43] *Ivi*, art. 9.2, lett. e.

[44] Tra queste: assolvere agli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale; 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; nell'espletazione delle attività proprie di una fondazione, associazione o di altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali; accertare, esercitare o difendere un diritto in sede giudiziaria; soddisfare esigenze di carattere pubblico; perseguire finalità che rientrano nell'ambito della medicina preventiva o della medicina del lavoro; soddisfare esigenze di interesse pubblico attinenti al settore della sanità pubblica; perseguire finalità di interesse pubblico relative all'archiviazione, alla ricerca scientifica, o in ambito storico e statistico (cfr. art. 9.2, lett. e-i).

[45] A questo proposito, merita di essere menzionato il rinnovato ruolo conferito dal GDPR alle Autorità nazionali di controllo, soprattutto per quanto concerne gli spazi di "flessibilità" previsti dal Regolamento (così F. Pizzetti, *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", 2018, n. 1).

[46] Art. 4, GDPR.

[47] *Ibidem*.

[48] C. Colapietro, *I principi ispiratori*, cit., p. 15; R. Ducato, *La crisi della definizione di dato personale nell'era web 3.0*, in F. Cortese, M. Tomasi (a cura di), "Le definizioni nel diritto", Quaderni della Facoltà di Giurisprudenza, 2016, pp. 145-178, in particolare p. 164.

[49] N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, in "Law, Innovation and Technology", vol. 10, 2018, n. 1, pp. 40-81.

[50] A. Thiene, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo*, in "Le Nuove leggi civili commentate", 2017, n. 2, pp. 410-444, in particolare p. 410.

[51] Art. 4.15, GDPR.

[52] Va detto che la sopra menzionata proposta di Regolamento che istituisce uno spazio europeo per i dati sanitari supplisce parzialmente a questa lacuna, almeno per quanto concerne l'accesso e lo scambio delle cartelle cliniche elettroniche e dei dati sanitari elettronici nell'area dell'Unione.

[53] Il Titolo V comprende gli articoli 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".

[54] *Ivi*, art. 78.5.

[55] Cfr. art. 12 d. l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 221.

[56] *Ibidem*. 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».

[57] Art. 9, lett. i.

[58] 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 aprile 2020.

[59] *Ibidem*.

[60] *Ibidem*.

[61] Dir. 2002/58/CE, del 12 luglio 2002.

[62]EDPB, *Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19*, 19 marzo 2020. 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. Cfr. art. 9 Dir. 2002/58/CE.

[63]*Ibidem*.

[64]EDPB, *Lettera della Presidente alla Commissione europea*, cit.

[65]A mero titolo esemplificativo, si rinvia al lavoro di D. Lyon, K.D. Haggerty, K. Ball, *Introducing Surveillance Studies*, in "Routledge Handbook of Surveillance Studies", Routledge, 2011, pp. 1-11.

[66]*Ivi*, p. 395.

[67]N. Martinez-Martin, T.R. Insel, P. Dagum et al., *Data mining for health*, cit., p. 3.

[68]Ciò che si evince, in particolare, dal tenore dell'art. 7.2 del GDPR.

[69]*Ivi*, art. 4.4.

[70]*Ivi*, art. 22, co. 1.

[71]*Ivi*, art. 9, co. 2, lett. g, richiamato dall'art. 22, co. 4.

[72]*Ibidem*.

[73]Cfr. il d.lgs. 10 agosto 2018, n. 101, 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 GDPR, compito che il Garante ha evaso con il provvedimento del 13 dicembre 2018 (Documento n. 9068972).

[74]Cfr. Garante per la protezione dei dati personali, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario* (Documento n. 9091942).

[75]Art. 9, par. 2, lett. g., GDPR.

[76]*Ivi*, lett. i.

[77]*Ivi*, lett. h e par. 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.

[78]*Ibidem*.

[79]Cfr. art. 12, co. 5, nonché art. 79 del Codice novellato.

[80]M. Garber, *The Eric Loomis Case and Predictive Crime Assessments: When Algorithms Take the Stand*, in "The Atlantic", 2016.

[81]N. Martinez-Martin, T.R. Insel, P. Dagum et al., *Data mining for health*, cit., p. 3.

[82]Come messo in evidenza in dottrina, la "costituzionalizzazione" del diritto alla protezione dei dati personali accanto alla più classica figura del diritto alla privacy avrebbe sancito il passaggio definitivo dall'*habeas corpus*, all'*habeas data* (cfr. C. Colapietro, *I principi ispiratori*, cit., p. 14), ovvero dell'emersione di una concezione plurivoca di protezione delle informazioni personali che formano il contenuto dei dati, che si riflette nella scelta di riprendere la distinzione già operata nella Carta dei diritti fondamentali dell'Unione europea (rispettivamente, artt. 7 e 8). Secondo M. Bassini, *La svolta della privacy europea*, cit., p. 588, in particolare, 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». Altri autori hanno mantenuto una visione più critica rispetto agli effetti del GDPR, che 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» (cfr. F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in "Le Nuove leggi civili commentate", vol. 40, 2017, n. 2, pp. 369-409.

[83]Cfr. considerando n. 6 del GDPR.

[84]International Medical Informatics Association, *Code of Ethics for Health Information Professionals*, 2016, p. 1.

[85]C. Colapietro, *I principi ispiratori*, cit., p. 2. Come messo in luce da recenti casi di *privacy breach* – tra i quali spicca il caso della società di consulenza Cambridge Analytica del 2016 –, i processi di digitalizzazione che hanno ridisegnato il volto delle società contemporanee fanno in modo che sia possibile porre in essere violazioni non solo di grave entità e facilmente ripetibili nel tempo, ma che coinvolgano una vastissima platea di utenti allo stesso tempo. Non va sottaciuto, inoltre, come alcuni di questi casi hanno reso evidente il potenziale economico che si cela nell'accesso e gestione di enormi pool di dati, ma anche i rischi che l'uso indebito di queste informazioni possa comportare per la tenuta delle istituzioni democratiche, soprattutto laddove il trattamento di tali dati non si limiti alla semplice "estrazione" di un'inferenza, ma siano utilizzati per tentare di manipolare surrettiziamente il pensiero degli utenti che si interfacciano ai servizi digitali.

[86]W.N. Price II, K. Spector-Bagdady, T. Minssen et al., *Shadow Health Records Meet New Data Privacy Laws*, in "University of Colorado Law Legal Studies Research Paper", vol. 363, 2019, n. 6426, pp. 448-450.

[87]Nel dettaglio, tali misure consistono in: «a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici; b) gestione degli incidenti; c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi; d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi; e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità; f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza; g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza; h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura; i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi; j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso».

[88]N. Martinez-Martin, T.R. Insel, P. Dagum et al., *Data mining for health*, cit., p. 3.

[89]M. Marks, *Artificial Intelligence Based Suicide Prediction*, in "Yale Journal of Health Policy, Law, and Ethics", vol. 18, 2019, n. 98.

[90]G. Stanghellini, F. Leoni, *Digital Phenotyping: Ethical Issues, Opportunities, and Threats*, in "Frontiers of Psychiatry", vol. 11, 2020.

[91]I. Wallenburg, R. Bal, *The gaming healthcare practitioner: How practices of datafication and gamification re-*

configure care, in "Health Informatics Journal", vol. 25, 2018, n. 3, pp. 549-557; K.-C. Lun, *The Datafication of Everything. Even Toilets*, in "Imia Yearbook of Medical Informatics", vol. 27, 2018, n. 1, pp. 234-236.

[92] C. Botrugno, *La nuova Geografia del diritto alla salute. Innovazione tecnologica, relazioni spaziali e forme di sapere*, IF Press, 2021.

* * *

Between dataveillance and cybersecurity: digital phenotyping as seen by EU regulation 2016/679

Abstract: Contemporary societies increasingly rely on the opportunities created by technologies that make possible the production, collection, processing and reuse of huge datasets to obtain inferences that can be used in the most diverse fields. Among these there is also the medical-health sector, which has seen an unusual acceleration of the digitization processes coinciding with the advent of the COVID-19 pandemic. These processes have contributed to the consolidation of what can be defined as informational medicine, i.e., a paradigm that is increasingly based on the collection and analysis of data taken from the human body. The emergence of digital phenotyping, i.e. the quantification of human phenotypic characteristics through the analysis of the data offered by digital devices, must be framed in this context. As highlighted by the specialized literature on the subject, digital phenotyping can revolutionize the diagnostic-therapeutic process, especially in the field of mental health, ensuring greater accuracy and timeliness of intervention. However, the emergence of this innovative dimension risks blurring the boundaries between prevention and surveillance, representing a concrete threat not only for the personal sphere, but also, more generally, in terms of cybersecurity. Within this work, the risks that may derive from the diffusion of digital phenotyping are described in more detail through a constant comparison between the findings offered by the literature and the legal context of reference and, in particular, the discipline offered by the EU Regulation 2016/679.

Keywords: Digital phenotyping – Privacy – Data protection – Dataveillance – Cybersecurity – GDPR