Istituzione del Repository Sanitario Nazionale alla luce del GDPR

L'inestimabile potenziale nascosto nei dati clinico-sanitari perde la quasi totalità del proprio valore qualora, come ancora oggi accade, questi siano difficilmente accessibili in termini tecnici e amministrativi in quanto archiviati in formati eterogenei, spesso ancora analogici, in archivi sia pubblici che privati non comunicanti tra loro.

La gestione di tale mole di informazioni, definiti nel complesso Big Data, a motivo della dimensione e complessità, rappresenta in ogni ambito disciplinare una sfida prima ancora della loro analisi ed utilizzo. La disponibilità in formato digitale e standardizzato di una grande quantità di dati e l'accesso agli stessi è condizione imprescindibile per ottimizzare i processi di ricerca biomedica ed erogazione delle cure tramite sistemi di AI.

Per tali ragioni, il modello proposto all'interno del presente documento, al fine di superare la sfida della disponibilità del dato sanitario come carburante per i motori di calcolo, è quello di un Repository Sanitario Nazionale di costituzione pubblica, regolamentato nelle modalità di aggiornamento ed accesso secondo i principi di interesse reciproco tra il titolare del trattamento del dato e l'interessato sulla base del Regolamento 2016/679/UE in materia di trattamento dei dati personali, dei principi etici sanciti all'interno delle "Linee Guida della Commissione Europea per un'Intelligenza Artificiale Affidabile" pubblicate ad aprile 2019 e del "Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia" pubblicato a febbraio 2020.

Il modello proposto è quello di un Repository Sanitario Nazionale di governance e proprietà pubblica basato sul principio della solidarietà mutualistica del dato sanitario tra i cittadini, secondo il quale ogni cittadino contribuisce, proporzionalmente alle proprie possibilità, al Sistema Sanitario Nazionale, ricevendo in cambio servizi sanitari proporzionati al proprio bisogno personale di salute indipendentemente dal proprio contributo.

Tale modello sarebbe forzatamente semplicistico se non si prendessero in considerazione le dinamiche di governance del dato, di accountability e di rapporti tra pubblico e privato nella ricerca e sviluppo biomedicale.

Si rende dunque innanzitutto necessaria, nei paragrafi a seguire, un'analisi su quali norme del Regolamento 2016/679/UE possano essere applicate anche allo sviluppo delle nuove tecnologie e, in particolare, a quelle genericamente ricomprese sotto il termine di AI.

Premesse

Premessa 1: trattamento dei dati personali all'interno del Repository Sanitario Nazionale

Le categorie giuridiche tradizionali in materia di protezione dei dati personali necessitano di svariate riflessioni quando riferite all'ambito dell'analisi dei Big Data sanitari. In questo settore, infatti, si assiste ad una graduale perdita di distinzione tra informazioni personali considerate a livello normativo (art. 9 reg. UE 679/2016) "particolari", come quelle relative alla salute, ed altre che, seppur riguardanti aspetti dello stile di vita della persona, come abitudini alimentari, abitudini sportive e localizzazione geografica, possono implicare trattamenti ad alto rischio, poiché, a partire delle inferenze da questi dati, è possibile giungere a conclusioni che riguardano la sfera privata degli interessati, compresi aspetti relativi alla loro salute.
In linea con questa posizione è la sentenza della Corte Europea dell'8 aprile 2014 «Comunicazioni elettroniche - Direttiva 2006/24/CE - Servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione - Conservazione di dati generati o trattati nell'ambito della fornitura di tali servizi - Validità - Articoli 7, 8 e 11 della Carta dei diritti fondamentali dell'Unione europea» che cita: *"Questi dati, presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati"*.
Pertanto si auspica che anche i dati relativi allo stile di vita della persona registrati nel Repository Sanitario Nazionale vengano trattati come dati particolari.

Premessa 2: trattamento dei dati per finalità di assistenza o di ricerca

La Real World Evidence (RWE) sarà sempre più percorribile in una sanità digitalizzata. In questo scenario le informazioni generate dalle comuni pratiche assistenziali di trattamento, diagnosi e prevenzione possono essere utilizzate per fornire risposte riguardo la fase post commercio di un farmaco o device medico.
Pertanto si auspica che i dati provenienti dall'assistenza sanitaria vadano a confluire all'interno del Repository Sanitario Nazionale tramite consenso - in conformità all'art. 7 del Reg. UE 679/2016 - che permetta il trattamento del dato ai fini di ricerca scientifica.

Limiti delle competenze degli Stati membri in materia di protezione dei dati personali

Dal 25 maggio 2018 la normativa relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, è il Regolamento europeo 2016/679, d'ora in poi "Regolamento" ovvero "GDPR (General Data Protection Regulation)", e non sono più le sole leggi nazionali singolarmente considerate. Queste ultime, infatti, possono continuare ad avere efficacia anche dopo la data indicata solo nelle materie specificatamente indicate dal GDPR o laddove, nei casi previsti dalla normativa europea, prevedano forme di tutela più restrittive. Fuori da questo campo, ove in contrasto col GDPR, le singole leggi nazionali devono essere disapplicate e, anche nelle materie lasciate alla loro competenza, devono assicurare e rispettare i principi del Regolamento. In accordo con il Considerando 8 del Regolamento gli Stati possono adottare normative nazionali al di fuori delle materie strettamente indicate solo se esse hanno come scopo di integrare gli elementi utili a garantire maggiore coerenza e comprensibilità a livello nazionale.

Dunque poiché agli Stati membri, quando operanti nel disciplinare in materia di trattamenti di dati personali devono necessariamente tener conto dei principi e valori del GDPR, di fronte allo svilupparsi delle nuove tecnologie di AI le Autorità garanti, al fine di svolgere al meglio il proprio ruolo di vigilanza, dovrebbero implementare il proprio organico con figure adeguate come Data Scientist, tecnologi ed informatici.

Libera circolazione dei dati

Benché la creazione di un Repository Sanitario Nazionale contenente i dati strutturati di milioni di concittadini possa innescare uno sviluppo di tecnologie sanitarie basate su software AI senza precedenti, esso sarebbe ugualmente limitato se non fosse pensato come interoperabile anche da parte degli altri Stati membri. A questo proposito il Regolamento afferma che la protezione dei dati personali e la libera circolazione dei dati all'interno dell'Unione sono due aspetti tra loro strettamente connessi nello stesso sistema normativo (art. 1 par. 1,3).

GDPR e ricerca scientifica

Il GDPR applica alla ricerca scientifica un "regime speciale" che incide su specifici aspetti del trattamento dei dati personali in questo settore, vale a dire:

- la liceità del trattamento;
- la limitazione delle finalità;
- i diritti degli interessati.

Secondo quanto previsto dal Garante europeo della protezione dei dati, EDPS (European Data Protection Supervisor) nel parere del 6 gennaio 2020, il regime speciale è applicabile solo ai trattamenti di dati finalizzati alla ricerca scientifica:

- che opera sulla base di **standard metodologici ed etici settoriali pertinenti**, e
- che è condotta con l'obiettivo di far crescere la conoscenza e il benessere collettivo della società, invece che servire *principalmente* uno o più interessi privati.

Il modello proposto prevede un Repository Sanitario Nazionale di costituzione pubblica e finalizzato a consentire la disponibilità in formato digitale di una grande quantità di dati e l'accesso agli stessi come condizione imprescindibile per ottimizzare i processi di ricerca biomedica ed erogazione delle cure tramite sistemi di AI.

Da ciò discende che la finalità appena descritta è senz'altro corrispondente all'obiettivo *principale* di far crescere la conoscenza e il benessere collettivo, indipendentemente dall'eventuale coinvolgimento di soggetti (es. Aziende, Associazioni, Fondazioni) che perseguono interessi privati

qualora questi si mantengano residuali rispetto all'obiettivo principale rappresentato dall'interesse pubblico.

Pertanto lo svolgimento della ricerca scientifica tramite il Repository Sanitario Nazionale:

- se effettuato sulla base di *standard metodologici ed etici settoriali pertinenti*;
- se volto all'obiettivo *principale* di far crescere la conoscenza e il benessere collettivo,

fa rientrare il trattamento dei dati svolto tramite il Repository nel campo di applicazione del "regime speciale" previsto per la ricerca scientifica.

Liceità del trattamento dei dati nel "regime speciale" per la ricerca scientifica

Lo svolgimento della ricerca scientifica tramite il Repository Sanitario Nazionale è legittimo soltanto se fondato su una corretta base giuridica ai sensi dell'art. 6 par. 1 del GDPR per quanto riguarda il trattamento di dati comuni e dell'art. 9 par. 2 per quanto riguarda il trattamento di dati particolari.

Al riguardo, le basi giuridiche per il trattamento dei dati, svolto da un *ente di sanità pubblica*, tramite il Repository Sanitario Nazionale, possono essere le seguenti, previste in alternativa:

- **laddove il Repository Sanitario Nazionale sia disciplinato a livello legislativo** il trattamento dei dati potrà essere basato sull'**interesse pubblico** (art. 6, par. 1, lett. e) in combinato disposto con l'art. 9, par. 2, lett. g) (interesse pubblico rilevante) o in combinato disposto con l'art. 9, par. 2, lett. i (interesse pubblico nel settore della sanità pubblica). L'utilizzo di questa base giuridica **non richiede l'ottenimento del consenso** da parte degli interessati **al trattamento** dei loro dati (che si differenzia, e deve essere tenuto distinto, dal **"consenso informato"** dei partecipanti umani alla ricerca). Tuttavia, come previsto dall'EDPS nel parere del 6 gennaio 2020, tale **"consenso informato" può comunque servire come salvaguardia** nei casi in cui il consenso non sia appropriato come base giuridica al trattamento dei dati;
- **laddove il Repository Sanitario Nazionale *non* sia disciplinato a livello legislativo** il trattamento dei dati potrà essere basato sul **consenso** (art. 6, par. 1, lett. a) in combinato disposto con l'art. 9, par. 2, lett. a). Nello specifico, poiché nel caso del Repository Sanitario Nazionale non è possibile individuare pienamente la finalità del trattamento dei dati personali

a fini di ricerca scientifica al momento della raccolta dei dati, ai sensi del Considerando 33 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**.

Con il progredire della ricerca, il *consenso per le fasi successive* del progetto può essere ottenuto prima che inizi la fase successiva. Tuttavia, tale consenso deve essere comunque in linea con gli standard etici applicabili per la ricerca scientifica.

Come indicato dalle Linee guida sul consenso del Gruppo di Lavoro Articolo 29 (WP29), il titolare del trattamento può applicare, in questi casi, ulteriori garanzie. L'articolo 89, paragrafo 1, ad esempio, sottolinea la necessità di implementare garanzie per le attività di trattamento dei dati a fini scientifici, storici o statistici. Queste finalità "devono essere soggette alle opportune garanzie, in conformità al presente regolamento, per i diritti e le libertà dell'interessato." La minimizzazione dei dati, l'anonimizzazione e la sicurezza dei dati sono citati come possibili garanzie in questo senso. L'anonimizzazione è la soluzione preferibile se la finalità della ricerca può essere raggiunta senza il trattamento di dati personali.

Quando le circostanze della ricerca non consentono un consenso specifico, i titolari possono compensare una non specificazione delle finalità fornendo regolarmente informazioni sullo sviluppo della finalità mentre il progetto di ricerca prosegue, in modo tale che, nel tempo, il consenso sia il più specifico possibile. Nel fare ciò, l'interessato ha almeno una conoscenza di base dello stato dei lavori, che gli consente di valutare se esercitare o meno, ad esempio, il diritto di revocare il consenso ai sensi dell'articolo 7, paragrafo 3.

Inoltre, avere a disposizione un piano di ricerca completo a disposizione degli interessati prima che acconsentano, potrebbe aiutare a compensare la mancanza di specificazione della finalità. Questo piano di ricerca dovrebbe specificare le domande di ricerca e i metodi di lavoro previsti nel modo più chiaro possibile. Il piano di ricerca può anche contribuire al rispetto dell'art. 7, par. 1, in quanto i titolari del trattamento devono dimostrare quali informazioni erano disponibili agli interessati al momento del consenso per poter dimostrare che il consenso è valido.

Laddove il consenso viene utilizzato come base legale per il trattamento, deve esserci la possibilità per l'interessato di revocare tale consenso. Tuttavia, la revoca del consenso potrebbe compromettere alcuni tipi di ricerca scientifica che richiedono dati che possono essere ricollegati agli individui, tuttavia nel GDPR è chiaro che il consenso possa essere ritirato e

che i titolari debbano agire in tal senso, in quanto non vi è alcuna esenzione a tale requisito per la ricerca scientifica.

A parere degli Autori la base giuridica per il trattamento dei dati svolto da un ente di sanità pubblica tramite il Repository Sanitario Nazionale che più di altre si addice agli obiettivi strategici dell'implementazione dei sistemi di AI in sanità è quella che vede il Repository Sanitario Nazionale disciplinato a livello legislativo, così che il trattamento dei dati potrà essere basato sull'interesse pubblico.
Il trattamento dei dati all'interno del Repository Sanitario Nazionale, difatti, riconoscendo il ruolo irrinunciabile nell'innovazione della ricerca e sviluppo di soluzioni tecnologiche sanitarie innovative, dovrebbe rientrare nella fattispecie dei compiti di interesse pubblico, al pari delle fattispecie definite nell' art. 9, paragrafo 2, lettere, g), e i).
D'altronde il Considerando 43 indica chiaramente che è improbabile che le autorità pubbliche - in cui rientrano le istituzioni sanitarie - possano fare affidamento sul consenso per il trattamento (poiché quando il titolare è un'autorità pubblica, vi è spesso un evidente squilibrio di potere nella relazione tra il titolare del trattamento e l'interessato) e che esistano altre basi legali che, in linea di principio, sono più appropriate all'attività delle autorità pubbliche.
Tuttavia l'uso del consenso come base giuridica per il trattamento dei dati da parte delle autorità pubbliche non è totalmente escluso dal quadro giuridico del GDPR: è però necessario che il consenso rimanga una *scelta libera*, e ciò si verifica solo quando agli interessati è consentito negare il proprio consenso senza subire alcun danno, ad esempio continuando a ricevere la medesima assistenza sanitaria.

Di seguito vengono analizzati i diritti dell'interessato alla luce della costituzione del Repository Sanitario Nazionale laddove il trattamento dei dati tramite il Repository Sanitario Nazionale sia basato sul consenso o sull'interesse pubblico.

Diritto al controllo dei dati

Nella realizzazione di una infrastruttura sociale digitale il diritto all'autodeterminazione informativa secondo cui i dati personali appar-

tengono all'interessato e sono soggetti alle dinamiche del diritto proprietario non pare applicabile. Difatti l'idea della proprietà del dato radicata nella dottrina europea è alla base della distanza di normativa in materia di privacy tra la cultura europea e quella americana, la quale ha dato prova di essere decisamente più abilitante verso lo sviluppo innovativo in ambito tecnologico. A questo proposito vengono in favore il parere n. 4/2015 del Garante europeo della protezione dei dati, EDPS (European Data Protection Supervisor), e il Considerando 7 del Regolamento, i quali aprono la strada ad una lettura più ampia del Regolamento che superi la visione del dato personale solamente come diritto proprietario verso la tutela del diritto alla protezione dei dati personali intesa come la garanzia che la persona mantenga il controllo sui dati che la riguardano. La prospettiva di proprietà del dato rimane comunque molto forte a tutela dei diritti specifici, come testimoniato dal consenso dell'interessato.

In merito al consenso per finalità di ricerca scientifica il Regolamento enfatizza la necessità che il consenso debba essere richiesto all'interessato sulla base di finalità specifiche e limitatamente a tali finalità. A questo proposito è di riferimento il Considerando 33 il quale, per via della difficoltà di definire pienamente le finalità della ricerca scientifica al momento della raccolta dei dati, stabilisce che "*In molti casi non è possibile individuare pienamente 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 […]*".

Il Repository Sanitario Nazionale può esprimere il suo massimo potenziale solo se interrogabile in occasioni distinte nel tempo per scopi di ricerca anche afferenti a settori differenti. In questo contesto si auspica un allargamento dei margini di azione nell'interpretazione del Regolamento affinché sia permissivo in questo ambito. Nella logica del diritto alla trasparenza (analizzato con dettaglio nel paragrafo successivo) si ritengono utili gli art. 13 par. 3 e art. 14 par. 4 che sanciscono l'obbligo del titolare, che intenda trattare i dati anche per finalità diverse da quella per cui sono stati raccolti, di fornire all'interessato informazioni in merito alle nuove finalità e ogni ulteriore informazione sulle modalità per esercitare i suoi diritti.
A questo proposito viene in ausilio il paragrafo 4 dell'art. 6 il quale cita

"laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o *degli Stati membri* che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: […]". Seguono quindi una serie di parametri molto ampi e che possono essere interpretati secondo modalità diverse.
Al fine di rendere abilitante il trattamento dei dati contenuti all'interno del Repository Sanitario Nazionale da parte del titolare e di sgravare ad esso responsabilità disincentivanti, pur riconoscendo la necessità di informare l'interessato, si richiamano sia l'art. 9 lettera j) che l'art. 89, che consentono il trattamento dei dati per finalità diverse da quella per la quale i dati personali sono stati raccolti anche senza il consenso dell'interessato nel caso della ricerca scientifica, a condizione che il trattamento sia effettuato da un professionista soggetto al segreto professionale.
Questa lettura del Regolamento appare di estrema importanza sia per l'elaborazione realisticamente percorribile dei dati contenuti all'interno del Repository Sanitario Nazionale sia per l'elaborazione dei dati ulteriori prodotti dagli algoritmi stessi.

Il Repository Sanitario Nazionale viene quindi a configurarsi come lo strumento cardine dello sviluppo delle tecnologie sanitarie basate su sistemi di AI contenendo al suo interno i Big Data sanitari, ordinatamente etichettati e di pronta interrogabilità, al quale differenti attori pubblici e privati possono accedere secondo modalità rigidamente regolamentate come di seguito descritte.

Diritto alla portabilità dei dati

L'art. 20 del Regolamento in materia di portabilità del dato dispone per il diritto dell'interessato di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano e di chiedere, se tecnicamente fattibile, la trasmissione diretta dei dati personali da un titolare all'altro senza impedimenti, a condizione

che il trattamento si basi sul contratto o consenso.

- **Laddove il trattamento dei dati tramite il Repository Sanitario Nazionale sia basato sul consenso**, il diritto alla portabilità dei dati si applica. Dunque nei confronti dei propri dati inseriti all'interno del Repository Sanitario Nazionale l'interessato mantiene il controllo proprietario del dato (il controllo sui propri dati è comunque garantito all'interessato dall'esercizio di tutti gli altri diritti normati negli artt. 15-22 del GDPR) e non solamente il diritto di accesso, finalizzato a conoscere se il titolare tratti o meno dati che lo riguardano e a quali finalità, anche al fine di esercitare il diritto di rettifica o di cancellazione.
- **Laddove il trattamento dei dati tramite il Repository Sanitario Nazionale sia basato sull'interesse pubblico**, il diritto alla portabilità non può essere esercitato dall'interessato per mancanza delle condizioni previste dall'art. 20 (consenso o contratto come base giuridica).

Principio di trasparenza

Nel quadro della libera circolazione del dato è rilevante l'art. 12 ed il principio di trasparenza in esso contenuto che prevede in capo al titolare del trattamento l'obbligo di adottare tutte le misure appropriate per fornire all'interessato non solo l'informativa come richiesto dagli art. 13 e 14, ma anche le comunicazioni necessarie a conoscere contenuto e modalità di esercizio previsti dagli articoli da 15 a 22 del Regolamento, quali il diritto di accesso, di rettifica, di cancellazione (oblio), diritto alla limitazione dei trattamenti, obbligo di notifica in caso di rettifica o cancellazione dei dati personali o imitazione del trattamento, diritto alla portabilità dei dati, diritto di opposizione, diritto a conoscere la logica nei processi decisionali automatizzati.

Come richiamato dalle Carte Etiche si ritiene che il principio di trasparenza possa riguardare non solo l'informazione complessiva sulle modalità dei trattamenti, ma anche sui rischi ad essi connessi come richiamato dall'art. 24, che pone, tra i doveri del titolare, quello di garantire e dimostrare di aver messo in atto le misure tecniche ed organizzative alla luce dei rischi connessi al trattamento.
In uno scenario nel quale le macchine valutano dati e traggono da essi informazioni utili ad orientare le azioni delle macchine stesse è fon-

damentale che il principio di trasparenza possa essere esercitato attraverso informative facilmente intellegibili. A questo proposito appaiono decisamente appropriati i paragrafi 7 e 8 dell'art. 12, i quali aprono all'utilizzo di *icone standardizzate* per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto.

Diritto di accesso

L'art. 15 del Regolamento sancisce il diritto azionabile dell'interessato, applicabile all'auspicato Repository Sanitario Nazionale, di conoscere i trattamenti relativi, le finalità, categorie di dati trattati, se sono stati o sono destinati ad essere comunicati a terzi, conoscere la "logica" dei trattamenti, le conseguenze nei confronti dell'interessato e avere una copia dei dati.

Diritto di rettifica

I dati inseriti all'interno del Repository Sanitario Nazionale dovranno seguire linee guida precise che soddisfino i requisiti tecnici della qualità del dato. Il diritto di rettifica contenuto nell'art. 16 si configura quindi come una forma di collaborazione dell'interessato col titolare per evitare danni che possano derivare all'interessato e alla collettività dall'uso di dati sbagliati o incompleti che esiterebbero nell'alterazione del funzionamento dell'algoritmo della macchina.

Diritto di cancellazione (diritto all'oblio)

Il diritto alla cancellazione dei dati è regolato dall'art. 17, che sancisce, in determinate ipotesi, il diritto dell'interessato ad ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e che comporta l'obbligo per il titolare di cancellare senza ingiustificato ritardo i dati personali.

- **Laddove il trattamento dei dati tramite il Repository Sanitario Nazionale sia basato sul consenso,** il diritto alla cancellazione è previsto. Inoltre, poiché nel Repository i dati possono essere trasferiti ad altro tito-

lare, secondo modalità ben precise di seguito affrontate, è rilevante il paragrafo 2 del suddetto articolo, secondo cui il titolare che ha ricevuto legittima richiesta di cancellazione da parte dell'interessato ha l'obbligo a farsi tramite di tale richiesta anche nei confronti di chiunque sappia essere venuto a conoscenza dei dati in questione e li stia trattando.

La norma non fa carico però al titolare di verificare se gli altri titolari abbiano adempiuto alla richiesta. Al fine di rafforzare la visione di rapporto fiduciario tra cittadino (interessato) e Istituzione titolare del Repository Sanitario Nazionale (titolare) si auspica a livello nazionale una lettura più stringente del Regolamento che comporti dunque l'obbligo da parte delle Istituzioni che governano il Repository Sanitario Nazionale di assicurarsi che le terze parti divenute titolari del trattamento abbiano adempiuto alla richiesta e di informare di conseguenza, con i dettagli relativi dell'operato, l'interessato.
L'Istituzione pubblica governante il Repository Sanitario Nazionale verrebbe quindi a porsi come "soggetto interposto" tra l'interessato e l'esercizio dei diritti da un lato e le terze parti pubbliche o private alle quali sono stati forniti i dati dall'altro.

Sempre sulla base del paragrafo 2 che nell'atto della cancellazione tiene conto della tecnologia disponibile e dei costi di attuazione, si ritiene che il diritto alla cancellazione dei propri dati dal Repository Sanitario Nazionale possa avvenire al di fuori degli algoritmi costruiti sulla base di una grande mole di dati, tra cui quelli in oggetto della richiesta di cancellazione, e che al momento di tale richiesta siano già esistenti.

Ad integrazione del paragrafo 2 dell'art. 17, l'art. 19 "obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento" riguarda tutti i destinatari ai quali il titolare li abbia trasmessi, indipendentemente dal fatto che li abbia resi pubblici e indipendentemente dal fatto che i destinatari siano o meno titolari a loro volta di specifici trattamenti.

- Laddove il trattamento dei dati tramite il Repository Sanitario Nazionale sia basato sull'interesse pubblico, l'istituzione sanitaria titolare del Repository è esentata dall'applicazione del diritto alla cancellazione, come disposto nel par. 3 lettera c) dell'art. 17, in quanto tratta dati di interesse pubblico nel settore della sanità pubblica.

Il diritto di limitazione dei trattamenti

Il diritto dell'interessato di limitare il trattamento del dato da parte del titolare è regolamentato dall'art. 18. Nell'ipotesi di un trattamento illecito l'interessato, venutone a conoscenza, può non chiedere la sospensione del trattamento. ma anche la sola limitazione. Nel caso invece nel quale il titolare non abbia più interesse a continuare il trattamento e quindi dovrebbe procedere alla cancellazione, ma l'interessato abbia interesse alla conservazione del dato per motivi di esercizio di un diritto in sede giudiziaria, egli può impedire la cancellazione del dato considerata l'ultima fase del trattamento.

Diritto di opposizione

Secondo l'art. 21 l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla *sua situazione particolare*, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Sempre sulla base della "sua situazione particolare" l'interessato può opporsi anche ai trattamenti dei suoi dati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, salvo quando il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

- **Laddove il trattamento dei dati tramite il Repository Sanitario Nazionale sia basato sul consenso**, questo diritto non trova applicazione ai sensi dell'art. 21.
- **Laddove il trattamento dei dati tramite il Repository Sanitario Nazionale sia basato sull'interesse pubblico**, poiché i dati personali sono trattati a fini di ricerca scientifica, l'interessato ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico, come avviene nel caso in oggetto.

Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

L'art. 22 sancisce il diritto dell'interessato a 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. Tale diritto non si applica, tra le altre eccezioni, in presenza del consenso dell'interessato. Inoltre l'art. 13 (2) lett. f) GDPR prevede che l'interessato debba essere informato circa "l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo […] e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato".

Anche in presenza di consenso da parte dell'interessato il titolare ha comunque il dovere di adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato e quest'ultimo gode sempre del diritto, riconosciutogli dal paragrafo 3 dello stesso articolo, di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione. Questa visione del Regolamento che affianca il potere di controllo a quello del consenso dell'interessato appare decisamente appropriata nel contesto di applicativi decisionali automatici o semi automatici in ambito sanitario. Allo stesso modo, secondo i principi etici, è necessario che l'interessato sia adeguatamente informato nel rispetto di quanto previsto dall'art. 12.
Del resto anche l'art. 15 in materia di diritto d'accesso, nella lettera h), impone al titolare di fornire, all'interessato che ne faccia richiesta, informazioni significative sulla logica utilizzata e sulle conseguenze previste dall'esito del trattamento quando si utilizzano sistemi decisionali automatizzati.

Si ritiene inoltre auspicabile che, se lo Stato dovesse decidere, come consentito dall'art. 84 del Regolamento, di prevedere sanzioni per la violazione dell'art. 22 ove si desse avvio a trattamento decisionale automatizzato in assenza di consenso da parte dell'interessato, si potrebbe considerare giustificato il ricorso a sanzione di tipo penale.

Responsabilità del Titolare del Trattamento

Il Titolare del trattamento (data controller) è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali" (art. 4. par. 1, n. 7 GDPR). In sostanza il titolare è colui che trat-

ta i dati senza ricevere istruzioni da altri, colui che decide "perché" e "come" devono essere trattati i dati. Il titolare del trattamento non è, quindi, chi gestisce i dati, ma chi decide il motivo e le modalità del trattamento. Nello scenario del Repository Sanitario Nazionale il Responsabile richiede l'utilizzo dei dati ai fini di ricerca sanitaria.

Dopo aver analizzato i diritti dell'interessato diventa ora necessaria un'analisi sulle responsabilità del Titolare del trattamento.

Questo proposito è disciplinato dall'art. 24 del Regolamento il quale chiarisce che il Titolare, sia prima di iniziare il trattamento che durante il suo svolgimento, deve sempre "mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario." Ne consegue la messa in opera di una *valutazione dei rischi* che il trattamento presenta per i diritti e le libertà delle persone fisiche. Tale valutazione non coincide necessariamente con la valutazione di impatto della protezione dei dati regolamentata dall'art. 35: essa si riferisce ad una valutazione dei rischi specifica (DPIA) da porre in opera dopo e in aggiunta a quella prevista dall'art. 24, qualora necessario.

Sulla base del paragrafo 2 del medesimo art. 24, secondo il quale il titolare deve attuare "politiche" adeguate di protezione, si pongono le basi normative per il ricorso alle Carte Etiche. Appare quindi appropriato che il titolare adoperi le *Linee Guida della Commissione Europea per un'Intelligenza Artificiale Affidabile* non solo per il trattamento dei dati come da succitato articolo 24, ma anche nella valutazione dell'impatto dell'applicazione del frutto della sua ricerca sulla sanità e, in ultimo, sul cittadino/paziente. Del resto lo stesso paragrafo 3 considera l'adesione a un Codice di condotta o a un meccanismo di Certificazione elementi utili per dimostrare il rispetto degli obblighi del titolare. Secondo le Linee Guida Europee, difatti, l'applicazione di un sistema di AI deve basarsi sui seguenti principi:

- *Azione e sorveglianza umane:* i sistemi di AI dovrebbero promuovere lo sviluppo di società eque sostenendo l'azione umana e i diritti fondamentali e non dovrebbero ridurre, limitare o sviare l'autonomia dell'uomo.
- *Robustezza e sicurezza:* per un'IA di cui ci si possa fidare è indispensabile che gli algoritmi siano sicuri, affidabili e sufficientemente robusti da far fronte a errori o incongruenze durante tutte le fasi del ciclo di vita dei sistemi di AI.

- *Riservatezza e governance dei dati:* i cittadini dovrebbero avere il pieno controllo dei propri dati personali e nel contempo i dati che li riguardano non dovranno essere utilizzati per danneggiarli o discriminarli.
- *Trasparenza:* dovrebbe essere garantita la tracciabilità dei sistemi di AI.
- *Diversità, non discriminazione ed equità:* i sistemi di AI dovrebbero tenere in considerazione l'intera gamma delle capacità, delle competenze e dei bisogni umani ed essere accessibili.
- *Benessere sociale e ambientale:* i sistemi di AI dovrebbero essere utilizzati per promuovere i cambiamenti sociali positivi e accrescere la sostenibilità e la responsabilità ecologica.
- *Responsabilità intesa anche come accountability:* dovrebbero essere previsti meccanismi che garantiscano la responsabilità e l'accountability dei sistemi di AI e dei loro risultati.

A questo proposito si auspica che le ricerche e progettualità legate all'analisi del dato sanitario contenuto all'interno del Repository Sanitario Nazionale siano sottoposte e gestite da un unico Comitato Etico di riferimento, che abbia la formazione e il commitment dedicato al supporto decisionale in materia di tecnologie sanitarie basate su AI.
Questa necessità si riscontra ad esempio nel caso delle larghe basi di dati di imaging radiologico, presenti nei sistemi RIS-PACS ospedalieri, vera e propria miniera informatica largamente inutilizzata, nella cui analisi tramite AI si incontra un ostacolo fondamentale nei vincoli autorizzativi, che risentono della diversa fase storica nella quale sono stati definiti. Infatti, l'archetipo dello studio farmacologico randomizzato sul quale ancora tendono a modellarsi le procedure dei Comitati Etici, non può essere un riferimento per le applicazioni di AI all'imaging, almeno per due principali ragioni:
- il disegno degli studi (prospettico versus retrospettivo)
- le dimensioni dei database (centinaia di pazienti versus migliaia, decine o centinaia di migliaia).

La possibilità di sviluppare training di sistemi di AI su grandi database dovrebbe potersi avvalere anche di disegni retrospettivi che, per le dimensioni e per numerosi altri fattori (p.es. costi e disponibilità di personale medico, impossibilità a contattare il paziente, curve di sopravvivenza a seconda delle patologie), non potranno acquisire il consenso infor-

mato dei singoli pazienti. Tali aspetti etici ripropongono in modo più marcato rispetto al passato anche la tematica dell'autorizzazione dell'adesione a studi multicentrici, nell'ambito AI resi ancora più necessari in funzione delle maggiori dimensioni dei database e della necessità di validazione esterna dei nuovi software, che dovrebbe poter superare l'ostacolo della ripetizione di tutta la procedura autorizzativa presso il Comitato Etico del centro che aderisce a uno studio già approvato dal Comitato Etico del centro coordinatore. Predisponendo una norma che preveda la comunicazione di adesione a studio già autorizzato da altro Comitato Etico con breve tempistica silenzio-assenso (sulla scia del modello olandese) si potrebbero in generale accorciare i tempi ed evitare, o quantomeno ridurre, anche la non infrequente discrepanza di pareri tra comitati etici sul territorio nazionale.

Ruolo dell'Autorità di Controllo Nazionale

L'interessato esercitando i suoi diritti, con particolare riferimento all'art. 15 (diritto di accesso), potrà sempre verificare quale sia stata la valutazione del rischio operata dal titolare e quali le misure adottate.

Pare evidente che il controllo della conformità all'art. 24 al trattamento dei dati non possa svolgersi solamente tra il singolo interessato e il titolare ma, in quanto interesse collettivo e di tutela di una auspicata società digitale, sia l'Autorità di controllo nazionale a vigilare agli adempimenti del titolare in materia di valutazione del rischio.
Allo stesso modo seguendo il meccanismo di Certificazione come elemento utile per dimostrare il rispetto degli obblighi del titolare richiamato sempre dal par. 3 dell'art. 24 si ritiene efficace la messa in opera da parte dell'Autorità di controllo nazionale di una certificazione che per la sua durata abiliti il titolare al trattamento dei dati presenti all'interno del Repository Sanitario Nazionale.

L'Autorità di controllo nazionale sulla base degli art. 57 e 58 riveste ruolo determinante che non si esaurisce con l'attività di vigilanza e controllo ma può estendersi anche ad una funzione di guida relativamente alla corretta attuazione del Regolamento. Tra i poteri concessi all'Autorità di controllo rientra anche quello di "condurre indagini sotto forma

di attività di revisione sulla protezione dei dati" (art. 58, par. 1, lettera b) a dimostranza di un ruolo proattivo nel monitoraggio costante dell'aderenza al Regolamento da parte del titolare. A questo scopo viene in ulteriore ausilio il paragrafo 2 dell'art. 58 in quale include i cosiddetti "poteri correttivi" che consentono all'Autorità di intervenire direttamente sul Titolare con ammonimenti, correzioni, ingiunzioni, sanzioni amministrative pecuniarie.

Valutazione di rischio e di impatto: ruolo del titolare

La valutazione del rischio regolamentata dall'art. 24, prevista per tutti i trattamenti che devono iniziare o in corso, richiede che il titolare sia tenuto a definire le misure adeguate da adottare sia dal punto di vista organizzativo che tecnologico. L'art. 24 prevede l'obbligo di una generica valutazione del rischio mentre l'art. 35 "Valutazione d'impatto sulla protezione dei dati" rappresenta necessariamente una fase successiva, ed eventualmente consequenziale, alla valutazione prevista dall'art. 24 e si applica qualora sia necessaria una specifica valutazione del rischio Data Protection Impact Assessment (DPIA).

La valutazione dell'impatto prevista dall'art. 35 richiede una valutazione specifica dell'impatto quando "il trattamento prevede l'uso di nuove tecnologie" e di conseguenza "considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche". Tra i casi di valutazione dell'impatto rientrano prevedibilmente "i trattamenti, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1" e quindi i dati relativi alla salute. Il concetto di "larga scala" viene riportato nel Considerando 91 secondo il quale rientrano in questa categoria "i trattamenti che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato".

Il trattamento e dei Big Data sanitari presenti all'interno del Repository Sanitario Nazionale e le relative finalità presentano moltissimi punti in comune nell'ambito dello sviluppo di soluzioni da applicare ai processi del Sistema Sanitario. A questo proposito si auspica la creazione di una *Checklist Specifica di Risk Assessment* di riferimento e validazione istituzionale

utile a recepire in un unico processo standardizzato la valutazione richiesta dagli art. 24 e 35. Il fine è rendere più veloci ed uniformi le valutazioni di rischio derivanti dal trattamento dei dati presenti nel Repository Sanitario Nazionale.
Tale checklist dovrebbe tenere conto, anche in modalità dinamica secondo revisioni frequenti, del parere degli interessati, dei loro rappresentanti, degli interessi del soggetto pubblico e privato.

Valutazione di rischio e di impatto: ruolo delle Autorità

L'Autorità ha un ruolo centrale nella valutazione dell'impatto sia a seguito delle proprie funzioni assegnate dall'art. 35 paragrafi 4, 5, 6, 7 sia per la possibilità da parte del titolare di ricorrere ad una consultazione preventiva delle Autorità circa le misure da adottare a seguito della valutazione di impatto presente nell'art.36. Tale consultazione è obbligatoria qualora la DPIA svolta faccia emergere che il rischio elevato "non possa essere ragionevolmente attenuato sulla base delle tecnologie disponibili e ai costi di attuazione" (Considerando 94). Il paragrafo 5 dell'art. 36 sancisce, qualora previsto dal diritto di uno Stato membro, l'obbligo di ottenere l'autorizzazione preventiva in relazione a trattamenti che riguardano la protezione sociale e alla sanità pubblica.

Assume quindi rilievo che la normativa nazionale, ai fini di favorire il trattamento dei dati presenti nel Repository Sanitario Nazionale, recepisca la *Checklist Specifica Di Risk Assessment* summenzionata e che essa sia esaustiva nella valutazione del rischio del trattamento di dati sanitari in modo da soddisfare l'obbligo di valutazione preventiva.