

La tutela dei dati personali in ambito di assistenza sanitaria e sociosanitaria

di Federica Comito*

26 febbraio 2021

Sommario: 1. Introduzione. – 2. Il diritto alla salute e la tutela della privacy. – 3. I riferimenti normativi connessi alla privacy in materia sanitaria. – 4. Il trattamento dei dati personali in ambito sanitario. – 5. Gli obblighi dei soggetti che effettuano trattamenti dei dati.

1. Introduzione

Il tema dell'assistenza sanitaria e sociosanitaria e quello della tutela della riservatezza dei dati personali rappresentano settori estremamente connessi.

L'assistenza sociosanitaria ha, infatti, la necessità di aggiornarsi per rispondere alla domanda di servizi della popolazione e le nuove tecnologie offrono una serie di possibilità capaci di risolvere efficacemente notevoli difficoltà legate alla gestione del cittadino-paziente con le sue eterogenee esigenze. Al contempo, però, è necessario che ci sia un sistema di regole sempre più complesso ed incisivo che sia in grado di raccogliere, elaborare e distribuire in modo efficace ed efficiente una ampia mole di informazioni.

Il settore salute, il settore tecnologico e il settore normativo viaggiano tuttavia, a velocità differenti. Da ciò, l'esigenza di una nuova regolamentazione del settore privacy attraverso uno strumento normativo idoneo a fronteggiare le esigenze di cui sopra.

Come è noto il 25 maggio 2018 è entrato in vigore il Regolamento UE 2016/679, direttamente applicabile in tutti gli Stati membri dell'UE (Nuovo Regolamento Generale Europeo sulla Protezione dei Dati Personali, detto anche GDPR), che ha investito anche il settore dei servizi di natura sociosanitaria.

Il sopra citato Regolamento ha comportato, dunque, una svolta epocale nel mondo della *privacy* in quanto ha modificato sotto molteplici aspetti i principi fondamentali del trattamento dei dati personali. Le novità introdotte sono varie. Tra queste si

* Collaboratore amministrativo professionale AGENAS.

evidenzia la responsabilità diretta dei titolari del trattamento, in merito al compito di assicurare ed essere in grado di comprovare il rispetto dei principi applicabili al trattamento dei dati personali; la definizione della nuova categoria dei dati personali *ex art. 9 GDPR* (i c.d. dati sensibili di cui al precedente Codice *Privacy*); l'istituzione, ai sensi dell'art. 37 GDPR, della figura del responsabile della protezione dei dati (RPD o DPO) che ha il compito di assicurare una gestione corretta dei dati personali negli enti; l'introduzione *ex art. 30 GDPR* del Registro delle attività del trattamento dove sono delineati i trattamenti effettuati e le procedure di sicurezza attuate; l'obbligatorietà, ai sensi dell'art. 35 GDPR, in capo a ciascun ente, di effettuare una valutazione di impatto dalla protezione dei dati (c.d. DPIA) prima di procedere al trattamento; l'introduzione, *ex art. 25 GDPR*, dei concetti di *privacy by design*, ovverosia fin dalla progettazione, e di *privacy by default*, ovverosia per impostazione predefinita. Infine, particolarmente innovativa, è l'introduzione del principio di *accountability*, ossia la responsabilizzazione di tutti i soggetti coinvolti nel processo di trattamento dei dati. La *voluntas* del legislatore è stata quella di responsabilizzare i soggetti coinvolti nel trattamento dei dati, non mediante generici obblighi, ma attraverso l'applicazione di comportamenti proattivi.

I destinatari della norma dovranno, pertanto, ripensare in maniera attiva le modalità di gestione e utilizzo dei dati personali mediante una loro maggiore responsabilizzazione e prendersi cura dell'interessato, tutelandolo quanto più possibile.

Si è passati, quindi, da una concezione meramente formale di mero adempimento ad un approccio sostanziale di tutela dei dati ¹, che ha particolarmente inciso sui dati relativi alla salute.

2. Il diritto alla salute e la tutela della *privacy*

L'art. 32 della Carta Costituzionale riconosce il diritto alla salute. È questa un'importante novità introdotta dalla Carta Costituzionale: solo con l'entrata in vigore della Costituzione, tale diritto assume, infatti, rango di diritto fondamentale della persona garantito dal nostro ordinamento ai livelli più alti della gerarchia normativa.

Ai sensi dell'art. 32 della Carta Costituzionale, «La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività, e garantisce cure gratuite agli indigenti. Nessuno può essere obbligato a un determinato trattamento sanitario se non per disposizione di legge. La legge non può in nessun caso violare i limiti imposti dal rispetto della persona umana».

La portata innovativa della disposizione deriva dal collegamento della norma alla

¹ In tal senso, v. Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali – approccio basato sul rischio e misure di *accountability* di titolari e responsabili, in <https://www.garanteprivacy.it/regolamentoeu/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili>.

posizione giuridica soggettiva e dal riconoscimento di un vero e proprio diritto soggettivo: la salute, per la prima volta, è un bene protetto quale diritto del singolo e non solo come interesse della collettività. A causa della difficoltà di tipo culturale di accettare e riconoscere un concetto di salute ampio e innovativo, nonostante la chiarezza testuale dell'articolo 32 della Carta Costituzionale, la disposizione inizia a produrre effetti normativi innovativi solo a partire dagli anni 70.²

Solo a decorrere da tale periodo, il concetto di salute si colora di contenuti, apparendo sempre più complesso: la salute si aggancia all'equilibrio psicofisico della persona e si definisce in relazione all'ambito sociale, lavorativo, scolastico, ambientale, permeando tutti gli spazi delle relazioni interpersonali.

La portata veramente innovativa dell'art. 32 si coglie dal momento in cui la Giurisprudenza costituzionale inizia a considerare il diritto alla salute, non più solamente in una dimensione verticale, ossia un diritto opponibile tra i cittadini e i pubblici poteri, ma attribuendogli una portata orizzontale, quale diritto da far valere tra tutti i consociati³.

Quanto al diritto della *privacy*, esso oltre ad intendersi quale diritto alla non intromissione nella sfera privata di ogni soggetto, è interpretato secondo un'accezione più dinamica quale diritto alla tutela dei dati personali, consentendo al soggetto il potere di controllare in maniera autonoma la diffusione dei propri dati.

Il diritto alla *privacy* trova il suo fondamento, a livello Europeo, nella Carta dei diritti fondamentali dell'UE. In particolare, ai sensi dell'art. 8, «ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica...».

Il diritto alla riservatezza, in ambito nazionale, può essere collocato nell'ambito di quei diritti di nuova generazione, non sussistenti all'epoca dell'emanazione della Costituzione.

Ne consegue che questo diritto è, spesso, stato desunto dall'interpretazione sistematica di altre norme della Carta Costituzionale, quali l'art. 13 sulla libertà personale, l'art. 14 sulla inviolabilità del domicilio e l'art. 15 sulla segretezza della corrispondenza.

Oggi, similmente ai diritti di c.d. "nuova formazione", ha trovato la sua tutela costituzionale tramite un collegamento alla fattispecie di cui all'art. 2 della Costituzione ai sensi del quale «la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede

² MORANA D, La salute come diritto costituzionale, Giappichelli, Torino, 2018, 4 s.

³ Cfr. Corte cost., Sent. n. 37 del 1991. La Corte ha riconosciuto la scomponibilità nei due aspetti – entrambi fondamentali – di "diritto dell'individuo" e di "interesse della collettività"

l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale»⁴.

3. I riferimenti normativi connessi alla *privacy* in materia sanitaria

Il diritto alla *privacy* è stato dapprima positivizzato in fonti normative Europee e successivamente nazionali.

In particolare, la Direttiva 95/46/CE relativa al trattamento dei dati personali, rappresenta la prima occasione per l'ordinamento EU di prevedere una disciplina organica sulla *privacy*, volta ad attenuare il divario di tutela presente all'interno dei singoli Stati.

A livello nazionale, il percorso di attuazione della sopra citata direttiva iniziò con la legge n. 675 del dicembre 1996, per poi proseguire con il d.lgs 30 giugno 2003, n. 196 (c.d. Codice della Privacy).

Tanto premesso, più nel dettaglio, si evidenzia che, sin dai primissimi riferimenti normativi europei in materia di tutela dei dati personali, i dati relativi alla salute sono stati oggetto di particolare tutela, essendo qualificati come idonei a rivelare lo stato di salute e conseguentemente, qualificati come dati sensibili. I c.d. dati sensibili sono da sempre stati destinatari di una disciplina speciale proprio in virtù del pericolo concreto di illecito utilizzo degli stessi.

A tal proposito, si guardi alla Convenzione n. 108/1981, adottata a Strasburgo dal Consiglio d'Europa il 28.01.1981 (c.d. Convenzione di Strasburgo) che, all'art. 6, prevede le categorie speciali di dati, tra cui quelli della salute, per i quali è escluso il trattamento in assenza di conformi garanzie offerte dall'ordinamento nazionale. Successivamente, la già citata Direttiva 95/46/CE ha espressamente previsto una serie di garanzie necessarie al fine disciplinare il trattamento di queste "particolari categorie di dati"⁵.

In coerenza con la normativa Europea, anche la disciplina nazionale ha previsto una particolare tutela per i dati sensibili e, nella specie, per i dati inerenti alla salute, originariamente con la legge n. 675 del 31 dicembre 1996 e, a seguire, con il Codice della *privacy*, d.lgs n.196 del 30 giugno 2003.

Il codice di cui sopra, in particolare, oltre a disciplinare in generale il trattamento dei dati sensibili⁶, pone particolare attenzione alla disciplina per il trattamento dei dati

⁴ Cfr. Corte Cass., sent. n 5658 del 1998 da cui si evince che il diritto alla riservatezza, quale diritto della personalità consente di individuare il correlativo fondamento giuridico ancorandolo direttamente all'art. 2 Costituzione

⁵ Cfr. Art. 8, Direttiva 95/46/CE del Parlamento Europeo del 24 ottobre 1995.

⁶ Cfr. Art. 4, comma 1 lettera d), d.lgs n.196 del 30 giugno 2003 , «i dati sensibili, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;».

personali in ambito sanitario⁷. L'aver previsto una disciplina di dettaglio per il trattamento dei dati personali in ambito sanitario, evidenzia la volontà del legislatore di regolare equamente il rapporto tra diritto alla salute e diritto alla riservatezza, mirando a garantire un corretto bilanciamento, da un lato, tra la libera circolazione delle informazioni funzionale alla tutela della salute e, dall'altro, la tutela della riservatezza.

La disciplina in materia di privacy è stata, infine, profondamente modificata in conseguenza dell'entrata in vigore del Regolamento UE 2016/679 (GDPR), immediatamente applicabile ed efficace nei singoli Stati membri, il quale ha introdotto importanti novità anche rispetto al trattamento dei dati relativi alla salute.

L'adeguamento normativo nazionale rispetto alla disciplina Europea è quindi, proseguito con l'emanazione del d.lgs del 10 agosto 2018, n.101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679», alcune delle quali hanno profondamente inciso sul Codice della privacy. Il nuovo GDPR e conseguentemente, il d.lgs del 10 agosto 2018, n.101, assicurano un'applicazione ed una conseguente protezione dei dati personali omogenea su tutto il territorio dell'Unione europea, garantendo così una migliore tutela ad un diritto fondamentale non solo per i cittadini europei, bensì per tutti gli individui che si trovano sul territorio dell'Unione⁸.

Ponendo l'attenzione sul Regolamento UE 2016/679, ai sensi dell'art. 6 del GDPR, il trattamento dei dati personali è ammesso, purché siano rispettati i principi delineati dall'art. 5 e i limiti di cui al successivo art. 6 del GDPR.

Non di meno, il Regolamento EU delinea una più restrittiva disciplina con riferimento al trattamento di categorie "particolari" di dati personali. Infatti, ex art. 9 del GDPR, è fatto divieto di trattamento dei dati personali c.d. "particolari", salva la presenza delle condizioni di cui al par. 2 del medesimo articolo. All'interno di tali dati rientrano i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Sono ricompresi nei dati relativi alla salute tutti gli aspetti che riguardano la salute fisica o mentale di una persona, compresa la prestazione dei servizi di assistenza sanitaria in quanto capaci di rivelare informazioni relative allo stato di salute. Esse comprendono informazioni sulla persona assunte sin dalla fase di accesso al servizio sanitario, o ancora, al momento della registrazione. Tali informazioni possono essere rappresentate anche da un numero o da un simbolo; in altre parole, è possibile definire dati relativi alla salute tutte quelle informazioni idonee a rivelare lo stato di salute fisica

⁷ Cfr. D.lgs n.196 del 30 giugno 2003, Titolo V, Parte II "Trattamento dei dati personali in ambito sanitario" (artt. 75 – 94).

⁸ CALIFANO L, COLAPIETRO C, Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679, Editoriale scientifica, Napoli, 2017.

o mentale di un soggetto e le prestazioni che riceve dai servizi sanitari e sociosanitari⁹.

Come sopra accennato, proprio in quanto considerati quali dati particolari, la cui illegittima divulgazione può arrecare ingenti danni alla persona, il GDPR, all'art. 9, sancisce la regola secondo cui il trattamento dei dati relativi alla salute è vietato.

Tale divieto non è assoluto, infatti il paragrafo 2 dell'art. 9 riconosce tutta una serie di condizioni di legittimità e liceità del trattamento dei dati sanitari¹⁰, riconducibili sostanzialmente a due categorie di eccezioni. Da un lato alla dimensione privatistica, poiché il trattamento dei dati è finalizzato a salvaguardare dei diritti fondamentali dello stesso interessato e di altri soggetti (es. lett. c) e dall'altra a quella pubblicistica, in quanto connesso alla tutela di interessi pubblici.

In tema di dati relativi alla salute è, inoltre, opportuno ricordare che il GDPR consente che gli Stati membri prevedano ulteriori condizioni di liceità. In particolare, l'articolo 9, comma 4, chiarisce che «Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute».

⁹ Cfr. Art. 4 e Considerando 35, GDPR.

¹⁰ Cfr. Art. 9, paragrafo 2, GDPR, «Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli 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, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per 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; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitano le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che 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; (C55, C56) h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; (C53) i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; (C54) j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

Recependo il dettato del comma 4 dell'art. 9 del Regolamento, il Legislatore italiano ha, pertanto, riconosciuto la possibilità di prevedere ulteriori condizioni per la liceità del trattamento dei dati relativi alla salute. In tal senso, con particolare attenzione ai dati sanitari, si ricorda l'art. 2 quater e l'art. 2 septies del d.lgs 101/2018.

In virtù dell'art. 2 quater¹¹, il Garante italiano promuove l'adozione di regole deontologiche (da riportare nell'allegato A del codice della Privacy), ne verifica la conformità alle norme vigenti in materia e, successivamente alla pubblica consultazione di almeno 60 giorni, le approva. Le regole deontologiche costituiscono condizioni essenziali per la liceità e la correttezza del trattamento dei dati personali.

Simili alle regole deontologiche sono le misure di garanzia disposte dal Garante mediante un provvedimento, così come previsto ex art. 2 septies del d.lgs. 101 del 2018¹².

Le misure di garanzia, attualmente non adottate dal Garante della Privacy, sono una serie di regole che hanno la medesima forza gerarchica delle disposizioni codicistiche e che costituiscono delle condizioni di liceità vere e proprie.

Le misure di garanzia sono revisionate biennialmente e sono adottate sentito il Ministero della Salute che, all'uopo, acquisisce il parere del Consiglio Superiore di Sanità.

Gli ambiti che dovrebbero essere disciplinati dalle misure di garanzia (contrassegni ZTL – gestione sanitaria – comunicazione diagnosi – prescrizioni ecc) sono oggi disciplinati dal vecchio codice della privacy (art. 83 e ss), e tali disposizioni rimarranno in vigore fino ad approvazione delle misure di garanzia¹³.

In conclusione, ulteriore riferimento normativo in materia di privacy è rappresentato dalle regole di condotta, introdotte dal GDPR. Diversamente dalle misure di garanzia e delle regole deontologiche, esse non costituiscono delle condizioni di liceità del trattamento. Il GDPR, ai sensi dell'art. 40, sancisce che «Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese».

¹¹ Cfr. Art. 2-quater (Regole deontologiche), d.lgs 101/2018, «Il Garante promuove, nell'osservanza del principio di rappresentatività e tenendo conto delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, l'adozione di regole deontologiche per i trattamenti previsti dalle disposizioni di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 4, e al capo IX del Regolamento, ne verifica la conformità alle disposizioni vigenti, anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto».

¹²Cfr. Art. 2-septies (Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute), d.lgs 101/2018, «In attuazione di quanto previsto dall'articolo 9, paragrafo 4, del regolamento, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo».

¹³In tal senso, il d.lgs 101/2018 espressamente chiarisce che le disposizioni di cui agli art. 83 e ss del d.lgs n.196 30 giugno 2003 sono abrogate ma il contenuto descrittivo resta in vigore fintanto che non siano adottate le misure di garanzia.

4. Il trattamento dei dati personali in ambito sanitario

Con riferimento al trattamento dei dati relativi alla salute, il legislatore comunitario ha stravolto l'approccio metodologico fino a quel momento previsto dal codice della privacy.

Oggi il Regolamento Europeo ha previsto, con riferimento ai dati particolari, quale regola generale l'esclusione del trattamento degli stessi¹⁴. Tuttavia, l'art. 9 statuisce che la regola possa essere derogata in tutta una serie di ipotesi¹⁵, che possono raggrupparsi in tre macro-aree. La prima macro-area ricomprende i trattamenti effettuati per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (art. 9 par. 2 lett. g)); la seconda, i trattamenti effettuati per finalità di medicina

¹⁴ Cfr. Art. 9, par. 1, GDPR, «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

¹⁵ 15 Cfr. Art. 9, par. 2 2., GDPR «Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: (C51, C52) a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli 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, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per 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; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitano le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che 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; (C55, C56) h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; (C53) i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; (C54) j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o del diritto nazionale degli Stati membri o conformemente al contratto con un professionista della sanità, effettuati da un professionista sanitario soggetto al segreto professionale, o sotto la sua responsabilità, o da altra persona anch'essa soggetta all'obbligo di segretezza (art. 9 par. 2 lett. h)); infine, i trattamenti effettuati per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9 par. 2 lett. i)).

E' opportuno precisare che i trattamenti in ambito sanitario seguono regole differenti, variando i presupposti di liceità, a seconda della finalità del trattamento perseguita. Per una completa analisi della tematica, è opportuno chiarire come la normativa antecedente al GDPR, distingueva il trattamento dei dati in materia di salute per finalità di cura, per il quale vigeva il binomio "informativa – consenso", e il trattamento per fini amministrativi ammesso in presenza di una norma di legge che indicasse i tipi di dati trattati e le operazioni eseguibili (es: il regolamento dei dati sensibili).

Tanto premesso, l'attuale disciplina, con riferimento alla finalità di cura prevede che il trattamento sia ammesso, *ex art. 9 par. 2 lett. h)*, ogniqualvolta effettuato per finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o del diritto nazionale degli Stati membri o conformemente al contratto con un professionista della sanità, effettuati da un professionista sanitario soggetto al segreto professionale, o sotto la sua responsabilità, o da altra persona anch'essa soggetta all'obbligo di segretezza; in presenza di tale specifiche finalità, non è richiesto alcun consenso dell'interessato. Resta, tuttavia, ferma la necessità che all'interessato sia illustrata una chiara e attuale informativa rispetto al trattamento dei dati. Il consenso, infatti, veniva prestato solo successivamente ad una completa informativa che veniva illustrata all'interessato.

La previgente normativa italiana, come sopra accennato e diversamente da oggi, al fine di consentirne il trattamento, richiedeva sia il consenso scritto dell'interessato che l'autorizzazione generale del Garante. Più precisamente, nei casi previsti *ex art. 76 del Codice dalla privacy* (oggi abrogato), i requisiti del consenso o dell'autorizzazione del Garante potevano anche alternativamente venire meno. Il consenso veniva prestato solo successivamente ad una precisa, chiara e attuale informativa che veniva illustrata all'interessato.

La ormai superata disciplina, inoltre, semplificava la procedura di manifestazione del consenso in caso di emergenza, stabilendo che l'informativa e il consenso al trattamento dei dati personali potevano intervenire senza ritardo, successivamente alla

prestazione. Attualmente, il riformato art. 82 del codice non menziona più il consenso nei casi di emergenza, non essendo quest'ultimo più necessario. In particolare, non si pone più attenzione ai c.d. "casi di emergenza", essendo comunque ammessi (e senza il consenso), i trattamenti dei dati quando necessari per i trattamenti effettuati per le finalità di cura di cui all'art. 9 par. 2 lett. h) del GDPR.

A causa delle difficoltà interpretative volte a comprendere cosa rientrasse nel trattamento necessario per garantire la finalità di cura, il Garante con provvedimento del 7 Marzo 2019 ha ribadito che i trattamenti ammessi sono quelli necessari per finalità di cura effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona soggetta all'obbligo di segretezza, chiarendo – inoltre - alcune ipotesi che, sia pure connesse alla finalità di cura, non rientrano in quanto previsto ex art. 9, par. 2 lett. h) e, pertanto, necessitano sia dell'informativa che del consenso. Tra queste ipotesi, si ricorda il trattamento dei dati sanitari per il tramite delle App mediche, del FSE¹⁶, DSE¹⁷, e dei Referti on-line.

Con riferimento al trattamento dei dati relativi al diritto alla salute per motivi di interesse pubblico, similmente a quanto previsto prima dell'entrata in vigore del Regolamento EU, ex art. 2 sexies del codice della privacy, si ammette qualora tali motivi siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. Pertanto, in tal caso, il trattamento non incontra il binomio "informativa – consenso", ma sarà la presenza di una base normativa a consentire la possibilità di trattamento. Ai sensi del comma 2 dell'art. 2 sexies sopra citato, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio

¹⁶ Il fascicolo sanitario elettronico è istituito, previo consenso dell'assistito, dalle Regioni e Province autonome, per finalità di cura. I professionisti sanitari, infatti, sempre previa autorizzazione del paziente, possono consultare i documenti contenuti nel fascicolo, ricostruendo rapidamente tutte le informazioni sanitarie che descrivano lo stato di salute del paziente. Inoltre, all'interno del FSE confluiscono anche tutti i documenti sanitari, come ad esempio, prescrizioni di medicinale, prescrizioni di visite specialistiche, referti ecc.

¹⁷ DSE, esso è lo strumento costituito presso uno specifico organismo sanitario (esempio un ospedale, una casa di cura ecc). Il DSE contiene la storia sanitaria di un paziente completa e sempre aggiornata, limitatamente, però, alle analisi ed alle prestazioni effettuate presso la struttura sanitaria che ha costituito il DSE. Il DSE è accessibile solo ai professionisti sanitari operanti in quella specifica struttura e che hanno in cura il paziente. È lo strumento appartenente ad ogni singolo titolare del trattamento dati (professionista o struttura sanitaria) in grado di unificare le informazioni relative ad un paziente ed ai trattamenti a cui si sottopone nel corso della sua permanenza in struttura. Il DSE, a differenza del Fascicolo Sanitario Elettronico, quindi, non descrive l'intera vita sanitaria del paziente, ma soltanto la storia sanitaria "vissuta" in una specifica struttura. Inoltre, diversamente dal FSE, il DSE non prevede un iter di attivazione a cura del paziente. Sarà il personale sanitario dell'ospedale che procederà alla raccolta del consenso in forma orale con contestuale annotazione informatica, nel momento in cui il paziente effettuerà un accesso presso l'ospedale.

Il paziente potrà dunque scegliere autonomamente se costituire o meno il DSE. Il mancato consenso alla sua costituzione non incide sulla possibilità di accedere alle cure richieste.

di pubblici poteri in particolari materie. Tra queste, rientrano le attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano¹⁸; i compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica¹⁹; la programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale²⁰; la vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria²¹; infine, la tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili²².

Ulteriormente, il trattamento dei dati relativi alla salute è consentito, *ex art.* 9 lett. i) del Regolamento EU se il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale. Al riguardo, il considerando 54 del sopra citato Regolamento precisa che «il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato. Tale trattamento dovrebbe essere soggetto a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche. In tale contesto, la nozione di sanità pubblica dovrebbe essere interpretata secondo la definizione del regolamento (CE) n. 1338/2008 del Parlamento europeo e del Consiglio: tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità. Il trattamento dei dati relativi alla salute effettuato per motivi di interesse pubblico non dovrebbe comportare il trattamento dei dati personali per altre finalità da parte di terzi, quali datori di lavoro, compagnie di assicurazione e istituti di credito». Da quanto sopra dettagliato, emerge che il trattamento dei dati sulla salute per sanità pubblica si legittima in forza di situazioni emergenziali, in presenza di gravi minacce alla salute. Ad

¹⁸ Art. 2 sexies comma 2 lett. t) codice privacy.

¹⁹ Art. 2 sexies comma 2 lett. u) codice privacy

²⁰ Art. 2 sexies comma 2 lett. v) codice privacy

²¹ Art. 2 sexies comma 2 lett. z) codice privacy

²² Art. 2 sexies comma 2 lett. aa) codice privacy

esempio, in virtù della Delibera del Consiglio dei Ministri 31 gennaio 2020, che ha dichiarato lo stato di emergenza nazionale fino al 31 luglio 2020, con ordinanza del Capo del Dipartimento della Protezione civile (O.C.D.P.C.) n. 630 del 3 febbraio 2020 è stato previsto che le PP.AA possano effettuare tutti i trattamenti di dati personali che risultino necessari all'espletamento delle funzioni attribuitegli nell'ambito dell'emergenza da COVID-19, adottando le misure necessarie nel rispetto dei principi dell'art. 5 del Regolamento²³.

5. Gli obblighi dei soggetti che effettuano trattamenti dei dati

I soggetti che trattano i dati che concernono la materia sanitaria sono tenuti a vari obblighi. Tali adempimenti, che la recente novella ha ulteriormente valorizzato, possono considerarsi espressione di una delle principali novità introdotte dal Regolamento EU, ovverosia del concetto di *accountability*. L'*accountability*, infatti, è un principio che si sostanzia in una molteplicità di processi volti a responsabilizzare i soggetti coinvolti nel trattamento dei dati²⁴. Tanto premesso, primo fra tutti gli obblighi, il dovere di informare l'interessato sulle modalità del trattamento²⁵, nell'ambito di una

²³ Cfr. art. 5, GDPR, «I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»). 2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo («responsabilizzazione»).

²⁴ Cfr. L.Dagani – A.Lopez – S.Familiari, L'applicazione del GDPR Privacy nei servizi socio-sanitari, 15, Maggioli editore, 2018;

²⁵ Cfr. C.Colapietro – F.Laviola, I trattamenti di dati personali in ambito sanitario, dirittifondamentali.it, ISSN: 2240-9823 . 22, «Riguardo ai trattamenti di dati in ambito sanitario, il Garante, nel citato provvedimento del 7 marzo 2019, ha suggerito di “fornire all'interessato le informazioni previste dal Regolamento in modo progressivo”. Con tale espressione l'Autorità ha voluto intendere che, dal momento che ai sensi art. 79 del Codice “nei confronti della generalità dei pazienti afferenti a una struttura sanitaria potrebbero essere fornite solo le informazioni relative ai trattamenti che rientrano nell'ordinaria attività di erogazione delle prestazioni sanitarie”, talune informazioni relative “a particolari attività di trattamento (es. fornitura di presidi sanitari, modalità di consegna dei referti medici on-line, finalità di ricerca) potrebbero essere rese, infatti, in un secondo momento, solo ai pazienti effettivamente

gestione trasparente dei dati. Il dettaglio delle informazioni da fornire è descritto dagli articoli 13 e 14 del Regolamento. In particolare, l'art. 13 del sopra citato Regolamento²⁶ delinea le informazioni da fornire qualora i dati personali siano raccolti presso l'interessato, mentre l'art. 14 descrive le informazioni da fornire qualora i dati personali non siano stati raccolti presso l'interessato. Più nel dettaglio, coerentemente con quanto descritto con gli artt. 13 e 14 del GDPR, l'informativa che ogni interessato deve ricevere, ricomprende l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; i dati di contatto del responsabile della protezione dei dati, ove applicabile; le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; infine, ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

Entrambe le disposizioni sopra richiamate descrivono, inoltre, le ulteriori informazioni che il titolare del trattamento è tenuto a fornire, nel momento in cui riceve le informazioni dall'interessato²⁷. Tra queste, si ricordano il periodo di conservazione

interessati da tali servizi e ulteriori trattamenti". Così facendo, secondo il Garante, si accrescerebbero i benefici derivanti da una maggiore consapevolezza rispetto alle informazioni "veramente rilevanti".

²⁶ Cfr. Considerato 60 e 62 del GDPR.

²⁷ Cfr. Art. 13, comma 2, GDPR «In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) il diritto di proporre reclamo a un'autorità di controllo; e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2. 4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.». Art. 14 comma 2 e ss « 2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; c) l'esistenza del diritto dell'interessato di

dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo, e l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi. Con riferimento alla conservazione dei dati personali, il Garante, con provvedimento del 7 marzo 2019, ha evidenziato che, eccetto le ipotesi in cui i tempi sono dettati da altre norme dell'ordinamento, il titolare del trattamento, in piena armonia con il principio di accountability «dovrà individuare tale periodo in modo che i dati siano conservati, in una forma che consenta l'identificazione degli interessati, per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati sono trattati (principio di limitazione della conservazione, art. 5, par. 1, lett. e) del Regolamento) e indicare tale periodo (o i criteri per determinarlo) tra le informazioni da rendere all'interessato».

Quanto al diritto di accesso, ai sensi dell'art. 15 del Regolamento, l'interessato potrà accedere ad una serie di informazioni, quali la finalità del trattamento, le categorie dei dati personali in questione, i destinatari o le categorie dei destinatari a cui i dati personali sono o saranno comunicati, il periodo di conservazione dei dati ecc.

Ulteriore, importante obbligo a carico dei titolari dei trattamenti effettuati in ambito sanitario è quello di designare il Responsabile della Protezione dei dati (o Data Protection Officer, DPO). In particolare, il Regolamento EU, all' art.31 par. 1, statuisce

chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca; e) il diritto di proporre reclamo a un'autorità di controllo; f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico; g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2: a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati; b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali. 4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2. 5. I paragrafi da 1 a 4 non si applicano se e nella misura in cui: a) l'interessato dispone già delle informazioni; b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni; c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge».

che il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; ancora, tale obbligo sussiste se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala. Infine, il DPO è obbligatorio ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Al fine di rendere maggiormente chiare le ipotesi in cui tale nomina è obbligatoria, il Garante della Privacy, con il già citato provvedimento, ha affermato che i trattamenti dei dati personali che riguardano i pazienti e che sono effettuati da un'azienda sanitaria appartenente al SSN devono ricondursi a quelli per i quali, ex art. 37, vige l'obbligo di nomina del DPO. Ciò, sia in quanto rientrano nella categoria di organismi pubblici, sia in quanto le attività principali del titolare o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali.

Infine, un altro obbligo in capo ai titolari di trattamenti di dati concernenti la salute è quello relativo alla tenuta del registro delle attività di trattamento. Anche quest'obbligo, descritto dall'art. 30 del GDPR, è espressione del principio di accountability, che consente di "responsabilizzare" il titolare del trattamento dei dati. Infatti, tramite il registro è possibile monitorare quale siano i trattamenti in corso e quali siano i conseguenti rischi.

Il suddetto obbligo non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1 del Regolamento, o i dati personali relativi a condanne penali e a reati di cui al successivo articolo 10²⁸.

²⁸ Cfr. Provvedimento del Garante del 7 marzo 2019 "essendo le fattispecie di esenzione di cui all'art. 30, par. 5 del Regolamento tra loro alternative, la deroga alla tenuta del registro non opera in presenza anche di uno solo degli elementi indicati dal predetto par. 5 (trattamento che presenta un rischio per i diritti e le libertà per l'interessato, trattamento non occasionale, trattamento che includa categorie particolari di dati di cui all'art. 9 o dati relativi a condanne penali e a reati)".