L'analisi del rischio del trattamento dei dati relativi alla salute in ambito sanitario

Privacy e "Cura" dei Dati in Sanità

Filippo Lorè


Filippo Lorè

Professore a contratto per l'insegnamento "Trattamento dei dati sensibili" – Dipartimento di Informatica dell'Università degli studi di Bari "A. Moro"

Corrispondenza a:
Dott. Filippo Lorè
Docente a contratto Università degli Studi di Bari
e-mail: Filippo.lore@yahoo.it

ABSTRACT
Il presente contributo muove i passi dalle disposizioni del Regolamento generale UE 2016/679 che impone al titolare del trattamento, secondo il principio dell'*accountability*, l'adozione di misure tecniche ed organizzative utili a dimostrare (e comprovare) la piena adesione alla disciplina europea in materia di protezione dei dati personali. L'atteggiamento formale alla tematica, quindi, deve lasciare il passo a quello sostanziale che si concretizza nell'approccio basato sulla valutazione e sugli impatti del rischio (*risk based approach e impact based*). L'implementazione delle misure di sicurezza legate al trattamento dati personali, anche in ambito sanitario, devono tendere necessariamente alla tutela della riservatezza, della disponibilità e dell'integrità degli stessi allo scopo di garantire agli interessati il libero godimento delle libertà fondamentali.
Il contributo traccia il percorso normativo vigente che il trattamento dei dati personali deve seguire, perché nel loro utilizzo non si verifichi l'errore, la violazione o, addirittura, il danno. Questo richiede una attenta valutazione da parte del titolare, che deve seguire delle tappe obbligatorie per rilevare il livello di criticità emergenti per le persone fisiche coinvolte.
La ricerca di un equilibrio tra tutela della salute (pubblica) del cittadino e la tutela della riservatezza dei suoi dati personali passa attraverso l'analisi e l'osservanza della normativa privacy.

PAROLE CHIAVE: dati relativi allo stato di salute, privacy, analisi del rischio, valutazione dell'impatto, sicurezza delle informazioni

L'art. 5 del Regolamento UE 2016/679 afferma, tra gli altri, il principio di integrità e riservatezza: i dati devono essere 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 danneggiamento, anche accidentali, degli stessi. L'articolo 5, inoltre, al paragrafo 2, stabilisce che il titolare del trattamento (*Data Controller*) è competente per quanto espresso al paragrafo 1 e deve essere in grado di comprovarlo. Si tratta della c.d. *accountability* («responsabilizzazione») del titolare, una delle principali novità del Regolamento UE 2016/679, che attribuisce direttamente al titolare il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali. Nell'ambito del trattamento dei dati personali per finalità di cura del paziente, si segnala il Provvedimento del Garante per la protezione dei dati personali del 7 marzo 2019 [1], mediante il quale l'Autorità ha inteso chiarire alcuni aspetti riguardanti proprio i trattamenti dei dati relativi alla salute nel settore sanitario. Lo scopo dichiarato consiste nel dare un'interpretazione uniforme della normativa, e nel diradare, così, i dubbi interpretativi derivanti dal mutato assetto normativo. Invero, la normativa europea ha stabilito il generale divieto di trattamento per i dati attinenti alla salute di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria che rivelino informazioni relative al suo stato di salute [2]. Questo tipo di trattamento è consentito solo in presenza di taluni requisiti specifici individuati dall'art. 9, par. 2, del Regolamento UE 2016/679. Con il citato Provvedimento del 7 marzo 2019, il Garante è intervenuto sul fondamento giuridico del trattamento dei dati personali riguardanti la salute degli interessati.

Quanto alla disciplina relativa al trattamento dei dati relativi alla salute in ambito sanitario, le deroghe al generale divieto di trattare tali dati sono stabilite dall'art. 9, par. 2, del Regolamento UE 2016/679. Il divieto decade ogni qualvolta sussistano motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri [3], individuati, nell'ambito della normativa nazionale, dall'art. 2-sexies del Codice [4]; ancora, esso decade in presenza di motivi di interesse pubblico nel settore della sanità pubblica 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 [5]; infine, nei casi in cui il trattamento dei dati riguardanti la salute dell'individuo sia posto in essere per finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali ("finalità di cura") sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità, (effettuati da o sotto la responsabilità di un professionista sanitario) soggetto al segreto professionale o da altra figura, ugualmente tenuta all'obbligo di segretezza [6].

Quest'ultima eccezione presenta alcune particolarità, tanto è vero che l'Autorità di controllo fornisce un ulteriore chiarimento. I trattamenti per "finalità di cura", sulla base dell'art. 9, par. 2, lett. h) e par. 3 del Regolamento, sono propriamente quelli effettuati da (o sotto la responsabilità di) un professionista sanitario [7] soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza. Ne deriva che, in merito all'ambito oggettivo, i trattamenti afferenti, in senso lato, alla cura, richiedono, invece, una distinta base giuridica da individuarsi, eventualmente, nel consenso dell'interessato [8] o in un altro presupposto di liceità. Si pensi, in tal senso, ai trattamenti connessi all'utilizzo di "app" mediche che non rientrino nelle finalità della telemedicina, ai casi in cui il trattamento dei dati sia finalizzato alla fidelizzazione della clientela [9] o, ancora, alle operazioni sui dati personali effettuate per finalità promozionali o commerciali [10]**.** Con riguardo a quest'ultima categoria di dati, potrebbero essere oggetto di questo trattamento, oltre ovviamente ai dati c.d. comuni, categorie particolari di dati, come, ad esempio, quelli in grado di rivelare l'origine razziale o etnica, le convinzioni religiose o filosofiche, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla

salute o alla vita sessuale o all'orientamento sessuale della persona [11]. Inoltre, in specifiche circostanze, potrebbero essere oggetto di tali trattamenti dati relativi a condanne penali, reati o a connesse misure di sicurezza.

Come conseguenza, per il titolare del trattamento assume ancor più rilevanza l'obbligo di implementare le misure di sicurezza, tecniche ed organizzative, in piena adesione alle disposizioni del legislatore europeo in materia di protezione dati. Sovente le modalità del trattamento, in special modo in presenza di un utilizzo di nuove tecnologie, quali la c.d. sanità digitale, rendono il rischio elevato e il titolare del trattamento deve procedere ad una valutazione degli impatti [12] che il trattamento potrebbe avere sui diritti e sulle libertà dell'interessato, qualora si dovessero verificare determinate minacce. A tale scopo, ai sensi dell'art. 35, par. 7, lettera c), del Regolamento UE 2016/679, la richiamata valutazione d'impatto deve contenere, tra l'altro, una ponderazione circa i rischi relativi al libero godimento dei diritti fondamentali degli interessati. Secondo quanto enunciato, altresì, nel Considerando 75 del Regolamento UE 2016/679, i rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare, tra gli altri, da operazioni di trattamento di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo. In secondo luogo, tale danno può verificarsi se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro inibito l'esercizio del controllo sui dati personali che li riguardano. Il rischio per i diritti e le libertà fondamentali delle persone fisiche può verificarsi, altresì, nel momento in cui sono trattati informazioni di carattere personale che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza. Ancora, il richiamato pregiudizio si riscontra qualora il trattamento implichi la valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti. In ultimo, vi è pericolo che si concretizzi un danno qualora vengano effettuate operazioni di dati personali di persone fisiche vulnerabili, in particolare minori, oppure se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Per ogni rischio occorrerà, dunque, individuare la probabilità dell'evento, nonché la gravità dello stesso. Nel 2017, l'Agenzia ENISA [13] ha pubblicato il manuale sulla sicurezza nel trattamento dei dati personali [14], che funge, tuttora, da ausilio per le organizzazioni chiamate a rispettare, in ordine alle operazioni di trattamento dei dati personali, criteri di sicurezza valutabili in modo oggettivo. Allo scopo di rispettare le disposizioni previste dall'art. 35, par. 7, lettera c), del Regolamento UE 2016/679, è necessario procedere ad una valutazione d'impatto che contenga, a sua volta, una preventiva analisi dei rischi per i diritti e le libertà degli interessati. Questa procedura, nello specifico, si compone di due fasi. La prima fase consiste in una vera e propria analisi dei rischi del trattamento di dati personali che si vuole svolgere, mentre, la seconda fase, è costituita da una procedura di autovalutazione delle misure di sicurezza implementate dal *data controller*. Con riguardo alla prima di queste fasi, il primo *step* richiede la corretta definizione delle operazioni effettuate sui dati personali e il relativo contesto; il secondo passo è rappresentato dalla comprensione e valutazione dell'impatto (*gravità delle conseguenze*) [15]; il terzo *step* consiste nella definizione di possibili minacce e nella determinazione delle loro probabilità (*probabilità di occorrenza della minaccia*); con il quarto *step* si attua una valutazione finale del rischio, combinando la probabilità di accadimento della minaccia con la gravità delle possibili conseguenze. In ultimo, si procede all'implementazione delle misure di sicurezza necessarie per ridurre il rischio. Il punto di

partenza della valutazione del rischio è fondamentale per il titolare del trattamento dei dati, al fine di definire i confini del sistema di elaborazione dei dati (in corso di valutazione) e il relativo contesto. Nel fare ciò, l'organizzazione deve considerare le diverse fasi del ciclo di vita dei dati (ad esempio, raccolta, archiviazione, utilizzo, trasferimento), insieme ad aspetti rilevanti, come i soggetti destinatari dei dati e i mezzi utilizzati per l'elaborazione. Con riferimento al secondo degli *step* elencati pocanzi (valutazione dell'impatto), il titolare del trattamento dei dati è guidato a valutare il potenziale impatto sui diritti e sulle libertà delle persone che un incidente di sicurezza (correlato al sistema di elaborazione dei dati) potrebbe comportare, in seguito ad una potenziale violazione di riservatezza, integrità e disponibilità dei dati personali. La valutazione dell'impatto è un processo qualitativo e pertanto il *data controller* deve considerare una serie di fattori, quali, a titolo esemplificativo: la tipologia di dati, le criticità legate alle operazioni di trattamento, il volume dei dati personali, le caratteristiche speciali del responsabile del trattamento [16], nonché le categorie degli interessati [17]. Procedendo, vengono considerati quattro livelli di impatto (Basso, Medio, Alto, Molto alto). Nel livello Basso non si ha nessun impatto rilevante, trattandosi di problematiche che l'interessato può superare senza problemi, quali fastidio, irritazione e perdita di fiducia; il livello Medio racchiude pregiudizi significativi che gli interessati dovrebbero essere in grado di superare nonostante alcune difficoltà, quali costi aggiuntivi, impossibilità di accedere a servizi o opportunità (ad esempio, rifiuto di accesso ai servizi aziendali), paura, mancanza di comprensione, stress, disturbi fisici lievi, disturbi psicologici lievi e perdita di riservatezza; il livello Alto si verifica, invece, quando l'impatto si manifesta con conseguenze significative che gli interessati dovrebbero essere in grado di superare, seppur con gravi difficoltà. Si pensi, ad esempio, a casi di perdita finanziaria (a titolo meramente esemplificativo, appropriazione indebita di fondi e frode), lista nera da parte delle banche, danni alla proprietà, perdita del posto di lavoro, citazione in giudizio, peggioramento della salute, disturbi psicologici a breve o medio termine, perdita di controllo sull'uso dei dati personali, danno reputazionale e/o discriminazione, impossibilità di esercitare i diritti (non solo quelli previsti dalla normativa privacy) e qualsiasi altro svantaggio economico o sociale significativo. Il livello Molto Alto, infine, racchiude tutte quelle conseguenze significative, o addirittura irreversibili, che gli interessati non possono superare: stigmatizzazione, squilibrio di potere, perdita di riservatezza di dati personali coperti da segreto professionale, debito sostanziale, incapacità al lavoro, disturbi psicologici a lungo termine, disturbi fisici gravi e morte. Se ne desume che, quest'ultimo caso, verrà preso in esame quando l'evento temuto si è manifestato in tutta la sua forza.

Sulla base dei livelli di impatto appena esaminati viene effettuata, ad opera del titolare del trattamento, una analisi in termini di riservatezza, integrità e disponibilità dei dati personali, nonché, successivamente, una valutazione d'impatto globale, che, nel caso del trattamento dei dati relativi alla salute in ambito sanitario si porrà, ovviamente, ad un livello Molto Alto. Con riferimento al terzo degli *step* elencati pocanzi, è opportuno ricordare che una minaccia consiste in qualsiasi circostanza o evento, la cui realizzazione può influire negativamente sulla sicurezza dei dati personali. In questa fase, l'obiettivo è comprendere il livello di pericolo relativo all'ambiente generale del trattamento dei dati personali (esterno o interno) e valutare, conseguentemente, la probabilità di accadimento di un evento (probabilità di occorrenza di una minaccia). A questo proposito, si potrebbero considerare vari livelli e tipi di minacce alla riservatezza, integrità e disponibilità dei dati personali. La valutazione della probabilità di insorgenza di una minaccia, dunque, può essere solo qualitativa, in quanto legata allo specifico ambiente di elaborazione dei dati personali. Sono tre i livelli di probabilità riscontrabili, nel seguente ordine: Basso, secondo cui è improbabile che la minaccia si materializzi; Medio, quando è possibile che la minaccia si concretizzi; Alto, quando vi è concreta probabilità che la minaccia si verifichi. Per semplificare il processo, possiamo scomporre in quattro macro aree di valutazione le probabilità relative alle violazioni. La prima riguarderà le risorse di rete e tecniche (hardware e software); la seconda analizzerà i processi

o le procedure relative al trattamento dei dati; la terza esaminerà parti e persone diverse coinvolte nell'operazione di elaborazione; da ultimo, si analizzerà un'area di valutazione del settore di riferimento e delle dimensioni del trattamento. All'esito, la probabilità di occorrenza della minaccia coinciderà con il più alto dei punteggi ottenuti. Per ognuna di queste aree sarà allora opportuno, per il titolare del trattamento, porsi una serie di quesiti. Per la prima area di valutazione, relativa alla rete e alle risorse tecniche, occorrerà valutare se: parte del trattamento dei dati personali venga eseguito mediante rete Internet; l'accesso a un sistema interno di trattamento dei dati personali venga consentito ad altri soggetti (ad esempio per determinati utenti o gruppi di utenti); il sistema di elaborazione dei dati personali sia interconnesso ad altro sistema o servizio IT, esterno o interno all'organizzazione; persone non autorizzate possano accedere facilmente all'ambiente di elaborazione dei dati; il sistema di elaborazione dei dati personali sia progettato, implementato o gestito senza seguire le migliori *best practices*. Dopodiché, sulla base delle valutazioni di cui sopra, è necessario valutare la probabilità che si verifichino minacce per l'intera area di valutazione. Nel caso del trattamento dei dati relativi alla salute in ambito sanitario, tale valutazione si pone, presumibilmente, ad un livello Medio. Allo stesso modo, si può procedere per le altre aree di valutazione. Per la seconda area di valutazione, relativa ai processi o alle procedure per il trattamento dei dati, occorrerà che il titolare del trattamento valuti se: le responsabilità in relazione al trattamento dei dati personali siano chiaramente definite [18]; l'utilizzo della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione sia circoscritto; il personale dipendente sia stato autorizzato a trasferire, archiviare o altrimenti elaborare dati personali al di fuori dei locali dell'organizzazione; le attività di trattamento dei dati personali possano essere eseguite senza la creazione di file di registro. Come per la prima, anche per questa seconda area di valutazione si dovrà valutare la probabilità che si verifichino le minacce. Nel caso del trattamento dei dati relativi alla salute in ambito sanitario, tale valutazione è ipotizzabile ad un livello Basso. Nell'area di valutazione relativa alle parti e alle persone coinvolte nel trattamento dei dati personali, occorrerà valutare se: il trattamento dei dati personali venga eseguito da un numero indefinito di dipendenti; parte dell'operazione di trattamento dei dati venga eseguita da un contraente o terza parte (responsabile del trattamento dei dati); gli obblighi delle parti e delle persone coinvolte nel trattamento dei dati personali siano chiaramente definiti; il personale coinvolto nel trattamento dei dati personali sia stato adeguatamente formato in ordine alle misure di sicurezza; le persone e le parti coinvolte nel trattamento dei dati trascurino di archiviare e/o distruggere in modo sicuro le informazioni personali. Anche per questa terza area di valutazione si dovrà valutare la probabilità che si verifichino minacce. Nel caso del trattamento dei dati relativi alla salute in ambito sanitario, tale valutazione si pone ad un livello Medio. Infine, per la quarta ed ultima area di valutazione, relativa al settore di riferimento e al volume di dati trattati, si valuterà se: il settore di riferimento sia incline agli attacchi informatici [19]; l'organizzazione abbia subito attacchi informatici o altri tipi di violazione della sicurezza negli ultimi due anni; si siano ricevute notifiche e/o reclami in merito alla sicurezza del sistema IT (utilizzato per il trattamento dei dati personali) nell'ultimo anno; le operazioni di trattamento riguardi un grande volume di persone e/o dati personali [20]; esistano buone pratiche di sicurezza. Anche per quest'ultima area di valutazione si dovrà valutare la probabilità che si verifichino minacce. Nel caso del trattamento dei dati relativi alla salute in ambito sanitario, tale valutazione si pone, ragionevolmente, ad un livello Medio. A questo punto si procederà alla valutazione globale delle minacce (probabilità di occorrenza), che, alla luce delle valutazioni fin qui esposte, sulla scorta della tabella di seguito riportata, nel caso del trattamento dei dati relativi alla salute in ambito sanitario si pone ad un livello Medio, considerato che il valore complessivo è di 7.

PROBABILITA' ACCADIMENTO EVENTI CHE COMPROMETTONO LA RISERVATEZZA	RISCHIO POTENZIALE PER LA RISERVATEZZA IMPATTO PER RISERVATEZZA			
	BASSO	MEDIO	ALTO	MOLTO ALTO
BASSO	Molto Basso	Basso	Basso	Basso
MEDIO	Basso	Basso	Medio	Medio
ALTO	Basso	Medio	Alto	Alto
MOLTO ALTO	Medio	Medio	Alto	Molto Alto

Possibilità che si verifichino uno o più eventi temuti:

- *Basso (da 0 a 5): l'evento temuto non si manifesta*
- *Medio (da 6 a 12): l'evento temuto potrebbe manifestarsi*
- *Alto/Molto Alto (da 13 a 16): l'evento temuto si è manifestato*

Tabella 1: analisi globale delle minacce sulla base del modello ENISA

Il quarto *step* consiste nella valutazione finale del rischio, che verrà stabilito in base alla Tabella 2 di seguito riportata. Nel caso del trattamento dei dati relativi alla salute in ambito sanitario, considerati i livelli di rischio ottenuti negli *step* 2 e 3, ovvero un livello Molto Alto per i possibili impatti per gli interessati e un livello Medio per le probabilità di occorrenza delle minacce, la valutazione finale del rischio si porrà ad un livello Alto.

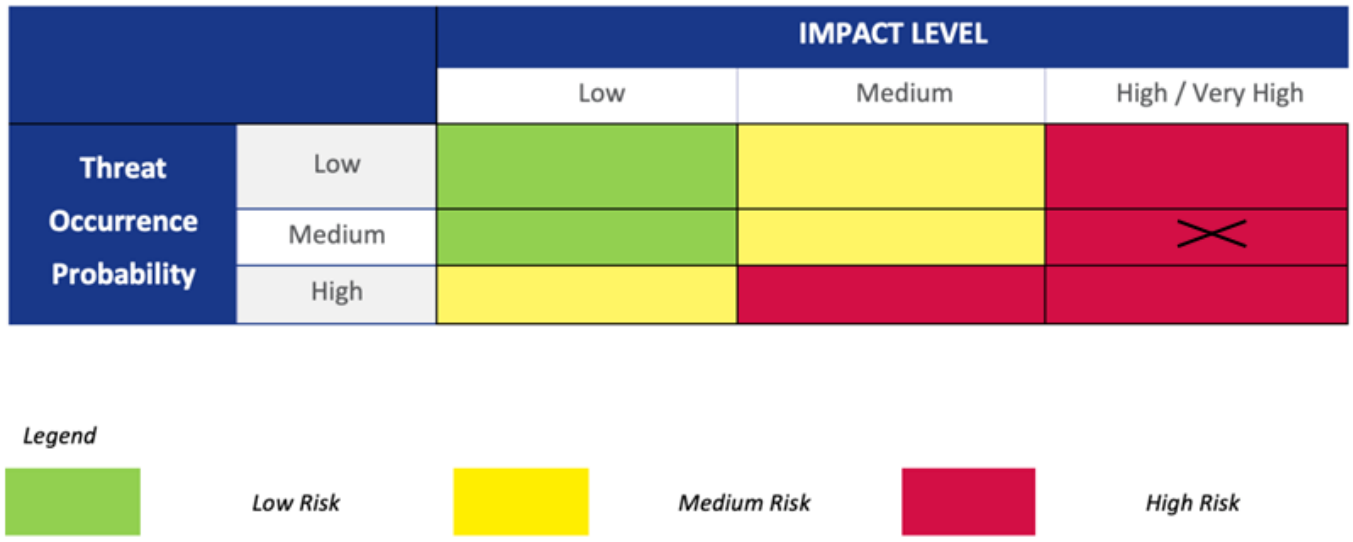

Tabella 2: valutazione del rischio sulla base del modello ENISA

Infine, come quinto ed ultimo *step* di questa prima fase della procedura e a seguito della valutazione del livello di rischio, il titolare del trattamento potrà procedere alla selezione di misure di sicurezza adeguate alla protezione dei dati personali. L'adeguatezza delle misure a livelli di rischio specifici non deve essere percepita come assoluta, poiché, a seconda del contesto del trattamento dei dati personali, l'organizzazione potrà anche adottare opportune misure aggiuntive.

Concludendo, la seconda fase della procedura consiste in un'autovalutazione delle misure di sicurezza implementate, allo scopo di tenere sotto controllo il livello di rischio. Il titolare del trattamento, infatti, sulla base delle risultanze della procedura, potrebbe dover (ri)verificare lo stato di adozione ed attuazione delle misure (tecniche ed organizzative) proposte. Attraverso l'autovalutazione, allora, il titolare potrà analizzare il livello di rischio per una particolare operazione di trattamento dei dati personali (ad esempio, raccolta, archiviazione, consultazione, comunicazione), fornendo una breve descrizione del contesto, tenendo sotto controllo le misure già implementate e quelle, invece, di prossima implementazione. All'interno di tale scenario, nel settore sanitario risulta strettamente necessario il rispetto di specifici requisiti di sicurezza [21] mediante l'adesione a obblighi normativi derivanti, ad esempio, dalla Direttiva e-privacy, dalla Direttiva NIS, dalla Direttiva sui servizi di pagamento (PSD 2), dal Regolamento UE 2019/881 in materia di

cybersicurezza [22], dalla Legge n. 133 del 18 novembre 2019, nonché dagli indirizzi diramati dalle Autorità di controllo europee in materia di protezione di dati personali, le quali hanno fornito diversi contributi in ordine alla definizione delle misure di sicurezza [23].

Note

[1] Provvedimento del Garante per la protezione dei dati personali del 7 marzo 2019, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, 7 marzo 2019, in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9091942

[2] Si veda il Considerando 35 al Regolamento UE 2016/679.

[3] Art. 9, par. 2, lett. g) Regolamento UE 2016/679, «Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: […] 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».

[4] L'art. 2 sexies del D.Lgs n.196, così come modificato dal D.Lgs n. 101/2018, stabilisce una elencazione dei trattamenti fondati su un "rilevante interesse pubblico" effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri. Si tratta, a titolo esemplificativo, dei seguenti trattamenti in materia di documentazione delle attività istituzionali di organi pubblici, attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci; attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano; compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica; programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale; vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria; tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;

[5] Art. 9, par. 2, lett. i) Regolamento UE 2016/679, «Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: […] 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».

[6] Art. 9, par. 2, lett. h), Reg. UE 2016/679, «Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: […] 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». Si veda anche l'art. 75 del Codice *privacy*, il quale nella sua nuova formulazione stabilisce che il trattamento dei dati personali effettuato per finalità di

tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere h) ed i), e 3 del regolamento, dell'articolo 2-septies del codice, nonché nel rispetto delle specifiche disposizioni di settore.

[7] Professionista sanitario è colui che, in forza di una disposizione di legge, può trattare dati sanitari: esercenti una professione sanitaria e gli organismi sanitari pubblici. Tra gli esercenti una professione sanitaria vi sono il farmacista, il medico chirurgo, l'odontoiatra, il veterinario, lo psicologo, l'infermiere, l'ostetrico, l'infermiere pediatrico, l'esercente professioni sanitarie riabilitative. Sono esclusi l'operatore di interesse sanitario e arti ausiliari delle professioni sanitarie come massaggiatore, ottico, odontotecnico, puericultrice.

[8] Art. 9, par. 2, lett. a) Reg. UE 2016/679 secondo il quale si prevede che il generale divieto di trattamento di categorie particolari dei dati decade qualora l'interessato presti validamente il consenso.

[9] Si pensi ai trattamenti effettuati dalle farmacie attraverso programmi di accumulo punti, al fine di fruire di servizi o prestazioni accessorie, attinenti al settore farmaceutico-sanitario, aggiuntivi rispetto alle attività di assistenza farmaceutica tradizionalmente svolta dalle farmacie territoriali pubbliche e private nell'ambito del Servizio sanitario nazionale (SSN).

[10] A titolo esemplificativo, promozioni su programmi di screening, contratto di fornitura di servizi ammnistrativi, come quelli alberghieri di degenza.

[11] Franco Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016, p. 298.

[12] Fabio Di Resta, *La nuova "Privacy europea": I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Giappichelli Editore-Linea Professionale, 2018, pp. 114-118.

[13] Acronimo di *European Union Agency for Network and Information Security*. L'ENISA funge da punto di riferimento per pareri e competenze in materia di cybersicurezza per le istituzioni, gli organi e gli organismi dell'Unione nonché per altri portatori di interessi pertinenti dell'Unione.

[14] Traduzione non ufficiale in italiano della pubblicazione ENISA "*Handbook on Security of Personal Data Processing*", https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

[15] S. Spiekermann, M. C. Oetzel, *A systematic methodology for privacy impact assessments: a design science approach*, European Journal of Information Systems, Volume 23, 2014 – Numero 2, p.5

[16] A. Santoro, *Nuove frontiere per l'efficienza dell'amministrazione fiscale: tra analisi del rischio e problemi di privacy*, La finanza pubblica italiana, Rapporto 2019, Il Mulino, 2019, p. 54

[17] S. J. De, D. Le Métayer, *Privacy Risk Analysis*, Synthesis Lectures on Information Security, Privacy and Trust, September 2016, ISBN 9781627054256, pp.93-96.

[18] Giacomo Conti, *La protezione dei dati personali per titolari e responsabili del trattamento*, Maggioli Editore, 2019, pp. 126-129.

[19] G. Ziccardi, P. Perri, *Tecnologia e diritto*, Informatica Giuridica, Vol. 2, Giuffrè Editore, ISBN 9788828810353, 2019, pp. 103-115.

[20] G. D'Acquisto, F. Pizzetti, *Regolamentazione dell'economia dei dati e protezione dei dati personali*, in Analisi Giuridica dell'Economia, 01/2019, Il Mulino, 2019, pp. 89-108.

[21] Mirza B. Murtaza, *Risk Management For Health Information Security And Privacy, American*

Journal of Health Sciences, Second Quarter 2012, Volume 3, Number 2.

[22] F. Lorè, *La sicurezza dei dati personali: misure e strategie alla luce delle recenti novità normative in materia di cybersecurity*, Rivista Ratio Juris, 2019, https://www.ratioiuris.it/la-sicurezza-dei-dati-personali-misure-e-strategie-alla-luce-delle-recenti-novita-normative-in-materia-di-cybersecurity/

[23] Il Garante per la protezione dei dati personali francese nelle Linee Guida "Privacy Impact Assessment (PIA)" fornisce una definizione di rischio assimilabile alla formulazione di "evento temuto", https://www.cnil.fr/en/guidelines-dpia