Il regolamento generale sulla protezione dei dati e le principali innovazioni in materia di sanità elettronica

Maria Gabriella Virone [1]

[1] *Dottore di ricerca in diritto e nuove tecnologie, Università degli Studi di Bologna*

ABSTRACT

At a distance of twenty years from the adoption of Directive 95/46/EC, the scenario has been changed. In particular, the use of Information and Communications Technologies has, among others, given: a) the definition of new business organizational models; b) new methods of collecting and usability of the data; c) the spread of digital forms for the storage of sensitive data; d) the increased transfer of personal data across national borders, internal and external.
In light of these changes, the European Union has set new goals in terms of protection of personal data in order to establish an atmosphere of trust among consumers. The proposal for a General Data Protection Regulation was officially presented by the European Commission on January 25th 2012 and is pending approval.
With the entry into force of the new regulatory text, also the national health system and the hospitals will be called upon to review methods of organization and internal processes. It is desirable to define new organizational policies that transpose three key elements of the proposed regulation: Privacy by Design, the Data Protection Office, the Privacy Impact Assessment.

Keywords: Data Protection; General Data Protection Regulation; e-Health

The General Data Protection Regulation and the main innovations in the field of e-health
Pratica Medica & Aspetti Legali 2015; 9(2): 31-36
http://dx.doi.org/10.7175/PMeAL.v9i2.1173

Corresponding author
Maria Gabriella Virone
mariagabriella.virone@gmail.com

Disclosure
L'autore dichiara di non avere conflitti di interesse di natura finanziaria in merito ai temi trattati nel presente articolo

INTRODUZIONE

La protezione dei dati personali è un tema sul quale, nel corso dei trascorsi decenni, la dottrina e la giurisprudenza, nazionale ed europea, più volte si sono interrogate per definirne peculiarità e limiti nonché per delineare provvedimenti e azioni normative. Altre branche del sapere, come la filosofia e la sociologia, hanno esaminato gli effetti sulla persona delle violazioni di informazioni sensibili e portato avanti iniziative volte a delineare, ad esempio, i profili etici del fenomeno. Non è, infine, mancato l'interesse degli operatori sanitari per le questioni afferenti il tema in esame, considerato il loro diretto coinvolgimento durante l'esercizio della professione in vicende, talora, anche di natura contenziosa. Altrettanto centrale è, poi, l'attenzione dei principali beneficiari, i cittadini/pazienti, cui i dati personali (identificativi e/o sensibili) si riferiscono.

In questo contesto non è ridondante ricordare che la protezione dei dati personali è, anzitutto, riconosciuta come diritto fondamentale dall'Unione Europea, un diritto distinto ma strettamente legato al «diritto al rispetto della vita privata e familiare».

Ad oggi, pietra miliare della normativa comunitaria in materia di protezione dei dati è la direttiva 95/46/CE che disciplina la tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati [1]. Implementata dalle legislazioni nazionali, la direttiva si applica in tutti gli Stati membri dell'Unione nonché in Islanda, Liechtenstein e Norvegia.

A distanza di un ventennio, però, lo scenario che la direttiva 95/46/CE aveva dinanzi a sé è mutato. In particolare, l'uso delle tecnologie dell'informazione e della comunicazione ha, tra gli altri, determinato:

- la definizione di nuovi modelli organizzativi aziendali;
- nuove modalità di raccolta e di fruibilità dei dati;
- la diffusione di forme digitali per la memorizzazione dei dati sensibili;
- il trasferimento crescente di dati personali attraverso le frontiere nazionali, interne ed esterne.

Inoltre, come rilevato dalle stesse istituzioni comunitarie, le disposizioni vigenti non hanno impedito la frammentazione delle modalità di applicazione della protezione dei dati personali tra gli Stati membri, né hanno eliminato l'incertezza giuridica e la diffusa percezione tra i cittadini che le operazioni *on line* comportino notevoli rischi [2-4].

Alla luce dei suddetti cambiamenti e criticità, l'Unione europea si è posta nuovi obiettivi sul fronte della protezione dei dati personali, proprio al fine di istaurare un clima di fiducia tra i consumatori. Le due linee strategiche perseguite possono così essere sintetizzate:

- delineare una politica forte e coerente in materia di protezione dei dati personali;
- predisporre un quadro legislativo comunitario più solido e "globale", idoneo alle sfide delle nuove tecnologie [5].

In questo senso, poi, è stata importante l'entrata in vigore del Trattato di Lisbona [6], il quale, all'articolo 16, paragrafi 1 e 2, riconosce il «diritto alla protezione dei dati personali» e assegna al Parlamento ed al Consiglio il compito di adottare norme in materia di protezione dei dati personali secondo la procedura legislativa ordinaria.

IL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

Quanto premesso è alla base della Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (o regolamento generale sulla protezione dei dati) [7].

Dopo mesi di intenso dibattito durante i quali sono stati avanzati più di tremila emendamenti al testo originario, la Proposta di regolamento è stata ufficialmente presentata dalla Commissione europea il 25 gennaio 2012; a distanza di un triennio si attende ancora l'approvazione definitiva per le ulteriori modifiche apportate al testo.

Prima di entrare nel merito dell'esame dell'articolato normativo, è bene richiamare la natura giuridica del regolamento comunitario, anche al fine di comprendere l'innovatività della revisione del quadro legislativo europeo.

Ai sensi dell'articolo 288, comma 2, del Trattato sul funzionamento dell'Unione Europea (TFUE), «Il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri» [6]. Dunque, a differenza della direttiva, che «[…] vincola lo Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi» (*ex* articolo 288, comma 3, TFUE), il regolamento non richiede alcun atto di recepimento o di attuazione da parte degli Stati membri, è direttamente applicabile dai giudici nazionali e prevale su disposizioni interne incompatibili.

L'univocità delle regole tra i ventotto Paesi membri ha, peraltro, considerevoli benefici anche sul fronte del contenzioso, dal momento che sia i cittadini sia gli operatori del diritto hanno la possibilità di conoscere, con esattezza ed *ex ante*, la normativa applicabile.

Tuttavia, nel caso del regolamento generale sulla protezione dei dati, una significativa eccezione a tale principio è costituita dal capo III, le cui norme consentono agli Stati membri, attraverso apposite disposizioni interne, di limitare gli obblighi e i diritti dell'interessato al trattamento.

Alla legislazione nazionale è altresì affidata la regolamentazione delle sanzioni penali sulla cui uniformità rimangono seri dubbi da parte degli osservatori più attenti.

Inoltre, come è stato evidenziato [8], se la normativa nazionale di recepimento della direttiva 95/46/CE sarà abrogata con l'entrata in vigore del regolamento, altrettanto non può sostenersi per tutti quei provvedimenti regolamentari e autorizzativi emessi dal Garante per la protezione dei dati personali sui quali occorrerà verificare per singolo atto la conformità o meno al regolamento stesso.

Diversi aspetti, pertanto, potranno essere chiariti soltanto con l'entrata in vigore del testo definitivo del regolamento generale sulla protezione dei dati.

PRINCIPALI INNOVAZIONI IN MATERIA DI SANITÀ ELETTRONICA

Gli articoli di seguito illustrati mostrano alcune delle principali novità previste dalla proposta di regolamento e i cui effetti si ripercuoteranno anche sul Servizio Sanitario Nazionale. L'impegno

che ne deriverà sarà essenzialmente a carico di tutti i soggetti a vario titolo coinvolti nel recepimento e nell'attuazione della normativa. In altre parole, tanto i vertici aziendali, quanto gli amministrativi e gli operatori sanitari saranno individualmente chiamati a rivedere sistemi organizzativi, procedure, percorsi formativi, modalità di erogazione dei servizi, ecc.

Come anzitutto evidenzia il considerando 66, «Nel definire le norme tecniche e le misure organizzative atte a garantire la sicurezza del trattamento, la Commissione deve promuovere la neutralità tecnologica, l'interoperabilità e l'innovazione e, ove opportuno, la cooperazione con i paesi terzi». Alla base, dunque, della revisione del quadro normativo in materia di protezione dei dati personali vi è l'attenzione al bilanciamento di alcuni importanti principi: la sicurezza dei sistemi informativi da una parte e l'interoperabilità e la neutralità tecnologica dall'altra. Questo aspetto è centrale per il Servizio Sanitario Nazionale che sempre più di frequente si trova ad operare in un'ottica di interdipendenza con i sistemi sanitari dei Paesi dell'Unione proprio a seguito di una maggiore mobilità di pazienti e operatori sanitari [9].

In particolare, l'adozione e implementazione di *standard* che promuovano l'interoperabilità tra sistemi indipendenti, il miglioramento della compatibilità tra dati e informazioni sanitarie nonché la riduzione delle ridondanze è un processo in essere da decenni nella sanità elettronica che richiede, però, una continua collaborazione sinergica tra i portatori d'interesse, soprattutto alla luce delle nuove sfide dovute all'utilizzo delle tecnologie dell'informazione e della comunicazione nel settore sanitario.

Ai sensi dell'articolo 2, comma 1, l'ambito di applicazione della proposta di regolamento riguarda anche «il trattamento dei dati personali interamente o parzialmente automatizzato e non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi». L'apertura al digitale da parte del legislatore europeo richiede, però, da parte del Servizio Sanitario Nazionale la predisposizione di interventi formativi *ad hoc* (ad esempio sulle regole del trattamento automatizzato dell'informazione), destinati agli operatori socio-sanitari affinché questi acquisiscano idonee conoscenze e competenze per l'esercizio dell'attività professionale.

L'articolo 5, rubricato «Principi applicabili al trattamento dei dati personali», ricorda, tra gli altri, che i dati devono essere trattati in modo trasparente nonché devono essere «adeguati, pertinenti e limitati al minimo necessario rispetto alle finalità perseguite» (c.d. principio della minimizzazione dei dati). Ciò implica che i dati personali non pertinenti o, se sensibili (come nel caso delle informazioni sulla salute), non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione, non dovranno essere intellegibili.

Il principio di trasparenza è altresì richiamato dall'articolo 11 che introduce l'obbligo per i responsabili del trattamento (ovvero «la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità, le condizioni e i mezzi del trattamento di dati personali» – nel caso del settore sanitario un'azienda sanitaria, un policlinico, ecc.) di fornire informazioni trasparenti, comprensibili e facilmente accessibili.

Il combinato disposto degli articoli 14, 4 (comma 1, nn. 7 e 8) e 22 (comma 1) evidenzia invece a carico del responsabile del trattamento l'onere della prova di un'informativa dettagliata sul trattamento dei dati personali, del relativo consenso "esplicito" nonché della conformità del trattamento dei dati al regolamento.

Come di recente evidenziato dall'Autorità Garante per la protezione dei dati personali [10,11], la diffusione di nuovi strumenti tecnologici per i processi diagnostico-terapeutici, quali le applicazioni mediche mobili, riapre alcuni dei temi summenzionati (in particolare la necessità di intervenire sul consenso esplicito previo) e richiede, pertanto, provvedimenti mirati sia da parte degli sviluppatori dei *software* sia da parte degli organismi di vigilanza al fine di prevenire possibili violazioni della *privacy*.

Il tratto innovativo apportato dalle nuove tecnologie investe anche «procedure e meccanismi per l'esercizio dei diritti dell'interessato»: l'articolo 12, infatti, sancisce che qualora i dati siano trattati con modalità automatizzate, «il responsabile del trattamento predispone i mezzi per inoltrare le richieste per via elettronica».

Il medesimo canale telematico verrà utilizzato per garantire il diritto di accesso dell'interessato: in questo senso si esprime il comma 2 dell'articolo 15, secondo cui «Se l'interessato presenta la richiesta in forma elettronica, le informazioni sono fornite in formato elettronico, salvo indicazione diversa dell'interessato».

L'articolo 17 della proposta di regolamento in esame disciplina il c.d. diritto all'oblio e alla cancellazione, prevedendo l'obbligo a carico del responsabile del trattamento che abbia divulgato dati personali «di informare i terzi della richiesta dell'interessato di cancellare tutti i link verso tali dati, le loro copie o riproduzioni». La norma riconosce, pertanto, «il diritto a che nessuno riproponga nel presente un episodio che riguarda la nostra vita passata e che ciascuno di noi vorrebbe, per le ragioni più diverse, rimanesse semplicemente affidato alla storia» [12].

Altro diritto conseguente all'avvento del digitale è quello alla portabilità dei dati (articolo 18), ovvero al trasferimento dei dati personali da un sistema di trattamento elettronico a un altro, senza che il responsabile del trattamento possa impedirlo. Come presupposto, e al fine di migliorare l'accesso dell'interessato ai dati personali che

lo riguardano, è previsto il diritto di ottenere tali dati dal responsabile del trattamento in un formato elettronico strutturato e di uso comune.

L'articolo 18 appena invocato assume un'attualità rilevante soprattutto a fronte di quella mobilità transfrontaliera summenzionata: a titolo esemplificativo, il paziente in cura in Italia che desideri trasferirsi in un altro paese dell'Unione per proseguire il piano terapeutico è legittimato a richiedere la portabilità dei propri dati; lo stesso dicasi se desideri spostarsi da una regione italiana all'altra. Tuttavia, affinché la fruibilità e l'utilizzo dell'informazione sanitaria siano realmente possibili è indispensabile che il sistema sanitario nazionale continui ad operare sulle modalità con cui i dati vengono forniti all'utente (c.d. formati dei dati). In questo senso importanti contributi tecnologici sono stati raggiunti con l'attuazione dei principi degli *Open Data* e dei *Linked Open Data*.

Il soggetto tenuto a garantire l'osservanza del regolamento è il responsabile del trattamento: ai sensi del comma 1, dell'articolo 22, egli è gravato dell'onere «di dimostrare che il trattamento dei dati personali effettuato è conforme al […] regolamento». In particolare, egli è tenuto a predisporre in modo efficace le seguenti misure:

- conservazione della documentazione;
- attuazione dei requisiti di sicurezza;
- esecuzione della valutazione d'impatto sulla protezione dei dati;
- autorizzazione preventiva o di consultazione preventiva dell'autorità di controllo;
- designazione di un responsabile della protezione dei dati.

Altra importante novità introdotta dalla proposta di regolamento, sollecitata peraltro dalla diffusione delle nuove tecnologie, è la «protezione fin dalla progettazione e protezione di default» (c.d. *Privacy by Design* e *Privacy by Default*). Nel rispetto dell'articolo 23 i sistemi informativi sanitari dovranno rispettare le misure di sicurezza previste dalla normativa e, in particolare, lo strumento informatico dovrà essere progettato in modo tale da contenere e prevenire gli abusi di dati personali e sensibili dei pazienti, attraverso opportune limitazioni d'uso e trattamento. In questo senso, l'utente (e con esso la riservatezza e la protezione dei dati) saranno sempre più posti al centro del sistema informatico.

La norma segue il principio di neutralità tecnologica (di cui al considerando 66 richiamato) dal momento che lascia un'ampia libertà agli sviluppatori circa le modalità operative per raggiungere l'auspicato risultato. Tuttavia, come osservato da alcuni [13], non sarebbe stato secondario fornire delle indicazioni metodologiche comuni per operare sul *design* dei sistemi informativi.

Il capo IV, sezione 2, della proposta di regolamento disciplina la «sicurezza dei dati», introducendo l'obbligo di notificazione e comunicazione delle violazioni di dati personali a carico del responsabile del trattamento (articoli 31 e 32), con una eccezione: «Non è richiesta la comunicazione di una violazione dei dati personali all'interessato se il responsabile del trattamento dimostra in modo convincente all'autorità di controllo che ha utilizzato le opportune misure tecnologiche di protezione e che tali misure erano state applicate ai dati violati. Tali misure tecnologiche di protezione devono rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi» (articolo 32, comma 3).

La «valutazione d'impatto sulla protezione dei dati» (c.d. *Privacy Impact Assessment*) (articolo 33) e la «autorizzazione preventiva e consultazione preventiva» (articolo 34) sono introdotte nella sezione 3 del capo IV. In particolare sono previsti:

- l'obbligo per responsabili e incaricati del trattamento di effettuare una valutazione d'impatto in materia di protezione dei dati prima di trattamenti che presentino rischi al riguardo;
- il controllo preliminare nei casi in cui il responsabile del trattamento o l'incaricato del trattamento devono ottenere l'autorizzazione preventiva dell'autorità di controllo o consultare tale autorità prima di trattare i dati.

L'articolo 35 introduce una nuova figura, il «responsabile della protezione dei dati» (o *Data Protection Officer*), obbligatoria per il settore pubblico e per il settore privato (in particolare per le grandi imprese o quando le attività principali del responsabile del trattamento e dell'incaricato del trattamento consistono in trattamenti che richiedono il controllo regolare e sistematico degli interessati).

I compiti del responsabile della protezione dei dati sono disciplinati dall'articolo 37 e, in generale, qualificabili come attività di:

- sorveglianza e controllo sull'attuazione ed applicazione del regolamento;
- coordinamento delle politiche aziendali di protezione dei dati personali;
- conservazione della documentazione relativa alla protezione dei dati personali e notifica di eventuali violazioni;
- gestione dei rapporti con il titolare e il responsabile del trattamento;
- cooperazione con l'Autorità Garante per la protezione dei dati personali.

A questo proposito, soprattutto in riferimento al Servizio Sanitario Nazionale, si ricorda che la figura del «responsabile della protezione dei dati» è stata di fatto introdotta il 22 maggio 2014 dall'Autorità Garante per la protezione dei dati personali, chiamata ad esprimere un parere su uno schema di decreto del Presidente del Consiglio dei ministri in materia di fascicolo sanitario elettronico (FSE). Di seguito le parole del Garante: «[…] Nel tavolo di lavoro si è fatto riferimento

alla figura del "responsabile della protezione dei dati". Al riguardo, pur condividendo la scelta di non inserire nel regolamento una disposizione che obblighi i titolari del trattamento ad istituire tale figura, l'Autorità, in ragione della particolare delicatezza delle informazioni trattate nell'ambito del FSE utilizzate per le molteplici finalità previste dalla legge, auspica che ogni titolare coinvolto dall'applicazione del presente decreto individui al suo interno una figura di responsabile della protezione dei dati che interloquisca con il Garante, anche in relazione ai casi di data breach previsti nell'articolo 24, comma 9 dello schema» [14].

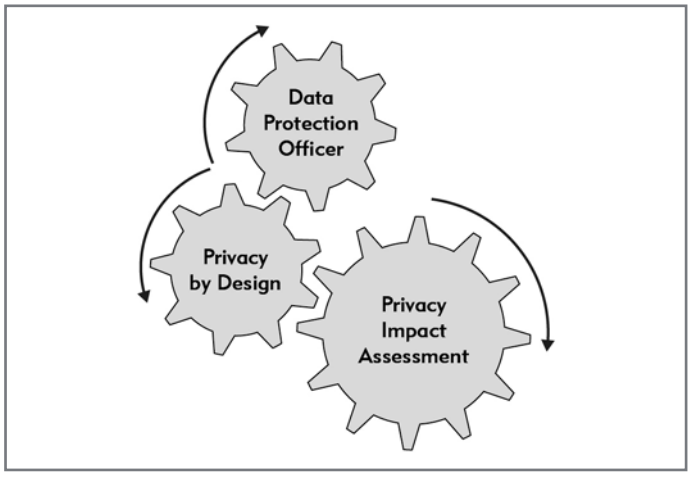

Figura 1. Pilastri per le policy aziendali

CONCLUSIONI

Al termine dell'analisi del regolamento generale sulla protezione dei dati personali è possibile notare un'assoluta continuità rispetto alla direttiva 95/46/EC soprattutto per ciò che concerne i principi generali. Eccezioni sono la minimizzazione dell'utilizzo dati e la *Privacy by Design*.

Gli ambiti di effettiva innovazione possono essere così sintetizzati:

- attenzione ai profili pratici della protezione dei dati personali (ad esempio per ciò che concerne l'implementazione dei principi e l'applicazione dei diritti e degli obblighi);
- definizione di un processo di semplificazione e riduzione dei costi (tra gli altri, si ricorda l'eliminazione dell'obbligo generale di notificazione all'autorità di controllo prima di procedere al trattamento e l'introduzione dell'obbligo di notificare eventuali violazioni).

Le strutture sanitarie nazionali, soggetti titolari del trattamento dei dati personali, sono altamente complesse; per tale ragione esse necessitano nuove *policy* aziendali che recepiscano i tre elementi cardine della proposta di regolamento: la *Privacy by Design*, il *Data Protection Officer*, il *Privacy Impact Assessment* (Figura 1).

Parimenti si auspica l'approvazione in tempi brevi del testo definitivo del regolamento generale sulla protezione dei dati personali la cui attuazione richiederà un ulteriore periodo di due anni. Tale osservazione è perlopiù conseguenza del fatto della costante evoluzione tecnologica, la cui rapida crescita potrebbe paradossalmente svuotare l'originalità di alcuni principi innovativi (come il diritto all'oblio) nel tempo consolidatisi tra i ventotto Paesi dell'Unione europea.

BIBLIOGRAFIA

1. Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Gazzetta ufficiale delle Comunità europee L 281 del 23 novembre 1995
2. Report from the Commission - First Report on the implementation of the Data Protection Directive (95/46/EC). COM/2003/0265 final, 15.03.2003
3. Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, 2007/C 255/01. Gazzetta ufficiale dell'Unione europea C 255 del 27 ottobre 2007
4. European Commission. Special Eurobarometer 359. Attitudes on data protection and electronic identity in the European Union. Brussels: TNS Opinion & Social, 2011
5. Communication from The Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union. COM(2010) 609 final. Brussels, 4.11.2010
6. Trattato sul funzionamento dell'Unione Europea (versione consolidata). Gazzetta Ufficiale dell'Unione Europea C 326/47 del 26 ottobre 2012
7. Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati). COM(2012) 11 final. Bruxelles, 25.1.2012

8. Pollicino O. Regolamento Europeo sulla Privacy, ancora in discussione. Diritto 24, Il sole 24 ore, 12.12.2014
9. Direttiva 2011/24/UE del Parlamento europeo e del Consiglio del 9 marzo 2011 concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera. Gazzetta ufficiale dell'Unione europea L 88/45 del 4 aprile 2011
10. Garante per la protezione dei dati personali. App mediche: Garante privacy, serve più trasparenza nell'uso dei dati. Doc-Web: 3374496, 10.9.2014
11. Garante per la protezione dei dati personali. Global Privacy sweep 2014. I risultati dell'indagine svolta da 26 autorità per la privacy di tutto il mondo. Doc-Web: 3374906, 10.9.2014
12. Barca F. Diritto all'oblio e diritto alla storia. Intervista a Guido Scorza. Una Città, 2012
13. Fabiano N. Privacy by Design: l'approccio corretto alla protezione dei dati personali. Diritto 24, Il sole 24 ore, 20.04.2015
14. Parere del Garante su uno schema di decreto del Presidente del Consiglio dei ministri in materia di fascicolo sanitario elettronico - 22 maggio 2014. Registro dei provvedimenti n. 261 del 22 maggio 2014. Doc-Web: 3230826, 22.5.14