DIRITTO D'IMPRESA, Privacy

GDPR, quanti pasticci nella legge europea 2017: ecco cosa rischia l'Italia

di **Andrea Lisi**

L'Italia avanza lentamente e in modo scoordinato nell'armonizzazione della disciplina nazionale con il GDPR. Ancora poca chiarezza sul Responsabile del trattamento e troppo generiche le norme sul riutilizzo dei dati sanitari, in forma anonima, per scopi statistici e di ricerca. Futuro inquietante all'orizzonte

Mentre altri Stati Europei hanno provveduto da tempo ad armonizzare la propria disciplina nazionale con l'arrivo piuttosto impetuoso del GDPR[1], l'Italia timidamente muove i suoi primi passi verso tale obiettivo in modo a prima vista poco coordinato e convincente.

Si fa riferimento ovviamente alle novità in materia di protezione dei dati personali (e quindi modificative di alcuni articoli del Codice[2]) appena introdotte dalla legge 20 novembre 2017, n. 167 (in vigore dal 12 dicembre p.v.)[3]. Tali novità giungono piuttosto inaspettate perché un'altra normativa (legge 25 ottobre 2017, n. 163[4]) solo pochi giorni prima aveva delegato il Governo ad armonizzare il Codice per la protezione dei dati personali proprio con il GDPR, dando però 6 mesi di tempo per effettuare tali modifiche!

Sinceramente, leggendo i contenuti delle modifiche appena introdotte, non si riescono a comprendere le ragioni di tale urgenza e si avverte la spiacevole sensazione che il legislatore italiano si muova con una mano senza sapere cosa faccia l'altra. E del resto a volte – anzi troppo spesso – la fretta è cattiva consigliera,soprattutto quando si deve intervenire su materie delicate regolamentate in un apparato normativo sistematico (quale il Codice è) e occorrerebbe procedere invece con la pazienza, la consapevolezza e la lucidità dei chirurghi quando utilizzano il loro bisturi per intervenire in un'operazione a cuore aperto…tutte caratteristiche che, purtroppo, sembrano recentemente mancare al nostro legislatore!

In ogni caso, la novità a mio avviso più rilevante, nell'ottica di armonizzazione con le disposizioni del "Regolamento privacy" europeo, va ad impattare sulla nomina a Responsabile del trattamento dei dati ex art. 29 del Codice[5]. Come ho avuto modo recentemente di spiegare, tale figura da tempo presente nell'ordinamento italiano differisce sostanzialmente dal Responsabile del trattamento previsto in modo piuttosto dettagliato nell'art. 28 del GDPR [6].

Nell'attuale formulazione del Codice in materia di protezione dei dati personali, infatti, il Responsabile del trattamento dei dati personali non agisce solo per conto del Titolare, ma è da

questi preposto al trattamento, acquisendo quindi la facoltà di sostituirlo nelle scelte, sia all'interno e sia all'esterno dell'organizzazione di riferimento. Del resto, lo stesso Codice precisa che tale figura debba essere individuata tra soggetti che per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Quindi la figura italiana del Responsabile del trattamento dei dati in molte delle sue estrinsecazioni pratiche in tante aziende o PA italiane si è avvicinata di molto a quanto il Regolamento prevede oggi per la diversa (e delicata) figura del DPO (Data Protection Officer o Responsabile della protezione dei dati personali).

E in ogni caso la figura italiana del Responsabile del trattamento dei dati personali è una figura facoltativa che il Titolare del trattamento può decidere di nominare internamente alla sua struttura per motivi organizzativi e di opportunità. Allo stesso modo tale figura, come delineata nel Codice, nella sua genericità e astrattezza, è stata utile anche ai fini della regolamentazione dei rapporti giuridici tra titolari e fornitori esterni (nominati quindi responsabili esterni del trattamento dei dati).

Come già accennato, invece, l'art. 28 del GDPR disciplina con maggiore puntualità il ruolo e le attribuzioni del Responsabile del trattamento dei dati rispetto a quanto attualmente contemplato nel D.Lgs. 196/2003 e tale figura, per i compiti a essa attribuiti e nella descrizione delle sue funzioni, può essere ricondotto – a mio avviso – alla sola figura giuridica del Responsabile esterno del trattamento. Alla luce di ciò, e in attesa del completo coordinamento normativo tra Codice e GDPR, considerata l'attuale non incompatibilità formale tra la figura del Responsabile interno come disciplinata in Italia e quella del Responsabile (esterno) del trattamento prevista in Europa, non si poteva escludere che questa facoltà di nomina in capo al Titolare prevista nel Codice potesse permanere nella nostra disciplina nazionale. Le modifiche caoticamente appena introdotte sembrano andare proprio in questa direzione, anche se il coordinamento tra Codice e GDPR resta a mio avviso insufficiente sotto questo specifico punto di vista.

In ogni caso la Legge 167/2017, con il suo art. 28, ha modificato l'art. 29 del Codice, introducendo un nuovo comma (il comma 4 bis) e sostituendo il comma 5 dello stesso articolo. Il nuovo art. 29 del Codice, quindi, avrà questa nuova formulazione:

"Art. 29. Responsabile del trattamento

Il responsabile è designato dal titolare facoltativamente.

Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

4-bis. Fermo restando quanto previsto ai commi 1, 2, 3 e 4, il titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 2. I titolari stipulano con i predetti responsabili atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento; i predetti atti sono adottati in conformità a schemi tipo predisposti dal Garante.

Il responsabile effettua il trattamento attenendosi alle condizioni stabilite ai sensi del comma 4-bis e alle istruzioni impartite dal titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2, delle proprie istruzioni e di quanto stabilito negli atti di cui al comma 4-bis."

Il tentativo legislativo di coordinare tra Codice e GDPR la figura interna ed esterna di Responsabile del trattamento mi sembra evidente, ma il risultato lascia forse un po' a desiderare dal punto di vista della chiarezza e della sintesi.

Accanto a questa importante novità, degne di nota sono le previsioni presenti nello stesso art. 28 in materia di protezione dei dati e ricerca[7].

In particolare, viene prevista la possibilità, per scopi statistici e di ricerca scientifica, di riutilizzo dei dati personali, anche sensibili, (ad esclusione di quelli genetici), a condizione che siano adottate forme preventive di minimizzazione e di anonimizzazione dei dati ritenute idonee a tutela degli interessati, previa autorizzazione del Garante. Sinceramente la genericità di questa disposizione lascia sconcertati poiché gli scenari che essa sembra prefigurare appaiono piuttosto inquietanti. Vogliamo davvero consentire massicci riusi di dati anche sanitari senza consenso? È questo il futuro che vogliamo consegnare a briglie sostanzialmente sciolte ai giganti del mondo digitale? E siamo sicuri che tutto questo sia in linea con lo spirito del GDPR che dovremmo attuare?

Infine, sempre in ambito di protezione dei dati, vanno ricordate le norme sul potenziamento delle risorse dell'Autorità Garante (art. 29) e la preoccupante estensione a 72 mesi dei termini di conservazione dei dati di traffico telefonico e telematico (art. 24).

Mi sia consentito, infine, di considerare ormai esilarante la solita clausola di invarianza finanziaria[8] ai fini dell'attuazione di queste disposizioni inserita ormai abitualmente come postilla e sigillo finali a coronamento della poca, reale attitudine che il nostro legislatore ha nell'affrontare materie così complesse.

[1]General Data ProtectionRegulation (Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la

direttiva 95/46/CE).

[2] Codice in materia di protezione dei dati personali (contenuto come è ben noto nel Decreto legislativo 30 giugno 2003, n. 196).

[3]Legge 20 novembre 2017, n. 167, Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2017. (17G00180) (GU Serie Generale n.277 del 27-11-2017)

[4] Legge di delegazione europea 2016-2017, approvata in via definitiva il 18.10.2017, «Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea» – Legge di delegazione europea 2016-2017 (GU n.259 del 6-11-2017):

Art. 13 – Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

Il Governo è delegato ad adottare, entro sei mesi dalla data di entrata in vigore della presente legge, con le procedure di cui all'articolo 31 della legge 24 dicembre 2012, n. 234, acquisiti i pareri delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

I decreti legislativi di cui al comma 1 sono adottati su proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia, di concerto con i Ministri degli affari esteri e della cooperazione internazionale, dell'economia e delle finanze, dello sviluppo economico e per la semplificazione e la pubblica amministrazione.

[5] Secondo l'attuale art. 29 del Codice:

1. Il responsabile è designato dal titolare facoltativamente.

Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

[6] Articolo 28 – Responsabile del trattamento

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

1. a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico
2. b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza
3. c) adotti tutte le misure richieste ai sensi dell'articolo 32;
4. d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
5. e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
6. f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

7. g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
8. h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.

La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.

Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.

Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

[7] Al capo III del titolo VII della parte II, dopo l'articolo 110 è aggiunto il seguente:

«Art. 110-bis. (Riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici). – 1. Nell'ambito delle finalità di ricerca scientifica ovvero per scopi statistici può essere autorizzato dal Garante il riutilizzo dei dati, anche sensibili, ad esclusione di quelli genetici, a condizione che siano adottate forme preventive di minimizzazione e di anonimizzazione dei dati ritenute idonee a tutela degli interessati.

Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del riutilizzo dei dati, anche sotto il profilo della loro sicurezza».

[8] Art. 30 Clausola di invarianza finanziaria

Dall'attuazione delle disposizioni di cui alla presente legge, con esclusione degli articoli 6, 7, 8, 10, 11 e 29, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni interessate provvedono agli adempimenti previsti dalla medesima legge con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.