Le Nuove Responsabilità del Titolare del Trattamento Dati

Date : 9 maggio 2017

L’entrata in vigore del Regolamento Europeo sul trattamento dei dati personali, prevista per il prossimo 25 maggio 2018, segnerà un passaggio importante nella gestione della privacy. Si passerà, infatti, da un approccio formale ad uno più sostanziale finalizzato a tutelare in modo organizzato e consapevole i dati personali.

La nuova normativa, al contrario di quanto disposto dal codice della privacy che prevede adempimenti formali e burocratici (informativa, consenso, notificazione al Garante, misure di sicurezza minime ed idonee), introduce nuove misure volte a promuovere la protezione dei dati personali fin dalla progettazione delle operazioni di trattamento.

Le nozioni di Privacy by design, Privacy by default, l'accountability impongono al Titolare del trattamento di trattare i dati personali sulla base di:

- una valutazione della probabilità e della gravità del rischio legato al trattamento dei dati (PIA);
- l’implementazione di misure di sicurezza adeguate per limitare i rischi;
- un modello organizzativo che garantisca la compliance al regolamento.

Il Titolare, prima di iniziare a trattare i dati personali, deve avere chiare: le finalità e le modalità del trattamento, nonché i soggetti interni ed esterni alla propria organizzazione che, di fatto, tratteranno i dati personali. Solo in questo modo il titolare del trattamento potrà misurare la propria responsabilità ed assumersi eventuali conseguenze negative.

Il trattamento dei dati, quindi, al fine di limitare il più possibile i rischi di perdita di integrità dei dati ed i rischi per i diritti e le libertà delle persone fisiche, dovrà essere esercitato con un nuovo approccio culturale tale da valutare ed organizzare in modo concreto e non formale le operazioni sui dati personali.

L’innovativo principio dell’ accountability introdotto dal Regolamento e comunemente tradotto, a mio parere, in maniera troppo riduttiva, come “responsabilizzazione” deve essere applicato oltre che ai temi della privacy, anche ai temi giuridici legati alla digitalizzazione dei processi aziendali, come ad esempio, alla formazione e conservazione del documento informatico.

Dal punto di vista della responsabilità civile, trattare i dati personali, con questo approccio vorrà dire anche documentare e quindi dimostrare in quale modo il trattamento dei dati è stato progettato e quale modello organizzativo è stato adottato, perciò, diventerà importante elaborare codici di condotta, ottenere certificazioni, sigilli o marchi di protezione dei dati per prodotti e/o servizi.

In un momento storico caratterizzato dall'utilizzo di tecnologia sempre più avanzata, definire questi aspetti, diventa ancora più importante, se si considera che l'utilizzo degli strumenti informatici e telematici utilizzati per trattare i dati personali accresce in modo esponenziale i rischi di perdita di integrità e, soprattutto, modifica le modalità di formazione della prova delle misure organizzative e di sicurezza adottate, nonché degli eventi legati al trattamento dei dati.

La raccolta on line dei dati personali, soprattutto nelle attività di e-commerce, per il tramite di form on line, comporta l'implementazione di procedure informatiche finalizzate a registrare e documentare in modo certo e sicuro la formazione della banca dati e, quando previsto, la manifestazione del consenso al trattamento espresso dall'interessato.

Tali procedure informatiche, nei casi di trattamento basato sul consenso dell'interessato, dovranno garantire al titolare di poter provare, oltre che la conformità alla normativa, anche che l'interessato abbia realmente espresso il proprio consenso; quindi, si dovrà fare una valutazione sulle modalità di raccolta e archiviazione dei dati ed, in particolare, sulle caratteristiche di autenticità, paternità ed integrità dei singoli record formati al momento della registrazione del dato personale e degli eventi ad esso legati (ad esempio consenso privacy).

Rispettare i principi e gli adempimenti prescritti dal Regolamento ed essere, quindi, conformi alla normativa non riduce, o esclude la responsabilità del titolare, o del responsabile rispetto ai danni subiti dall'interessato. Infatti, l'adozione delle predette misure organizzative esclude l'applicazione delle onerose sanzioni, previste sia dall'attuale, che dalla futura normativa, ma non rende immuni dalla responsabilità per i danni provocati all'interessato.

Trattare i dati personali in maniera consapevole ed organizzata permette al titolare di ridurre e misurare i rischi che incombono sui dati personali, in modo tale da valutare i possibili effetti di un trattamento illegittimo e nel caso, soprattutto con riferimento all'utilizzo degli strumenti informatici che per definizione non permettono di azzerare i rischi, sottoscrivere specifiche polizze assicurative a garanzia di eventuali richieste di risarcimento danni.

Dal punto di vista del risarcimento del danno, inoltre, il nuovo Regolamento conferma quanto stabilito dal Codice della privacy, ovvero, il trattamento dei dati personali è un' attività pericolosa disciplinata dall'art.2050 del codice civile, con il conseguente obbligo di risarcire i danni, patrimoniali e non patrimoniali, provocati all'interessato in conseguenza del trattamento stesso.

In tale fattispecie il codice civile prevede una presunzione di responsabilità extracontrattuale che può essere superata solo dalla produzione in giudizio di una prova particolarmente rigorosa. Infatti, in sede giudiziaria, il titolare o il responsabile si troverebbero in una posizione "svantaggiata" rispetto all'interessato, in quanto quest'ultimo dovrà provare solo il legame tra il

trattamento dei dati ed il danno subito, mentre il titolare o il responsabile del trattamento dovranno dimostrare di aver adottato misure organizzative e di sicurezza efficaci ed adeguate per prevenire il danno contestato.

I soggetti eventualmente responsabili dei danni sono individuati dal Regolamento all'articolo 82 e sono, per motivi diversi, il Titolare ed il Responsabile del trattamento. Differentemente da quanto previsto dall'attuale Codice della privacy che riconduce la responsabilità civile a "Chiunque" tratti i dati personali, il Regolamento restringe il campo a soggetti ben determinati.

Il titolare ed il responsabile rispondono per il danno cagionato all'interessato nel caso in cui il trattamento violi quanto disposto dal Regolamento. Inoltre, il responsabile del trattamento ne risponderà nel caso in cui agisca in modo difforme, o contrario rispetto alle legittime istruzioni del titolare.

Quanto previsto dall'articolo 82 pone in evidenza l'importanza, per il titolare, di valutare le caratteristiche organizzative e le competenze del soggetto che verrà nominato responsabile del trattamento e per quest'ultimo, valutare attentamente il contenuto della nomina.

Infatti, l'oggetto della nomina a responsabile del trattamento, che ha una natura contrattuale, è la designazione da parte del Titolare di un soggetto che verrà delegato a trattare dati personali. Nella nomina dovranno essere individuati i seguenti aspetti: le categorie di dati personali, i trattamenti delegati, le finalità ed i mezzi del trattamento, le misure di sicurezza adottate, precise istruzioni su come adempiere all'incarico ricevuto e la sua durata.

Nel caso della esternalizzazione del trattamento e, quindi, dell'affidamento a terzi di pezzi "dell'organizzazione privacy" del titolare e dei dati da quest'ultimo raccolti e di cui è responsabile, è fondamentale stipulare un contratto di servizi in cui siano ben definite le modalità, le finalità del trattamento dei dati, gli obblighi e responsabilità.

La ripartizione della responsabilità civile e dell'onere della prova, nel rapporto tra titolare e responsabile si basa sul contenuto della nomina e/o del contratto di servizi; l'individuazione del responsabile della privacy, quindi, non deve essere visto come un mero adempimento formale, bensì come un punto strategico per attuare le procedure di trattamento dei dati personali definite in sede di progettazione (privacy by design).

La necessità di un contratto di servizi, oltre ad essere necessario per definire le responsabilità dei soggetti delegati al trattamento dei dati personali, è prevista dallo stesso Regolamento che all'articolo 28 dispone che il trattamento dei dati, affidato ad un responsabile, sia disciplinato da un contratto, o da altro atto giuridico.

Quest'obbligo è ribadito anche in caso di esternalizzazione della conservazione dei documenti informatici e, quindi, dei dati personali. Infatti, le regole tecniche (Decreto del Presidente del Consiglio dei Ministri 3 Dicembre 2013) sui sistemi di conservazione dei documenti informatici, dispongono che il processo di conservazione possa essere affidato ad un soggetto esterno mediante un contratto di servizio che preveda gli obblighi e le responsabilità e che quest'ultimo dovrà assumere il ruolo di responsabile del trattamento.

Per quanto riguarda la tipologia di danno risarcibile, il regolamento ricalca quanto previsto dal Codice della privacy e riconosce il risarcimento sia del danno patrimoniale, che di quello non patrimoniale.

Con riferimento alla quantificazione del danno non patrimoniale, le recenti sentenze della Cassazione attenuano le conseguenze per chi tratta i dati personali, nel senso che il risarcimento del danno non patrimoniale è dovuto solo nel caso in cui sia superato il livello di tollerabilità ed il pregiudizio non sia futile.

Le recenti decisioni della Cassazione (Cassazione civile, sez. I, 23/05/2016, n. 10638 Cassazione civile, sez. III, 13/10/2016, n. 20615, Cassazione civile sez. VI 11 gennaio 2016 n. 222, Cassazione Civile, sez. III, sentenza 15/07/2014 n° 16133) nello specificare che il danno patrimoniale derivante dal trattamento dei dati personali non si sottrae alla verifica della gravità della lesione e non può mai ritenersi in re ipsa, ma va debitamente allegato e provato da chi lo invoca, riducono le cause delle c.d. liti "bagatellari".

L’accertamento del danno, quindi, sarà di fatto rimesso al giudice del merito che dovrà quantificare il danno non solo sulla base delle prove prodotte, ma anche sulla base del contesto temporale e sociale in cui si è verificato il danno stesso.

Pertanto, nella valutazione iniziale del modello organizzativo privacy, le dinamiche processuali e gli orientamenti giurisprudenziali, diventeranno elemento determinante per valutare la probabilità e la gravità del rischio legato al trattamento del dato personale, nonché della responsabilità civile e del conseguente impatto economico legato alla quantificazione del danno patrimoniale e non patrimoniale lamentato dall'interessato e delle sanzioni amministrative inflitte dall'Autorità di controllo.

A cura di: **Andrea Battistella**