CONFINDUSTRIA

Osservazioni al progetto di Relazione del Parlamento Europeo sulla proposta di Regolamento in materia di protezione dei dati personali

Premessa

Il 25 gennaio 2012, la Commissione UE ha presentato una proposta di Regolamento sulla tutela e la libera circolazione dei dati personali delle persone fisiche, volto a sostituire la Direttiva 95/46/CE. L'iniziativa fa seguito a una Conferenza svoltasi nel maggio 2009 e a due consultazioni, avviate rispettivamente a luglio 2009 e a novembre 2010.

Il Regolamento si propone di armonizzare la normativa europea in tema di privacy e di adeguarla allo sviluppo tecnologico, nonché ai servizi della società dell'informazione. Inoltre, il provvedimento mira a semplificare gli adempimenti burocratici a carico dei titolari, per ridurre i costi connessi alla loro esecuzione.

Sul piano generale, l'iniziativa della Commissione è positiva. In primo luogo, si condivide la scelta di procedere con un regolamento che, essendo direttamente applicabile all'interno degli Stati membri, consente di assicurare una maggiore uniformità normativa nell'Ue. In secondo luogo, particolarmente positivo è l'approccio di circoscrivere le tutele e le garanzie in tema di privacy ai dati delle persone fisiche, in linea con quanto già previsto dalla Direttiva n. 46/1996 e dal nostro Codice privacy (D.Lgs n. 196/2003).

Tuttavia, come evidenziato nelle considerazioni che seguono, lo schema di Regolamento presenta alcune criticità, in quanto non affronta in modo deciso il tema della semplificazione di alcuni adempimenti legati al rispetto della disciplina privacy.

Inoltre, il Regolamento non prevede una specifica disciplina per i trattamenti derivanti dall'utilizzo di alcuni strumenti di comunicazione elettronica innovativi (es. *cloud computing*, dispositivi di geolocalizzazione, sistemi di rilevazione dei dati biometrici) che, invece, sarebbe opportuno introdurre.

Con riferimento allo schema di Regolamento, lo scorso 10 gennaio 2013, è stata presentato in Commissione LIBE del Parlamento Europeo (di seguito, anche PE) un progetto di Relazione contenente alcune modifiche al testo della proposta.

Il PE interviene su diversi aspetti dello schema di Regolamento, senza tuttavia correggerne le principali criticità. Infatti, alcune disposizioni della proposta di Regolamento, confermate anche dal PE, risultano poco in linea con l'obiettivo di semplificare gli adempimenti privacy.

Di seguito, alcune osservazioni sugli aspetti più critici del progetto di Relazione parlamentare.

Considerazioni particolari

1. Esclusione delle imprese individuali dall'ambito di applicazione del Regolamento

Il Considerando n. 12 della proposta, confermato anche dal progetto di Relazione del PE, precisa che la tutela offerta dal Regolamento non può essere invocata per il trattamento dei dati delle persone giuridiche, *"in particolare delle imprese dotate di personalità giuridica, compreso il nome, la forma giuridica e i contatti",* anche quando il nome della persona giuridica contiene il nome di una o più persone fisiche.

Con riferimento alle imprese, la norma sembrerebbe far riferimento soltanto a quelle con personalità giuridica e non, più in generale, ai soggetti che esercitano un'attività economica a prescindere dalla forma giuridica rivestita ovvero dal riconoscimento della personalità (art. 4, n. 15 della proposta di Regolamento). Ciò determinerebbe l'effetto di escludere dall'ambito di applicazione della normativa privacy le imprese dotate di personalità giuridica e di ricomprendervi quelle che, invece, ne sono prive (es. imprenditore individuale).

Tale distinzione, basata esclusivamente sulla personalità giuridica del soggetto economico a cui si riferiscono i dati, non sembrerebbe essere giustificata da particolari esigenze di protezione. Infatti, in entrambi i casi, i dati riguarderebbero lo svolgimento di un'attività economica, pertanto, i rischi sottesi alle relative operazioni di trattamento sarebbero sostanzialmente identici.

Peraltro, un simile sistema imporrebbe agli operatori l'onere di differenziare gli adempimenti privacy nei confronti dei propri *partner* commerciali, a seconda che abbiano o meno personalità giuridica, vanificando, di fatto, i vantaggi derivanti dall'esclusione dei primi dall'ambito di operatività del Regolamento.

Pertanto, al fine di semplificare e uniformare gli adempimenti privacy connessi allo svolgimento delle attività economiche, sarebbe necessario estendere l'esclusione dal campo di applicazione del Regolamento al concetto più ampio di impresa e sopprimere dal testo del Considerando n. 12 le parole "*e, in particolare*" e "*dotate di personalità giuridica*".

2. Consenso

Il Considerando n. 25 e l'art. 4, n. 8 della proposta di Regolamento, confermati anche dal progetto di Relazione parlamentare, prevedono che il consenso al trattamento deve essere manifestato in maniera esplicita. Inoltre, il Considerando n. 25 precisa che non costituisce consenso quello manifestato tacitamente ovvero passivamente.

Tali norme, attualmente limitate ai soli trattamenti aventi ad oggetto dati sensibili (art. 8, par. 2, lett. *a)* della Direttiva 45/96), evidenziano un approccio troppo rigido della proposta di Regolamento alle modalità di manifestazione del consenso. Infatti, il riferimento al consenso esplicito rischia di imporre ai titolari l'utilizzo generalizzato del

sistema dell'*opt-in* (consenso esplicito preventivo), a prescindere dal tipo di dati trattati e delle specifiche finalità da perseguire.

Ciò comporterebbe maggiori oneri a carico delle imprese titolari che, per trattamenti poco rischiosi, non potrebbero beneficiare di sistemi più flessibili, come quello dell'*opt-out* ovvero dell'esonero dal consenso. Inoltre, tale approccio risulterebbe poco in linea con le esigenze dell'economia digitale che, per la rapidità della sua evoluzione, necessita di sistemi agevoli e proporzionati agli interessi coinvolti.

Sarebbe opportuno, quindi, eliminare il riferimento al consenso esplicito dal Considerando n. 25 e dall'art. 4, n. 8, al fine di rendere le modalità di autorizzazione al trattamento più flessibili e applicabili nella pratica.

Inoltre, sempre per semplificare gli adempimenti privacy connessi alla manifestazione del consenso e di adeguarli ai rischi connessi alle tipologie di trattamento e alle relative finalità, si potrebbe prevedere:

- l'esonero del consenso per le comunicazioni di dati personali effettuate nell'ambito di gruppi e altre forme organizzate di attività d'impresa (es. RTI, ATI, reti d'impresa), come attualmente previsto dal nostro Codice privacy (v. art. 24, co. 1, lett. i-ter) del D.Lgs n. 196/2003). L'obiettivo è di agevolare la circolazione di informazioni non sensibili, attinenti alla sfera organizzativa o gestionale interna di un gruppo ovvero di altre forme organizzate di attività d'impresa. Ad esempio, la comunicazione senza consenso potrebbe riguardare i dati trattati per la gestione accentrata dei servizi di tesoreria o di amministrazione nei gruppi, per lo svolgimento di piani o progetti formativi per tutti i dipendenti delle società di uno stesso gruppo, nonché quelli trattati per finalità di partecipazione o esecuzione di attività imprenditoriali in forma congiunta (è il caso delle attività svolte da consorzi, reti di imprese, RTI o ATI aggiudicatrici di appalti);
- l'esonero dagli obblighi di informativa e consenso preventivi per il trattamento di dati, comuni e sensibili, contenuti nei *curricula vitae* spontaneamente inviati, in linea con quanto stabilito dal nostro Codice privacy (v. artt. 13, co. 5-*bis*, 24, co. 1, lett. *i-bis)*, 26, co. 3, lett. *b-bis*). Tali adempimenti, infatti, risultano privi di utilità pratica e ingiustificati sul piano giuridico, in quanto il soggetto che riceve un CV "spontaneo" si trova nell'impossibilità di fornire l'informativa preventiva all'interessato e il soggetto che lo invia manifesterebbe un consenso non informato.

Sempre in tema di consenso, il Considerando n. 34 e l'art. 7, par. 4 della proposta di Regolamento, confermati dal progetto di Relazione del PE, prevedono che il consenso dell'interessato non legittima il trattamento quando tra la sua posizione e quella del titolare vi sia un "*notevole squilibrio*". Al riguardo, il Considerando n. 34 precisa che tale squilibrio è ravvisabile quando l'interessato è in posizione di dipendenza rispetto al titolare, come nel caso dei trattamenti effettuati dal datore di lavoro nell'ambito del rapporto lavorativo.

Nonostante quest'ultima specificazione, l'espressione "notevole squilibrio" risulta poco chiara e particolarmente generica. Inoltre, il "notevole squilibrio" sembrerebbe escludere qualsiasi possibilità di trattamento dati, in quanto, in presenza di tale condizione, non rileverebbero neanche le ipotesi di esonero dal consenso per

adempiere a obblighi contrattuali (art. 6, par. 1, lett. b) ovvero a obblighi di legge (art. 6, par. 1, lett. c). Ciò soprattutto alla luce dell'esempio riportato dalla proposta di Regolamento (trattamenti effettuati nell'ambito del rapporto di lavoro).

La norma in esame, quindi, finirebbe per ostacolare l'esecuzione di innumerevoli rapporti contrattuali e, con particolare riferimento all'attività d'impresa, rischierebbe di paralizzarne lo svolgimento. Si pensi, infatti, ai rapporti lavorativi e ai rapporti con i consumatori che, per effetto della nuova previsione, risulterebbero sostanzialmente bloccati.

Inoltre, non è chiara la *ratio* di tale previsione, considerato che, la comune volontà delle parti (e più in generale, l'autonomia privata) dovrebbe comunque apparire sufficiente a giustificare il trattamento, salvo casi patologici di vizi del consenso.

Pertanto, con il Considerando n. 34 e il paragrafo 4 dell'art. 7 andrebbero eliminati.

3. *Direct Marketing*

Il Considerando n. 57 e l'art. 19, par. 2 della proposta di Regolamento estendevano il regime di *opt-out* ai trattamenti effettuati per finalità di *marketing* diretto. Tale principio era da considerarsi limitato al *marketing* mediante posta cartacea e al *marketing door-to-door*, in quanto alle attività promozionali effettuate tramite comunicazione elettronica (es. telefonate con o senza l'intervento di un operatore, *e-mail*, fax) continuavano ad applicarsi le disposizioni della Direttiva *E-privacy* (2002/58/CE), fatte salve dallo stesso Regolamento (Considerando n. 135 e art. 89).

Tuttavia, il progetto di Relazione parlamentare ha eliminato da tali disposizioni il riferimento al *marketing* diretto (Emendamenti nn. 37 e 156), pertanto, secondo la nuova impostazione, ai trattamenti connessi alle attività promozionali realizzate con la posta cartacea ovvero porta a porta deve ritenersi applicabile il più oneroso regime dell'*opt-in*.

Inoltre, al fine di favorire il *direct marketing* in ambito contrattuale, lo schema di Relazione inserisce tra i trattamenti necessari al perseguimento di un interesse legittimo del titolare - realizzabili senza il consenso dell'interessato - quelli connessi alle attività promozionali dirette effettuate per la promozione di beni e servizi "analoghi" a quelli oggetto del contratto (Emendamento n. 101).

Il sistema delineato dalla prima formulazione del Regolamento sembra maggiormente in linea con l'esigenza di ridurre gli oneri privacy a carico delle imprese. Il *direct marketing*, infatti, rappresenta un importante strumento di comunicazione, che consente di promuovere beni e servizi a costi contenuti rispetto a quelli necessari per l'acquisto di spazi pubblicitari su giornali, TV, radio.

La previsione di un sistema di *marketing* diretto, basato sul più agevole regime di *opt-out*, semplificherebbe gli adempimenti privacy connessi all'utilizzo di questo metodo pubblicitario e ridurrebbe i costi a carico delle imprese.

Inoltre, il regime di *opt-out* risulterebbe proporzionato rispetto alle esigenza di tutela dell'interessato, in quanto quest'ultimo deve essere informato sulle caratteristiche del trattamento e, in ogni momento, può opporsi allo svolgimento di *direct marketing* nei suoi confronti.

Pertanto, al fine di ridurre gli oneri derivanti dallo svolgimento di attività di *marketing* diretto, sarebbe opportuno ripristinare l'originaria formulazione del Considerando n. 57 e dell'art. 19, par. 2.

4. Profilazione

Il Considerando n. 58 e l'art. 20 della proposta di Regolamento vietano lo svolgimento di attività di *profiling*, a meno che:

1. non avvenga nel contesto della conclusione ovvero dell'esecuzione di un contratto;
2. non sia espressamente autorizzato da un atto normativo europeo o nazionale;
3. l'interessato abbia manifestato il proprio consenso (*opt-in*).

Sulla prima ipotesi di liceità, è intervenuto il progetto di Relazione parlamentare, che ne ha limitato la portata operativa. Infatti, la nuova norma prevede che, nell'ambito di un rapporto contrattuale, la profilazione è lecita soltanto se è necessaria ai fini della conclusione o esecuzione del contratto (Emendamento n. 160). Pertanto, con riferimento alla profilazione "contrattuale", i margini di intervento del titolare risultano notevolmente ridimensionati.

L'originaria formulazione della norma risultava maggiormente in linea con l'esigenza delle imprese di "monitorare" le preferenze e i comportamenti dei propri clienti. Infatti, la profilazione contrattuale può essere utile non solo ai fini dell'esatta esecuzione del contratto, ma anche per poter fornire al cliente prodotti/servizi corrispondenti ai suoi interessi. Tuttavia, per effetto della modifica, lo svolgimento di attività di *profiling* per queste ultime finalità non sarebbe coperto dalla scriminante in esame, ma richiederebbe il preliminare consenso dell'interessato. Sul piano operativo, l'adempimento di tale obbligo rischia di appesantire lo svolgimento delle ordinarie relazioni commerciali, nonché di compromettere i vantaggi - per imprese e consumatori - connessi al *profiling* contrattuale.

Pertanto, al fine di valorizzare le potenzialità della profilazione in ambito contrattuale, sarebbe opportuno ripristinare la versione orinaria dell'art. 20, par. 2, lett. *a)* della proposta di Regolamento.

Su un piano più generale, l'ipostazione seguita sia dalla proposta di Regolamento, sia dal progetto di Relazione, di prevedere l'*opt-in* per tutte le attività di *profiling* desta qualche perplessità Sarebbe auspicabile, infatti, differenziare il regime privacy applicabile in base ai rischi sottesi alle diverse operazioni di trattamento (es. natura dei dati, finalità). Infatti, non tutte le attività di profilazione presentano le stesse caratteristiche e gli stessi rischi, per cui, rispetto a quelle meno delicate sarebbe opportuno prevedere un regime privacy meno rigido (*opt-out*) e più equilibrato rispetto agli interessi del titolare e a quelli dell'interessato.

Ad esempio, soprattutto per le imprese che offrono beni e servizi sul *web* o tramite posta, la profilazione costituisce un importante strumento per fornire ai consumatori risposte in linea con le loro esigenze. Infatti, l'analisi delle scelte commerciali ovvero degli interessi di un soggetto consentono di modulare l'offerta in base alle sue preferenze.

In questi casi, il *profiling* si traduce in un beneficio per l'impresa, che potrebbe inviare informazioni commerciali "mirate", ma anche per il consumatore, che potrebbe ricevere informazioni necessarie a soddisfare i propri bisogni/gusti. Con riferimento a tale tipologia di profilazione, quindi, i rischi per il consumatore/interessato risultano attenuati, in quanto bilanciati dai vantaggi che lo stesso potrebbe conseguire. Pertanto, sul piano delle tutele, un sistema basato sull'*opt-out* risulterebbe più proporzionato e maggiormente in linea con l'esigenza di fornire all'interessato idonee garanzie di riservatezza (rimangono salvi l'obbligo di informativa e il diritto di opposizione) e semplificare gli adempimenti privacy a carico delle imprese.

5. Comunicazioni all'interessato

L'art. 13 della proposta di Regolamento, nella versione modificata dal progetto di Relazione (Emendamento n. 124), pone a carico del titolare l'obbligo di informare l'interessato dei soggetti cui ha comunicato la rettifica ovvero la cancellazione dei suoi dati.

Tale misura non è condivisibile, in quanto introdurrebbe a carico del titolare un onere superfluo e privo di utilità in termini di tutela dei dati. Infatti, il nuovo adempimento andrebbe ad aggiungersi all'obbligo generale del titolare di indicare nell'informativa privacy i destinatari dei dati personali (art. 14, par. 1, lett. f) e a quello di informare l'interessato, nel caso in cui questi ne faccia richiesta, dei soggetti terzi ai quali siano stati trasmessi i suoi dati personali (art. 15, par. 1, lett. c).

L'interesse dell'interessato di sapere a chi il titolare ha comunicato la rettifica ovvero la cancellazione dei propri dati personali è già ampiamente tutelato nell'ambito del Regolamento. Pertanto, la previsione di un ulteriore obbligo in tal senso risulterebbe eccessiva e, peraltro, onerosa per le imprese titolari.

Sarebbe quindi opportuno eliminare il secondo periodo dell'art. 13 della proposta di Regolamento.

6. Verifica dell'efficacia delle misure

L'art. 22, co. 3 della proposta di Regolamento prevede che il titolare del trattamento verifichi, attraverso revisori interni o esterni, l'efficacia delle misure adottate per garantire la liceità dei trattamenti a esso imputabili, nonché la loro conformità al Regolamento.

Tale previsione è confermata anche dal progetto di Relazione (Emendamento n. 173), che specifica che le attività di *audit* devono essere svolte da soggetti indipendenti.

La norma non è condivisibile, in quanto rischia di introdurre un inutile e gravoso onere amministrativo a carico del titolare del trattamento che, nel verificare l'adeguatezza delle misure adottate al fine di rispettare gli obblighi generali, dovrebbe necessariamente avvalersi di soggetti indipendenti.

La definizione dei meccanismi di *audit*, invece, dovrebbe essere rimesse ala libera scelta del titolare, sul quale ricade l'obbligo di dimostrare l'efficacia delle misure di scurezza adottate (ciò avviene anche attualmente rispetto agli adempimenti imposti

dalle norme nazionali), nonché le conseguenti responsabilità in caso di violazioni o inadempimenti.

Peraltro, il regime di responsabilità previsto dallo schema di Regolamento considera l'attività di trattamento dei dati come rischiosa, ponendo a carico del titolare l'onere di provare di aver adottato tutte le misure necessarie ad evitare il danno e di dimostrare che l'evento dannoso non era a lui imputabile (art. 77).

Sulla base di tali considerazioni, il paragrafo 3 dell'art. 22 andrebbe eliminato e il successivo paragrafo 4 coordinato, stralciando i riferimenti alle verifiche di efficacia.

7. Obbligo di documentazione

L'art. 28 della proposta di Regolamento, confermato dal progetto di Relazione del PE, pone a carico del titolare e di coloro che trattano i dati nel suo interesse l'obbligo di conservare la documentazione di tutti i trattamenti effettuati. In particolare, tale documentazione deve contenere le stesse informazioni oggetto dell'informativa (art. 14).

La relazione di accompagnamento allo schema di Regolamento chiarisce che l'obbligo di documentazione sostituisce quello di notificazione all'Autorità, pertanto, la nuova previsione dovrebbe realizzare una semplificazione per i titolari.

Tuttavia, la norma rischia di ampliare gli oneri burocratici a carico dei titolari. Infatti, il nostro Codice privacy (art. 37), conformemente a quanto ammesso dalla Direttiva 95/46/CE (artt. 18 e 19), circoscrive l'obbligo di notificazione soltanto ad alcune tipologie di trattamento, vale a dire a quelle aventi ad oggetto trattamenti rischiosi.

L'obbligo di documentazione contenuto nella proposta di Regolamento, invece, riguarda indistintamente qualsiasi operazione di trattamento, pertanto, i titolari dovrebbero compilare e conservare per ogni trattamento effettuato (decine o centinaia al giorno nel caso delle imprese), una modulistica dettagliata di informazioni.

Inoltre, tale adempimento risulta privo di utilità in termini di tutela dei dati. Infatti, il nuovo onere si aggiunge all'obbligo generale del titolare di provare che il trattamento è effettuato in conformità al Regolamento (art. 22, par. 1). Quindi, a fini probatori, il titolare è già tenuto a conservare la documentazione che attesta l'avvenuto adempimento degli obblighi generali di informativa e consenso.

Ne consegue che l'art. 28 e i riferimenti a tale disposizione presenti nelle altre disposizioni della proposta di Regolamento dovrebbero essere eliminati (es. art. 22, par. 2, lett. a).

8. Violazione di dati personali

L'art. 31 della proposta di Regolamento introduce la nuova fattispecie di "violazione di dati personali" e la estende a qualsiasi tipologia di trattamento di dati. La previsione è confermata anche dal progetto di Relazione parlamentare, che sul tema non prevede modifiche di natura sostanziale.

Attualmente la fattispecie della violazione di dati personali è prevista dalla Direttiva 2002/58/CE, come modificata dalla Direttiva n. 136/2009 (recepita in Italia con il D.lgs. n. 69/2012), per i soli trattamenti effettuati nell'ambito delle comunicazioni elettroniche.

La generalizzazione della nozione di violazione dei dati personali in relazione a tutti i trattamenti effettuati comporta un appesantimento degli oneri informativi a carico dei titolari, che sarebbero tenuti a notificare all'Autorità di controllo e a comunicare all'interessato (o agli interessati) qualsiasi violazione anche accidentale verificatasi durante l'attività (art. 32).

La misura appare dunque sproporzionata rispetto alle esigenze di protezione dei dati, laddove estesa anche a trattamenti che non presentano rischi specifici.

Si suggerisce, pertanto, di eliminare gli artt. 31 e 32 dallo schema di Regolamento e, per esigenze di coordinamento, anche la definizione di cui all'art. 4, n. 9.

9. Valutazione di impatto sulla protezione dei dati

L'art. 33 della proposta di Regolamento pone a carico del titolare l'obbligo di effettuare una valutazione di impatto sulla protezione dei dati personali nel caso di trattamenti che presentano rischi specifici (*cd.* valutazione d'impatto privacy). La valutazione deve avere ad oggetto il trattamento previsto, i relativi rischi, nonché la descrizione delle misure previste per prevenire tali rischi e garantire la protezione dei dati personali.

Il progetto di Relazione parlamentare apporta alcune modifiche al testo della norma, volte a specificare i casi in cui i trattamenti presentano rischi specifici (Emendamenti nn. 205, 206, 207, 208 e 209). Tuttavia, lo schema di Relazione conferma l'obbligo di effettuare la valutazione di impatto privacy, nonché i relativi contenuti.

L'art. 33 della proposta di Regolamento rischia di reintrodurre nel nostro ordinamento la redazione di un documento meramente formale e burocratico, sul modello dell'abrogato Documento Programmatico sulla Sicurezza (DPS). La valutazione d'impatto privacy, infatti, si riduce nella mera raccolta di informazioni e nella descrizione di aspetti generali relativi ai trattamenti effettuati o da effettuare, senza apportare alcuna effettiva utilità ai fini della protezione dei dati.

L'esperienza italiana attesta che la redazione di un simile documento, non procurando alcun beneficio in termini di tutela dei dati, è fonte esclusivamente di oneri per le imprese, pertanto, al fine di ridurre i costi a carico dei titolari, l'art. 33 della proposta, nonché i relativi riferimenti andrebbero eliminati dalle altre disposizioni dello schema di Regolamento (es. art. 22, par. 1, lett. c); art. 34, co. 2, lett. a).

Infine, con riferimento al novero dei trattamenti rischiosi che richiederebbero, quindi, la valutazione d'impatto privacy, non si condivide l'inclusione della videosorveglianza. Infatti, il ricorso a sistemi di videosorveglianza è sempre più frequente sia nelle attività commerciali, che in ambiti pubblici e privati per esigenze preventive e di sicurezza di persone, beni e locali, pertanto, il relativo trattamento ha assunto un carattere "ordinario" e non può considerarsi pericoloso.

10. Responsabile della protezione dei dati, cd. *privacy officer*

L'art. 35, par. 1 della proposta di Regolamento, nel testo emendato dal progetto di Relazione (Emendamento n. 223) impone al titolare la nomina di un "responsabile della protezione dei dati" (cd. *privacy officer*) quando il trattamento, tra gli altri casi, è effettuato da una persona giuridica e riguarda oltre 500 interessati all'anno (nel testo originario, il riferimento era all'impresa con più di 250 dipendenti - lett. b) ovvero richiede il controllo regolare e sistematico degli interessati (lett. c). In particolare, il *privacy officer* controlla il rispetto degli obblighi derivanti dal Regolamento e costituisce il referente del titolare nei rapporti con l'Autorità di controllo (art. 37).

Al riguardo, i successivi paragrafi 7, 8 e 9 prescrivono al titolare limiti e condizioni in via obbligatoria ai fini della nomina del *privacy officer*, tra cui la durata minima del mandato (4 anni), i casi di revoca ("se non soddisfa più le condizioni richieste"), le modalità stesse di affidamento dell'incarico (contratto di servizi) e obblighi informativi nei confronti dell'autorità di controllo e del pubblico.

Si tratta di aspetti di natura organizzativa e gestionale interna alla struttura del titolare del trattamento, la cui definizione deve necessariamente essere rimessa all'autonomia privata e non invece a una dettagliata disciplina regolamentare. Se così fosse, infatti, tali previsioni interferirebbero in maniera ingiustificata e senza alcun beneficio pratico con la libertà di iniziativa economica.

Allo stesso modo, l'art. 36 della proposta di Regolamento disciplina i rapporti tra il titolare del trattamento e il *privacy officer* in maniera molto dettagliata e poco chiara, con il rischio di comprimere l'autonomia organizzativa e operativa del primo e di ingenerare dubbi interpretativi.

A titolo esemplificativo, si richiama la previsione secondo cui il *privacy officer* è un subalterno diretto del capo dei superiori gerarchici del titolare e non già di quest'ultimo (art. 36, par. 2 - Emendamento n. 229). Non si comprende la *ratio* di tale previsione, che andrebbe eliminata, specie se si considera che il rapporto tra i citati soggetti è sussumibile nello schema del contratto di mandato.

Più in generale, la norma andrebbe corretta per garantire un corretto ed equilibrato bilanciamento tra i poteri/doveri del titolare e del *privacy officer*, salvaguardando le esigenze di semplificazione, flessibilità operativa e autonomia negoziale.

Sulla base di tali considerazioni, i paragrafi 7, 8 e 9 dell'art. 35 e l'intero art. 36 della proposta di Regolamento dovrebbero essere eliminati.

11. Atti delegati

Diverse disposizioni della proposta attribuiscono alla Commissione il potere di adottare atti delegati, al fine di integrare ovvero completare specifici aspetti della disciplina dettata dal Regolamento (es. artt. 9, par. 3; 14, par. 7); 17, par. 9; 22, par. 4). Tale approccio è confermato anche dal progetto di Relazione del PE che, nonostante alcune modifiche ai profili di intervento della Commissione (Emendamenti nn. 104, 144, 186, 191), lascia sostanzialmente impregiudicato il relativo ambito di azione.

L'eccessivo rinvio a norme attuative non è positivo, in quanto rischia di vanificare l'efficacia diretta dello strumento legislativo prescelto, nonchè di attenuare le garanzie di stabilità e certezza della normativa che si intende introdurre.

Sarebbe, quindi, opportuno limitare il ricorso alla legislazione delegata e circoscriverlo agli aspetti non essenziali della disciplina.

12. Sanzioni

L'art. 79 della proposta di Regolamento, confermato anche dal progetto di Relazione parlamentare, prevede sanzioni amministrative pecuniarie particolarmente elevate (fino al 2% del fatturato mondiale annuo).

Infatti, nonostante la norma indichi i criteri di quantificazione delle sanzioni (natura, gravità, durata, carattere doloso o colposo della violazione, grado di responsabilità e comportamenti precedenti del titolare, adozione delle misure di prevenzione, grado di cooperazione con l'Autorità di controllo per rimediare alla violazione), il sistema disciplinato dalla proposta di Regolamento risulta sproporzionato rispetto alle tipologie di illeciti considerati.

Sarebbe, pertanto, opportuno rivedere i massimi edittali delle sanzioni amministrative pecuniarie, al fine di adeguarli alla gravità delle violazioni e alle tipologia degli interessi di volta in volta tutelati.

Roma, 11 marzo 2013