PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4091 di lunedì 02 ottobre 2017

Le responsabilità civili e penali del responsabile della protezione dei dati

Entro il 25 maggio 2018 moltissimi titolari del trattamento dovranno designare un responsabile della protezione dei dati. Come scegliere un responsabile, che porterà sulle sue spalle responsabilità non trascurabili? Di A.Biasiotti e R.Scavizzi.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[BIA0001] ?#>

I titolari del trattamento, che debbono necessariamente designare un responsabile della protezione dei dati, hanno cominciato ad attivarsi, leggendo attentamente un documento, pubblicato dall'autorità garante nazionale, che in realtà non fa che sottolineare il fatto che la responsabilità finale della scelta del responsabile spetta esclusivamente al titolare.

A questo punto è ovvio che il titolare si chieda quali strumenti egli ha a disposizione per valutare le competenze la professionalità del candidato e, anche su questo aspetto, l'autorità garante ha dato delle indicazioni. È ormai in dirittura d'arrivo la pubblicazione della norma UNI-UNINFO su questo profilo professionale, che certamente sarà di grande aiuto a tutti i titolari coinvolti, in quanto un professionista, conforme a questa norma o, meglio ancora, certificato in conformità questa norma, darà garanzia di trovarsi davanti a un soggetto che opera a regola d'arte, come prevede il codice civile.

D'altro canto, anche i candidati al ruolo di responsabile della protezione dati personali debbono acquisire aggiornate informazioni sulle loro specifiche responsabilità. A questo tema è dedicato questo articolo, che affronta in maniera globale questo delicato tema, mettendo a confronto situazioni esistenti in Italia, in Europa e in altre parti del mondo.

I complessi ed articolati obblighi che incombono sul responsabile della protezione dei dati, sia in ambito Ue sia nelle aree al di fuori dell'Europa impongono agli aspiranti Responsabili della protezione dei dati un alto livello di competenza multidisciplinare.

Il ruolo del Data Protection Officer é oramai previsto e disciplinato, direttamente o indirettamente, oltre che in Europa anche in numerosi ordinamenti giuridici nord americani e asiatici.

Per quanto attiene allo 'scenario' europeo appare opportuno rammentare quanto statuito nella Sezione 4 del Regolamento 679/2016 ('General Data Protection Regulation ' d'ora innanzi 'GDPR') dedicata, appunto, alla articolata illustrazione della figura del 'Responsabile della protezione dei dati' (nella versione inglese 'DPO').

Ebbene, l'articolo 37 del GDPR è dedicato alla 'Designazione del Responsabile della protezione dei dati.

Secondo il predetto articolo, il DPO viene designato dal titolare ('Data controller') e dal Responsabile del trattamento ('Data processor') ogni qualvolta:

i. si tratti di trattamenti posti in essere da soggetti pubblici;
ii. le attività principali del titolare o del responsabile consistano in trattamenti che per la loro natura, finalità ed ambito di applicazione richiedano un monitoraggio regolare e sistematico degli interessati su larga scala;
iii. le attività principali del titolare o del responsabile consistano nel trattamento, su larga scala, di categorie particolari di dati personali (dati sensibili e giudiziari).

Ricordiamo al proposito che l'articolo 29 working party ha già emesso un prezioso documento che articola meglio le tre classificazioni sopra elencate.

In relazione ad un gruppo imprenditoriale si può scegliere di nominare un unico DPO. In ogni caso la designazione del soggetto che svolgerà il ruolo di Responsabile della protezione dei dati deve avvenire sulla base delle conoscenze specialistiche della normativa, delle prassi in materia di protezione dei dati personali e della capacità di assolvere i compiti meglio enunciati nell'art. 39 del Reg. 679/2016 (es: fornire consulenza al titolare ed al responsabile in merito agli obblighi previsti dal GDPR; sorvegliare l'osservanza delle prescrizioni contenute nel GDPR, fungere da punto di contatto con le autorità di controllo, etc).

Secondo l'art. 38 comma 3 del GDPR: "Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti". Dunque il DPO deve poter agire in piena autonomia ed indipendenza.

Non a caso, sempre in applicazione della cennata norma:

i. il DPO non può essere rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti;
ii. a tutela della propria indipendenza il Responsabile della protezione dei dati personali è tenuto a riferire "direttamente" al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

Da, ultimo, in relazione alla normativa europea, occorre riflettere in merito all'utilizzo del termine 'Data Protection Officer', nella versione inglese del testo del Regolamento 679/2016 che, nella traduzione italiana, diviene 'Responsabile della protezione dei dati'.

Al riguardo è opportuno soffermarsi su alcune definizioni adottate nell'ambito del *common law*. In particolare nel diritto anglosassone con il termine '*office*' ed '*officer*' si fà riferimento a particolari contesti ed a specifiche funzioni. Non a caso, come rilevato da autorevole dottrina, secondo il **diritto UK** con il termine '*office*' si vuole intendere un "ufficio, organo, funzione, incarico, carica, servizio pubblico o privato in genere [...]". Si tratta di un'espressione dalla "vasta accezione, essa indica, tra l'altro, il potere/dovere relativo ad un ufficio, carica, funzione o incarico pubblico o privato". In connessione con detta definizione, la prefata dottrina osserva come l'"*office*r' sia definibile come un "ufficiale, agente" o come "chiunque sia investito di un *office* pubblico o privato; dipendente, funzionario, ufficiale, incaricato, amministratore, pubblico o privato [...]". Non a caso, conclude l'autore, "il significato preciso del termine va accertato di volta in volta, tenendo conto della grande varietà di accezioni legislative [...]" (F. De Franchis, Dizionario giuridico inglese italiano, english italian, Law dictionary, pp. 1072,1073, Giuffré editore/Milano 1984).

Dunque, la definizione di Data Protection Officer non deve trarre in inganno e, piuttosto, riteniamo debba lasciar intendere che l'individuo, che sarà chiamato a ricoprire detto ruolo, non possa in alcun modo essere considerato come un mandante ('*agent*') o un soggetto che agisca in nome e per conto del titolare o del responsabile. D'altro canto, una siffatta lettura è confermata dalle disposizioni contenute nel GDPR secondo le quali il DPO deve poter agire in modo autonomo ed indipendente, sebbene sia designato dal Data controller e dal Data processor. Di talché l'uso del termine '*officer*' sembrerebbe attribuire al DPO un ufficio, una funzione privata o pubblica o un servizio di supervisione, coordinamento e garanzia, derivante sì da un incarico che però, in ogni caso, non imporrebbe al soggetto che svolge detta attività obblighi di subordinazione, di dipendenza o di esecuzione di direttive e/o ordini da parte dei designatori. E' in questo senso che alla luce della terminologia giuridica di matrice anglosassone ci sembra di poter delineare il ruolo del DPO.

Orbene, orientando la nostra breve disamina della funzione di DPO in ambito internazionale, su un piano comparatistico è interessante richiamare, seppur sinteticamente, quanto disciplinato in alcuni importanti *legal orders* nord americani ed asiatici, anche alla luce delle interessanti osservazioni formulate al riguardo dalla dottrina (Iapp, 'Legal Risks to being a DPO', C. Hanratty, Iapp.org).

Ebbene, cominciamo con il prendere in esame la normativa canadese.

Nell'Anti-Spam Law canadese (cd 'ASL') è previsto il divieto di invio di qualsivoglia email di natura commerciale in assenza di previo esplicito o implicito consenso da parte del destinatario. Qualora fosse accertata detta condotta da parte del mittente, in applicazione della ASL, la Canada Radio Television Commission (organismo che ha il compito istituzionale di verificare la corretta applicazione della predetta normativa), sarebbe legittimata all'applicazione di ammende nei confronti dei soggetti ai quali fosse risultata imputabile la cennata illecita attività.

Inoltre, secondo quanto statuito dall' ASL, nel caso si verificassero le predette violazioni, sarebbe riconosciuto alle persone fisiche ed agli enti il diritto di agire nei confronti dei contravventori.

Al riguardo, occorre precisare che detta prescrizione avrebbe dovuto entrare in vigore il 1 luglio 2017. Allo stato, però, essa è ancora al vaglio del legislatore canadese, che ne ha deciso la sospensione in attesa che il Parlamento si pronunci.

Qualora detta azione divenisse esperibile a seguito della entrata in vigore della norma che la disciplina, i soggetti lesi potrebbero agire per il risarcimento dei danni che, potenzialmente, potrebbero aver subito in conseguenza dell'illecito comportamento posto in essere dagli enti trasgressori. In aggiunta, sarebbero anche legittimati ad esperire altra azione nei confronti delle persone fisiche, che si fossero trovate a ricoprire i ruoli di *director* o *officer* negli enti, ove fossero state commesse le prefate infrazioni purchè detti soggetti fossero stati considerati come coloro che avevano autorizzato, partecipato o, in qualche modo, assentito alla commissione dei cennati illeciti disciplinati dall' ASL.

Relativamente al **sistema legale di Hong Kong** occorre richiamare la Hong Kong Personal Data Ordinance ('HKPDO') in vigore dal 1996.

L'applicazione di tale normativa è rimessa al Privacy Commissioner for Personal Data, il quale ha titolo per agire civilmente e penalmente nei confronti di qualsivoglia '*data user'* in conseguenza di vari illeciti. Fra questi illeciti vi è anche la mancata acquisizione del consenso da parte dell'interessato in caso di trattamento dei dati personali per finalità di marketing, il trasferimento di dati a terzi in assenza di consenso, la comunicazione di false informazioni nei confronti del Commissioner o, anche, la mancata esecuzione di un avviso di ingiunzione.

Inoltre, la *section* 66 della HKPDO prevede l'obbligo di risarcimento in capo al *data user* in favore della persona fisica che ha subito dei danni in conseguenza dell'illecito trattamento dei suoi dati personali. Nell'ordinamento in esame è previsto che l'interessato ('*data subject'*) possa presentare un'istanza al Commissioner affinché quest'ultimo lo assista nell'esperimento dell'azione di risarcimento danni. La legge vigente nello stato di Hong Kong per le violazioni in tema di corretto trattamento dei dati personali prevede ammende fino ad un massimo di circa 130.000 dollari USA e la reclusione fino a cinque anni. Da ultimo, il datore di lavoro può essere considerato responsabile, sul piano civilistico, dell'illecito commesso da un suo dipendente.

Per quanto attiene al **legal order delle Filippine** la norma di riferimento è il Data Protection Act del 2012.

L'organismo nazionale che si occupa di verificare la corretta applicazione delle prescrizioni contenute nel predetto Act è la National Privacy Commission. Tale istituzione ha il potere di infliggere sanzioni pecuniarie e detentive nel caso in cui si verifichino illeciti in tema di *data processing* quali, ad esempio, il trattamento non autorizzato dei dati personali, l'accesso non consentito a dati, causato da condotte negligenti, e la violazione intenzionale dei dati.

In tali casi le condotte illecite verrebbero punite con ammende che potrebbero raggiungere anche l'equivalente di 99.000 dollari

USA e sanzioni detentive, che varierebbero da 6 mesi a 5 anni di reclusione.

Secondo la legislazione in esame, se il trasgressore fosse una persona giuridica, la sanzione avrebbe come destinatari gli *officers* che mediante la loro condotta si dimostrasse abbiano partecipato all'illecito o, tramite il loro comportamento negligente abbiano, di fatto, permesso la commissione dell'illecito penale.

Esaminiamo ora il **sistema legale della Malesia.**

Nell'ordinamento giuridico della Malesia il trattamento dei dati personali è disciplinato dal Personal Data Protection Act.

L'organismo che si occupa di vigilare e dare attuazione alla prefata normativa è la Malaysian Communications and Multimedia Commission, la quale ha titolo per infliggere sanzioni di natura penale, che possono consistere in ammende e, anche, nella reclusione. Dunque, qualora una società non dovesse dare seguito alla richiesta di cessazione del trattamento dei dati personali per finalità di marketing da parte dell'interessato, la sanzione applicabile potrebbe consistere in un'ammenda, che potrebbe essere quantificata anche in un massimo di 63.000 dollari USA ed in un periodo di detenzione personale, che potrebbe arrivare fino a due anni. Si noti come la sanzione della reclusione potrebbe essere inflitta congiuntamente o, in alternativa, alla sanzione pecuniaria. Naturalmente, la scelta dei criteri di applicazione della sanzione dipenderebbero dalle valutazioni che l'organo competente sarebbe chiamato ad effettuare, in merito alla tipologia di illecito contestato, alle modalità di esecuzione dello stesso ed alla portata dei danni, in ipotesi, da esso conseguenti.

Similmente, la violazione delle restrizioni in tema di trasferimento di dati transfrontalieri, potrebbe comportare l'applicazione di una ammenda fino ad un massimo di circa 94.000 dollari USA. Qualora detta violazione risultasse più grave, potrebbe essere inflitta al trasgressore la sanzione della reclusione fino ad un massimo di due anni. Se fosse una azienda a violare le prescrizioni contenute nel Personal Data Protection Act, le persone fisiche che si fossero trovate a ricoprire il ruolo di *officer* all'interno della predetta struttura aziendale potrebbero essere raggiunte dalle prefate medesime sanzioni di natura pecuniaria e/o detentiva, autonomamente o congiuntamente all'ente a cui appartengono. Di talché, anche sul piano processuale, essi verrebbero giudicati nel medesimo procedimento insieme alla azienda ove essi abbiano svolto il ruolo di *officer.*

Il grado di responsabilità dell'*officer* verrebbe valutato in funzione del livello di autorità e potere di decisione di quest'ultimo nello svolgimento dei processi e delle attività all'interno dell'azienda che, in ipotesi, avrebbero comportato la violazione della norma in tema di protezione dei dati.

La **legislazione di Singapore** disciplina il tema della protezione dei dati mediante il Personal Data Protection Act del 2012.

L'organismo pubblico, che ha il compito di vigilare sulla corretta applicazione della normativa in materia di lecito trattamento dei dati personali, è la Data Protection Commission. La norma de qua contiene una serie di prescrizioni relative alle modalità di archiviazione, trattamento, uso, accesso etc di dati personali.

Nel sistema legale di Singapore sono previste sanzioni civili e penali, in relazione alle violazioni afferenti il trattamento dei dati personali.

Secondo una regola generale, in relazione agli ipotetici illeciti in materia di protezione dei dati, gli *officers,* che operano all'interno delle società, potrebbero risultare coautori dei comportamenti contestati insieme ai lavoratori subordinati a titolo di responsabilità per fatto altrui o indiretta ('*vicarious liability'*).

In caso di violazioni di obblighi in tema di corretto trattamento dei dati personali, le sanzioni potrebbero giungere fino ad un massimo di 7.500.000 dollari USA. Contestualmente, le autorità competenti potrebbero, in ipotesi, infliggere nei confronti degli autori di siffatte condotte una pena detentiva compresa fra uno e tre anni di reclusione.

Inoltre, la legge in vigore a Singapore riconosce ai soggetti lesi la facoltà di agire civilmente nei confronti degli enti (*companies, body of persons, etc*) responsabili dell'illegittimo trattamento dei dati personali, residenti nel territorio dello Stato, per il risarcimento dei danni.

In conclusione

Abbiamo voluto passare in rassegna la situazione esistente in vari paesi del mondo, perché in Europa ancora non sono stati definiti con chiarezza i principi di attribuzione di responsabilità, in caso di violazioni del regolamento generale sulla protezione dei dati, che vedono in qualche modo coinvolta la funzione del responsabile della protezione dei dati. Durante un recente convegno, tenuto a Piacenza, un relatore ha illustrato le possibili ipotesi di sviluppo di una copertura assicurativa, poggiata elogio di Londra, indirizzata alla copertura degli aspetti economici, conseguenti a violazioni del regolamento generale. È bene precisare che alcuni paesi europei, come appunto il regno unito, Germania e l'Austria, si trovano in una situazione di vantaggio, rispetto all'Italia, perché in questi paesi la figura del responsabile della protezione dei dati personali insiste da lungo tempo e quindi alcuni problemi, che in Italia stanno appena adesso sorgendo, sono stati già affrontati e risolti da tempo.

Per tutti coloro che si troveranno a svolgere l'attività di DPO in Europa o in aree extra UE può essere quindi raccomandabile stipulare una polizza assicurativa, in grado di garantire una copertura adeguata a fronte dei tanti gravosi e complessi obblighi che incombono sul responsabile della protezione dei dati. In particolare, gli autori desidero ricordare che una titolare del trattamento, con sede in Italia, che trasferisca dati personali in paesi fuori dell'unione europea non solo deve rispettare le specifiche indicazioni del regolamento europeo, ma deve anche rispettare le indicazioni del paese in cui i dati vengono trasferiti. Questa è la ragione per la quale abbiamo ritenuto opportuno offrire una panoramica di ciò che accade o potrebbe accadere trattando dati personali in altri paesi.

Operando sulla fronte della professionalità, non vi è dubbio che la pubblicazione di una norma e l'avvio di processi di certificazione, in conformità questa norma, possono costituire elementi garantistici che un responsabile della protezione dei dati può offrire al titolare del trattamento, che deve selezionare il soggetto idoneo a soddisfare le proprie esigenze, in grado di dare oggettive garanzie di professionalità, controllate maniera indipendente da un organismo terzo.

Adalberto Biasotti e Roberto Scavizzi

Questo articolo è pubblicato sotto una Licenza Creative Commons.

I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.

---

www.puntosicuro.it