



Senato della Repubblica

giovedì 31 maggio 2018

Uffici di Presidenza congiunti delle Commissioni speciali per l'esame degli atti urgenti presentati dal Governo

Audizione di Confesercenti nell'ambito dell'esame dell'atto del Governo n. 22 (adeguamento normativa nazionale circa la protezione delle persone fisiche con riguardo al trattamento dei dati personali).

Per le imprese rappresentate da Confesercenti le problematiche derivanti dall'applicazione nel nostro Paese, a far data dallo scorso 25 maggio, delle disposizioni del GDPR non sono date dalla mancata armonizzazione delle norme di cui al Regolamento europeo n. 679/2016 con quelle del Codice della Privacy, né possiamo dire di dover osservare, nel contesto dello Schema di decreto legislativo sul quale oggi siamo chiamati ad esprimere il nostro punto di vista, la presenza di disposizioni da emendare, se non per aspetti concernenti l'apparato sanzionatorio, come poi si dirà.

Il problema sorge piuttosto dalla modalità con cui la normativa comunitaria si atteggia, lasciando in teoria molto spazio all'autoregolazione, ma poi prevedendo tutta una serie di obblighi ed adempimenti che mal si attagliano alla struttura e alla dimensione delle micro e piccole imprese, tanto da far temere per le conseguenze immediate per la piccola imprenditoria, se è vero quanto recentemente la nostra Organizzazione ha dichiarato, facendo riferimento alla semplice osservazione di quanto accade sul territorio, e cioè che **l'applicazione del GDPR costerà ai circa 4 milioni di MPMI italiane almeno 2 miliardi di euro.**

Si tratta di una stima, oltretutto, estremamente conservativa: essa si basa infatti su una **spesa media di 500 euro ad impresa, il minimo richiesto dalle società di consulenza per gli adempimenti di base del GDPR.** Ma saranno moltissime le PMI che con tutta probabilità dovranno sborsare molto di più, dovendo nominare un DPO esterno responsabile del trattamento dati, che può costare, a seconda della complessità del trattamento e della dimensione dell'impresa, fino a 5mila euro l'anno.

Un conto decisamente troppo salato per una norma nata per limitare l'invasività e lo *spam* dei giganti di internet e della telefonia, ma che, in mancanza di norme o quanto meno indicazioni che conducano ad una indispensabile semplificazione, finirà per applicarsi anche a ditte individuali e piccole imprese come ristoranti, bar e sale da barba, che pagheranno, in mancanza dei richiesti adeguamenti, multe anche molto onerose.

E non è sufficiente la previsione, all'interno dello Schema di decreto (art. 22, comma 10), di modalità semplificate di adempimento degli obblighi da parte del titolare del trattamento, che il Garante potrà promuovere nelle Linee-Guida di indirizzo previste dallo stesso Schema di decreto per le misure organizzative e tecniche di attuazione dei principi del Regolamento UE.

Non lo è, inevitabilmente, per il ritardo con cui, approvato lo Schema da parte del Governo, il Garante predisporrà le Linee-Guida e le imprese potranno contare su misure adeguate ai propri casi, quando ormai moltissime saranno quelle che, per non rischiare di incorrere in sanzioni, si saranno fatte assistere da società di consulenza che le avranno "opportunamente" consigliate a spendere cifre esose.

Ma non lo è soprattutto perché, diversamente da quanto aveva previsto qualche anno fa, quando, con il DL n. 112/2008, aveva modificato l'art. 34 del Codice, **il legislatore non ha pensato, allo stato attuale, a norme di favore per le PMI, che, ad esempio, escludano l'applicazione di taluni adempimenti, a prescindere dalla natura dei dati trattati, per le imprese che trattino dati solo per finalità connesse allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile**, quali quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro.

A nostro avviso ciò sarebbe possibile già con il D. Lgs. di cui oggi si discute, senza attendere le previsioni del Garante nelle Linee-Guida, se si considera che la legge n. 163/2017 delega il Governo a modificare il Codice della Privacy in relazione a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili e coordinare le disposizioni vigenti con quelle recate dal Regolamento (UE) 2016/679.

Dunque, **per le fattispecie di cui si è detto, lo Schema di decreto potrebbe chiarire che alle MPMI di cui alla Raccomandazione 2003/361/CE non si applica l'adempimento di cui all'art. 30 del Regolamento**, laddove prevede che l'**obbligo di tenere un Registro delle attività di trattamento**, normalmente escluso per le imprese con meno di 250 dipendenti, vale invece per i trattamenti non occasionali o che includano categorie particolari di dati di cui all'art. 9, paragrafo 1 (quelli che il Codice definisce "dati sensibili").

Potrebbe altresì essere chiarito che alle MPMI, nei casi di cui si è detto, non si applica l'obbligo, di cui all'art. 35, di effettuare la **valutazione di impatto** prevista per le fattispecie in cui il trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche.

Infine, **si potrebbe prevedere l'esclusione dell'obbligo di cui all'art. 37**, che prevede la sistematica **designazione di un responsabile della protezione dei dati (DPO)** nel caso in cui le attività principali del titolare del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala, oppure nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9.

Sia nel caso dell'art. 35, che dell'art. 37, **ci si attenderebbe comunque una declaratoria dei concetti di "rischio elevato per i diritti delle persone fisiche" e di "larga scala"**.

Ancora, oltre alle predette esenzioni, le MPMI si attenderebbero che, nei **casi di semplice utilizzo di elenchi di clienti che abbiano fornito i propri dati identificativi limitati alle generalità, all'indirizzo del domicilio ed alla mail consentendo espressamente all'invio di promozioni e offerte (*direct marketing*)**, gli adempimenti siano ridotti al minimo, ossia ad una registrazione semplice, secondo un *format* elementare, oltre che alla messa in sicurezza dei dati, alla garanzia di non diffonderli e di comunicarli a terzi solo in caso di consenso espresso da parte dell'interessato.

Ciò detto, e tornando all'anticipata **problematica relativa all'apparato sanzionatorio**, non può non evidenziarsi anzitutto come l'art. 83 del Regolamento n. 679 preveda per la violazione delle disposizioni ivi stabilite un tetto massimo particolarmente elevato (fino a 10 e 20 mln di euro, a seconda delle fattispecie), stabilendo poi che se l'Ordinamento giuridico dello Stato membro non prevede nello specifico sanzioni amministrative pecuniarie, l'articolo 83, laddove individua le particolari sanzioni, potrà essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'Autorità di controllo e la sanzione pecuniaria irrogata dalle Autorità giurisdizionali nazionali.

Lo Schema di decreto legislativo prevede, all'uopo, una norma (art. 15) che inserisce nel Codice della Privacy l'art. 166, il quale reca i criteri di applicazione delle sanzioni amministrative pecuniarie.

Orbene, sia nel caso in cui eventualmente una violazione di cui al Regolamento comunitario non ricada nelle previsioni di cui al menzionato art. 166, sia nell'ipotesi in cui invece detta norma preveda la specifica violazione ricollegandola alla sanzione di cui all'art. 83, paragrafi 4 e 5, del Regolamento, **appare estremamente discrezionale il potere conferito al Garante nel determinare ed irrogare la sanzione**, senza considerare il fatto che **la mancata indicazione del minimo edittale non consente l'applicazione dell'istituto del pagamento in misura ridotta**, di cui all'art. 16 della legge n. 689/81, che infatti non viene neppure richiamato.

Si ritiene che di ciò il legislatore debba prendere atto per gli opportuni interventi correttivi, al fine di tener conto dell'esigenza di applicare alle MPMI un regime sanzionatorio progressivo ed adeguato.