Confartigianato Imprese

Camera dei Deputati
Senato della Repubblica

Commissioni speciali riunite

XVIII Legislatura

Audizione

Atto del Governo n. 22

“Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679, 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 (regolamento generale sulla protezione dei dati) (n. 22)”

Roma, 31 maggio 2018

Premessa

Dal 25 maggio scorso in tutta Europa trova applicazione il nuovo Regolamento Privacy.

Il Regolamento prevede un nuovo approccio teso a privilegiare l'aspetto sostanziale basato sul principio dell'*accountability*, (non più adempimenti meramente formali). In altri termini l'azienda è "responsabilizzata" ad analizzare la propria situazione e gli eventuali specifici rischi prima di porre in essere azioni concrete, anche da un punto di vista organizzativo.
In sostanza nessuna impresa, per quanto piccola e operante nei settori tradizionali, può dirsi automaticamente esclusa dalla nuova disciplina se non a seguito di un'adeguata valutazione dei rischi.

L'impresa deve, quindi, porre in essere una serie di azioni per essere in linea con le nuove disposizioni:

- mappare i trattamenti dei dati (ovvero verificare la sua situazione rispetto ai dati che tratta);
- individuare le azioni per essere in regola con la nuova normativa;
- dimostrare la conformità alla nuova disciplina.

Numerosi sono i passaggi nel Regolamento Europeo che focalizzano l'attenzione sulle esigenze delle micro, piccole e medie imprese (MPMI), in attuazione del principio di proporzionalità alla base dello Small Business Act europeo.
Basti pensare, a titolo esemplificativo, al considerando 13 laddove si invitano gli Stati membri e le Autorità di Controllo a *" […] considerare le esigenze specifiche della micro, piccola e media impresa nell'applicare il Regolamento"* ovvero all'esclusione dall'obbligo di tenuta del registro dei trattamenti per le imprese con meno di 250 dipendenti (art. 30 comma 5) salvo casi specifici o dalla previsione (art. 40) di codici di condotta che devono tenere contro delle "*esigenze specifiche delle micro, piccole e medie imprese".*

La stessa Commissione Europea, infine, in base al considerando 167, dovrebbe prevedere misure specifiche per le MPMI.

Confartigianato Imprese ritiene importante l'adozione del decreto legislativo all'esame delle Commissioni, al fine di creare un quadro normativo chiaro che sia in linea con la nuova disciplina e che non lasci spazi a dubbi interpretativi e conflitti tra le norme da applicare.

Nel merito dello schema di decreto legislativo, è condivisibile la scelta di aggiornare il Codice privacy concentrando la disciplina in un unico provvedimento che regoli e definisca gli ambiti di intervento che il Regolamento rimanda agli Stati Membri. Per la stessa finalità sarebbe utile ricondurre anche le norme in materia di privacy contenute nell'ultima Legge di bilancio 2018 (articolo 1, commi 1021 – 2024 – attribuzione di compiti al Garante) all'interno del presente provvedimento.

Il decreto dovrà però, in linea con il dettato europeo, prevedere chiaramente la definizione di strumenti e modalità semplificati per le micro e piccole imprese da sempre protagoniste dello scenario imprenditoriale ed economico tanto italiano, quanto europeo.
Obiettivo primario dovrà essere non gravarle di oneri e adempimenti sproporzionati rispetto alle reali esigenze di tutela dei dati personali.

Gli oneri dovrebbero essere, quindi, **proporzionati rispetto al rischio potenziale,** anche qualora quest'ultimo sia collegato al campo della sicurezza informatica (grado di sicurezza dei *server*, conservazione dei dati, trasferimento, ecc.) che certamente richiede un livello più elevato di garanzie rispetto al trattamento cartaceo.

Per Confartigianato, infatti l'adeguamento della normativa nazionale al Regolamento europeo deve rappresentare l'occasione per ribadire ed applicare il principio cardine della proporzionalità, secondo il criterio del "*Think Small First*" contenuto nello *Small Business Act* europeo, recepito in Italia nello "Statuto delle imprese" (L. n. 180/11) i cui principi costituiscono *norme fondamentali di riforma economico-sociale della Repubblica e principi dell'ordinamento giuridico dello Stato*.

Tra tali norme si richiama l'applicazione dei ***criteri di proporzionalità e****, qualora possa determinarsi un pregiudizio eccessivo per le imprese,* ***di gradualità*** *in occasione dell'introduzione di nuovi adempimenti e oneri a carico delle imprese,* ***tenendo conto delle loro dimensioni, del numero di addetti e del settore merceologico di attività*** (art. 6, co. 1).

Di seguito alcune osservazioni specifiche che, qualora recepite, consentirebbero all'emanando decreto di essere "a dimensione di micro e piccola impresa", evitando adempimenti e costi inutili per le imprese e consentendo, allo stesso tempo, di essere adeguate rispetto alla normativa europea.

- **Semplificazioni per le micro e piccole imprese – art. 14**

L'articolo 14 dello schema di decreto – che introduce il nuovo articolo 154-bis del Codice della Privacy – è relativo ai **poteri del Garante.**
Tali disposizioni attribuiscono un nuovo e fondamentale potere all'Autorità che potrà adottare **linee guida** contenenti le misure organizzative e tecniche *anche per singoli settori e in applicazione dei principi di cui all'articolo 25 del Regolamento* (*privacy by design e privacy by default*). In questo contesto bisognerà prevedere esplicitamente che tali linee guida abbiano al loro interno anche specifiche **modalità semplificate** di adempimento degli obblighi per le **micro e piccole imprese** così come previsto dal Regolamento europeo.

Una specifica semplificazione, ad esempio, potrebbe riguardare le imprese senza dipendenti, che trattano dati "non sensibili". Si tratta di una platea di imprese (ad esempio orafi, restauratori, riparatori di elettrodomestici, etc.) che certamente non effettuano trattamenti su "larga scala", né utilizzano sofisticati strumenti di profilazione dei propri clienti, né acquistano o rivendono dati personali e che, pertanto, presentano rischi minimi per la protezione dei dati personali.

Lo schema di decreto trasmesso in Parlamento prevede solo al comma 10 dell'art 22 - relativo alle disposizioni transitorie - la promozione da parte del Garante, all'interno delle linee guida, di modalità semplificate di adempimento degli obblighi del titolare del trattamento.

A nostro avviso è fondamentale, che già nel nuovo art. 154-bis relativo ai poteri del Garante, vengano previste le **modalità semplificate per le micro e piccole imprese** che, auspicabilmente, dovranno essere emanate **nel più breve tempo possibile,** data la necessità di garantire a tutte le imprese, in particolare alle più piccole, la possibilità di essere conformi al nuovo regolamento privacy senza un aggravio di oneri e costi.

Condizione proposta:

All'art. 14, comma 1, lett. d, capoverso Art. 154-bis, comma 1, lett. a), aggiungere infine i seguenti periodi: "*Le linee guida individuano modalità semplificate di adempimento degli obblighi del titolare del trattamento in considerazione delle esigenze delle micro, piccole e medie imprese, come definite dalla Raccomandazione 2003/361/CE. Le linee guida prevedono ulteriori specifiche modalità semplificate di adempimento degli obblighi del titolare del trattamento per le imprese senza dipendenti, che non trattano categorie particolari di dati ai sensi dell'art. 9 del Regolamento o dati relativi a condanne penali o reati ai sensi dell'art. 10 del Regolamento".*

All'articolo 22, comma 10, sostituire le parole: "*adottate*" con le seguenti: "*da adottare entro tre mesi dalla data di entrata in vigore del presente decreto legislativo*".

- **Periodo di grazia e sanzioni – art. 15**

In considerazione dell'applicazione dallo scorso 25 maggio del Regolamento e del fatto che l'ordinamento interno non è stato ancora adeguato, si ritiene indispensabile introdurre un periodo di moratoria relativo alle sanzioni pecuniarie. Un simile intervento è già stato adottato dal Garante francese (CNIL) e da quello austriaco. In entrambi i Paesi è stato concesso un *grace period* per i primi mesi di applicazione del Regolamento.
Inoltre, l'Organizzazione europea di rappresentanza dell'artigianato e delle micro e piccole imprese, UEAPME, della quale Confartigianato è membro fondatore, nelle scorse settimane ha chiesto alla Commissaria europea per la Giustizia, Vera Jourova un periodo di grazia di

un anno anche alla luce del fatto che molti degli orientamenti e delle note interpretative del cosiddetto Gruppo di Lavoro Art. 29 sono stati emanati solo negli ultimi mesi.

Anche in Italia è auspicabile prevedere un periodo di almeno sei mesi successivo all'entrata in vigore del provvedimento in esame nel quale, in caso di controlli relativi ai nuovi adempimenti, per le micro e piccole imprese non si applichino sanzioni economiche ma soltanto prescrizioni di adeguamento alla nuova disciplina. D'altronde, in linea con quanto previsto dall'art. 58 del Regolamento ogni Autorità di controllo, oltre al potere di infliggere una sanzione amministrativa, è dotata di un'ampia serie di poteri correttivi nei confronti del titolare del trattamento, tra cui ricordiamo, i poteri di:

a) rivolgere avvertimenti o ammonimenti;
b) ingiungere di soddisfare le richieste dell'interessato;
c) ingiungere di conformare i trattamenti alle disposizioni del regolamento;
d) ingiungere di comunicare all'interessato una violazione dei dati personali;
e) imporre una limitazione provvisoria o definitiva al trattamento.

Si auspica, pertanto, che alla luce dell'attuale situazione di incertezza normativa possano essere fornite indicazioni precise sull'applicazione progressiva dei poteri correttivi del Garante, tenendo conto della proporzionalità e della gravità delle eventuali violazioni rilevate e dell'eventuale recidiva.
In tal modo si accompagnerebbero le imprese nel percorso di *compliance* al Regolamento, evitando ripercussioni negative per le micro e piccole imprese che non potrebbero sopportare il peso di pesanti sanzioni.
Tale approccio dovrà essere attuato in maniera particolarmente scrupolosa in questa prima fase di applicazione del Regolamento, fintantoché le imprese – in special modo quelle di micro e piccola dimensione – non siano nelle condizioni di potersi adeguare al Regolamento attraverso gli istituti ad esse dedicati, in primis il Codice di condotta. Questo strumento - introdotto dall'art. 40 del Regolamento con la finalità di accompagnare nel processo di *compliance* le imprese con meno di 250 addetti - non è al momento utilizzabile in carenza di indicazioni uniformi sul funzionamento del monitoraggio previsto dall'art. 41 dello stesso Regolamento.

Osservazione proposta:

Si invita il Governo a valutare, in accordo con il Garante per la protezione dei dati personali, l'opportunità di prevedere che, in considerazione dell'attuale incertezza normativa e dell'impossibilità per le PMI di aderire ad un Codice di condotta, in caso di violazione dei nuovi adempimenti introdotti dal Regolamento europeo, si applichino esclusivamente i poteri correttivi attribuiti al Garante (di cui all'art. 58, paragrafo 2, del Regolamento) in luogo delle sanzioni economiche.

- **Marketing diretto – art. 11**

Si valuta positivamente il mantenimento dell'art. 130, comma 4, del Codice italiano che – in materia di marketing diretto – consente al titolare del trattamento di utilizzare, anche senza l'ottenimento del consenso, gli indirizzi di posta elettronica forniti dall'interessato nell'ambito della vendita di un prodotto o servizio, al fine di proporre prodotti o servizi analoghi. Si chiarisce in tal modo che il ***marketing* diretto** può essere effettuato sulla base del legittimo interesse del titolare. Sarebbe però opportuno chiarire che tale attività non deve essere svolta solo per le *e-mail*, ma anche attraverso altri strumenti oggi ampiamente utilizzati da imprese e clienti per le proprie comunicazioni (sms, social, whatsapp, etc.).

Condizione proposta:

All'art. 11, co. 1, lett. g), dopo il punto 6, inserire il seguente: 6-bis) al comma 4, aggiungere infine il seguente periodo "*La presente disposizione si applica anche nel caso di invio di sms, mms e di utilizzo dei social media o della posta cartacea".*

- **Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute – art. 2**

L'art. 2-septies inserito all'art. 2 dello schema di decreto, prevede che il Garante privacy debba adottare *misure di garanzia* in relazione ai trattamenti di *dati genetici, biometrici e relativi alla salute*. In proposito, il parere del Garante sullo schema di decreto legislativo contiene un'osservazione diretta a specificare che dette misure individuino anche le misure

di sicurezza (comprese tecniche di cifratura e di pseudonimizzazione, misure di minimizzazione, etc.). Una tale previsione potrebbe comportare un ulteriore aggravio di oneri per le imprese che trattano i dati in questione limitatamente ad un esiguo numero di persone. In tali casi misure come la cifratura o la pseudonomizzazione costituirebbero un onere sproporzionato rispetto al rischio concreto. Si prenda, ad esempio, il caso di una micro impresa che tratta i dati sensibili dei propri dipendenti: un trattamento di un numero assai ridotto di dati, effettuato sulla base di obblighi legali e contrattuali. Costringere l'azienda in esempio a cifrare i propri computer costituirebbe un costo evidentemente sproporzionato rispetto al rischio effettivo. Per evitare un simile aggravio si propone di applicare l'obbligo di adottare tali misure, limitatamente ai "*trattamenti su larga scala*", così come previsti dal considerando 91 del Regolamento europeo, ovvero ai trattamenti di una *notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*.

Osservazione proposta:

All'articolo 2-septies specificare che le misure di garanzia si applicano limitatamente ai trattamenti su larga scala.

- **Autorizzazioni generali del Garante in materia di diritto del lavoro - 21**

L'art. 21 dello schema di decreto prevede che il Garante individui, entro 90 giorni, quali prescrizioni, contenute nelle autorizzazioni generali in vigore, siano compatibili con il nuovo regolamento europeo, limitatamente ad alcune materie.

Le autorizzazioni generali sono previste dal Codice italiano privacy per consentire al titolare di trattare dati sensibili anche senza il consenso dell'interessato e hanno consentito di semplificare alcuni importanti trattamenti, *in primis* quello in materia di rapporto di lavoro.

L'autorizzazione generale in materia di rapporto di lavoro ha, infatti, consentito all'imprenditore di trattare i dati sensibili dei propri dipendenti senza richiedere il loro consenso in quanto trattamenti obbligati da norme o da contratti collettivi. Si concorda, pertanto, con l'osservazione, contenuta nel parere dello stesso Garante relativamente

all'art. 21, volta a prevedere che tale verifica di compatibilità riguardi anche l'**autorizzazione generale al trattamento di dati sensibili nel rapporto di lavoro**. Si ritiene, infatti, importante che le previsioni di tale autorizzazione, emanata nel 2016, siano verificate e mantenute, ove compatibili con il Regolamento, al fine di consentire alle imprese di proseguire a trattare tali dati in base a regole consolidate.

Si concorda, altresì, con l'osservazione del Garante volta a prevedere che la cessazione degli effetti delle autorizzazioni generali ritenute incompatibili dovrà prodursi al momento della pubblicazione in Gazzetta Ufficiale della versione finale del provvedimento.

Osservazioni proposte:

All'articolo 21:

a) al comma 1 sostituire le parole: "9, paragrafo 4" con le seguenti: "9, paragrafo 2, lett. b) e 4";
b) sostituire il comma 2 con il seguente: 2. *Le autorizzazioni generali, sottoposte a verifica a norma del comma 1, che sono state ritenute incompatibili con le disposizioni del regolamento (UE) cessano di produrre effetti al momento della pubblicazione in Gazzetta Ufficiale del provvedimento di cui al comma 1*.