



NOTE E COMMENTI

Il regolamento europeo sulla privacy e la fase di attuazione in Italia

Il 25 maggio 2018 è entrato in applicazione in tutti i Paesi dell'Unione il Regolamento europeo sulla privacy (GDPR – General Data Protection Regulation) approvato il 14 aprile 2016 (n. 2016/679), con il quale è stato delineato un nuovo quadro normativo in materia di protezione dei dati personali, che pone molte nuove regole e importanti adempimenti da rispettare (cfr. il sito web <https://ogl.chiesacattolica.it>).

In Italia, il 21 marzo 2018 il Consiglio dei ministri ha approvato, in esame preliminare, un decreto legislativo in attuazione dell'articolo 13 della legge di delegazione europea (n. 163 del 25 ottobre 2017). Il **21 maggio 2018** è scaduta la delega conferita dalle Camere al Governo: il termine è prorogato di tre mesi, ai sensi dell'articolo 31 della legge n. 234 del 2012 (Procedure per l'esercizio delle deleghe legislative conferite al Governo con la legge di delegazione europea).

Le modifiche al decreto legislativo n. 196/2003

Il corpus di norme all'esame è molto ampio: si tratta di 28 articoli raggruppati in sei Capi, che intervengono con abrogazioni e modificazioni

sulla quasi totalità dei 186 articoli del codice *privacy* vigente.

Nel suo complesso, lo schema di decreto legislativo reca un ampio intervento sul codice in materia di protezione di dati personali, di cui al decreto legislativo n. 196 del 2003. La parte più consistente delle modifiche riguarda l'abrogazione delle norme del codice incompatibili o sovrapponibili a quelle del regolamento europeo, che per loro natura sono direttamente applicabili nei singoli Stati. Altri interventi sono invece finalizzati ad adattare, attraverso novelle legislative, le previsioni del codice alle disposizioni del regolamento europeo non direttamente applicabili, che lasciano spazi di intervento ai legislatori nazionali.

Nella relazione di accompagnamento si evidenziano talune scelte compiute in sede di predisposizione dello schema. In particolare si sottolinea come, per garantire la continuità, siano stati **fatti salvi per un periodo transitorio i provvedimenti del Garante e le autorizzazioni**, che saranno oggetto di un successivo riordino, nonché i codici deontologici vigenti. Per le piccole e medie imprese, si è previsto che il Garante promuova modalità semplificate di adempimento degli

obblighi del titolare del trattamento dei dati personali. Non sono state modificate, infine, le disposizioni concernenti le comunicazioni elettroniche, in attesa che venga emanato l'apposito regolamento europeo.

Il parere del Garante della Privacy

In attesa della conclusione dell'esame parlamentare, il 22 maggio scorso il **Garante della Privacy** ha fornito il **proprio parere** sullo *schema di decreto legislativo per l'adeguamento della normativa nazionale alle disposizioni del nuovo Regolamento (Ue) 2016/679 sulla Data Protection (GDPR)*. Al riguardo, il Garante mette in evidenza alcune posizioni critiche, sottolineando l'opportunità di alcune modifiche e integrazioni, in particolare in materia di Data Retention con il prolungamento fino a 72 mesi (sei anni) dell'obbligo di conservazione dei dati di traffico telefonico e telematico, nonché alle chiamate senza risposta per anti-terrorismo. *“La conferma di tale deroga determina rilevanti criticità...in ordine al rispetto del principio di proporzionalità tra esigenze investigative e limitazioni del diritto della protezione dei dati dei cittadini”*, si legge nel parere del Garante.

Viene espressa poi *“preoccupazione”* per le disposizioni in materia di Piattaforma digitale nazionale dei dati (articolo 50) finalizzata a favorire la conoscenza e l'utilizzo del patrimonio informativo, detenuto, per finalità istituzionali, dai soggetti pubblici che in fase sperimentale sarebbe affidata al Commissario Straordinario per l'Attuazione dell'Agenda Digitale. *“La pur necessaria valorizzazione del patrimonio informativo pubblico non deve, infatti, avvenire a discapito della tutela dei diritti fondamentali e con possibili ricadute anche in termini di sicurezza nazionale”*, si legge nel parere del Garante, che teme quindi la concentrazione presso un unico soggetto di informazioni, anche sensibili e sensibilissime, con evidenti rischi di usi distorti e accessi non autorizzati di dati sensibili condivisi.

Per quanto riguarda il trattamento illecito di dati (art. 167 dello schema di decreto) il Garante chiede di valutare, per stabilire sanzioni penali, *“quale oggetto alternativo del dolo specifico il danno e non solo il profitto”*. In altre parole, il reato di uso illecito dei dati secondo il Garante dovrebbe

considerare soprattutto il danno d'immagine e reputazionale della vittima e non solo il profitto economico dell'autore dell'illecito.

In relazione ai servizi della società dell'informazione, **il Garante fissa a 14 anni (e non a 16) l'età minima per iscriversi ad un social network**. Se a 14 anni un ragazzo può denunciare atti di bullismo e dare il suo consenso all'adozione, sarebbe incoerente non consentirgli anche di iscriversi ai social a quell'età, tanto più che lo schema di decreto, in relazione ai servizi dell'informazione, indica che è consentito *“il trattamento dei dati personali del minore di età inferiore a sedici anni”*.

Il Garante solleva inoltre alcuni dubbi sulla nozione di *“riutilizzo”* che non viene definita dal decreto, che *“coincide con l'utilizzo da parte di terzi, a fini commerciali o non commerciali, diversi da quelli iniziali per i quali le informazioni sono state prodotte, e riguarda soltanto i documenti contenenti dati pubblici (indipendentemente che si tratti di dati personali o meno) nella disponibilità di pubbliche amministrazioni e di organismi di diritto pubblico”*.

Il Garante suggerisce di sostituire il termine *“riutilizzo”* con quello di *“trattamento ulteriore da parte di terzi”*.

Ridefinita la categoria dei “Dati sensibili”

Con l'entrata in vigore del Regolamento (UE), la categoria dei dati sensibili è stata ridefinita facendo ora riferimento a *“categorie particolari di dati personali”*. In generale, il trattamento di questi dati – che **sostanzialmente sono gli stessi già definiti “sensibili” con l'aggiunta dei dati genetici e biometrici e relativi all'orientamento sessuale** – è vietato, a meno che non trovi fondamento nel consenso esplicito dell'interessato ovvero nella necessità del trattamento stesso per una serie di motivi tassativamente elencati, che il parere del Garante propone di integrare. Per dare attuazione a questa disposizione il nuovo **articolo 2-sexies dello schema di decreto legislativo** disciplina il trattamento delle categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante, consentendolo solo in presenza di un fondamento legislativo o regolamentare che specifichi i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante. Sul punto, il Garante condiziona il proprio parere favorevole

alla modifica dell'articolo 2-sexies volta a prevedere che l'eventuale atto regolamentare che individua la base giuridica del trattamento dei dati sia adottato in conformità al parere espresso dal Garante. L'Autorità richiede inoltre che il fondamento normativo debba contenere anche le specifiche misure a tutela dell'interessato.

Tra i dati particolari si colloca anche la **categoria dei dati genetici, biometrici e relativi alla salute**, per il cui trattamento il Regolamento (UE) consente agli Stati membri di introdurre garanzie supplementari, e dunque di mantenere o introdurre ulteriori condizioni, comprese limitazioni. A tal fine, il nuovo **articolo 2-septies** prevede che il trattamento di questi dati sia subordinato all'osservanza di misure di garanzia, stabilite dal Garante con provvedimento adottato con cadenza almeno biennale, a seguito di consultazione pubblica. Sul punto il Garante condiziona il proprio parere favorevole alla specificazione del possibile contenuto delle misure di garanzia. Tali dati non possono inoltre essere diffusi. Infatti, l'articolo 2-septies, in relazione esclusivamente ai dati genetici ed a quelli relativi ad ambito sanitario, diagnostico e alle

prescrizioni di medicinali, prevede che nell'ambito delle misure di garanzia sia possibile anche, in caso di particolare ed elevato livello di rischio, introdurre il consenso come ulteriore misura di protezione dei diritti dell'interessato.

La materia, così come normata dallo schema di decreto legislativo, ha suscitato una **serie di critiche** in sede parlamentare, durante le prime sedute di discussione dell'atto governativo. In particolare, da alcune parti politiche si sostiene che "le indicazioni contenute nel regolamento europeo già risultano sufficienti a garantire un adeguato livello di tutela dei dati genetici, biometrici e relativi alla salute. Non vi sarebbe pertanto la necessità di introdurre ulteriori condizioni o limiti, in attuazione di quanto previsto dall'articolo 9, paragrafo 4, del regolamento europeo". Si osserva, inoltre, che le materie per le quali si prevedono le misure di garanzia, al comma 4 dell'articolo 2-septies, esulano in parte dal campo della tutela del dato sensibile. Si ritiene che analoghe considerazioni debbano riguardare il trattamento dei dati genetici.

(Consiglio dei ministri, seduta del 21/3/18)