CONFINDUSTRIA

Position Paper

Schema di Decreto Legislativo di adeguamento al GDPR

Osservazioni di Confindustria

16 Maggio 2018

Premessa

Il Consiglio dei Ministri del 21 marzo 2018 ha approvato in via preliminare lo **schema di Decreto Legislativo di adeguamento della normativa nazionale al Regolamento europeo sulla protezione dei dati personali** (di seguito: "Regolamento" o "GDPR"), che dà attuazione dell'art. 13 della Legge di Delegazione europea 2016 – 2017. Il 10 maggio scorso il provvedimento è stato trasmesso alle Camere e al Garante privacy per l'acquisizione dei relativi pareri.

Come noto, dal 25 maggio 2018 sarà operativo in tutta l'Unione europea il GDPR ed entro tale data i Legislatori nazionali dovranno rivedere la propria disciplina interna, al fine di adattarla a quella europea. Pertanto, lo schema di decreto allinea la regolamentazione italiana in tema di privacy alle disposizioni del Regolamento, novellando il vigente D.Lgs n. 196/2003 (*cd*. Codice privacy) e abrogandone espressamente le norme incompatibili.

Prima di passare all'esame dello schema di decreto, Confindustria ritiene opportuno soffermarsi su alcuni profili che emergono dalla riforma della disciplina sulla protezione dei dati personali.

In primo luogo, Confindustria ha accolto con favore l'intenzione del Legislatore europeo di procedere all'aggiornamento della normativa privacy nella **forma del Regolamento**. Esso, infatti, consente di assicurare in ambito Ue un'armonizzazione completa della regolamentazione sulla protezione dei dati personali, riducendo le difficoltà, le incertezze e i costi - derivanti da 28 regimi privacy differenti - che oggi sostengono le imprese che operano oltrefrontiera. L'auspicio, quindi, è che venga preservata **l'uniformità giuridica** che lo stesso GDPR mira a realizzare, limitando l'intervento nazionale ai profili strettamente necessari all'attuazione della disciplina europea, evitando l'introduzione di vincoli ulteriori e preservando il bilanciamento realizzato dal Regolamento tra libera circolazione dei dati, sviluppo tecnologico e diritti degli interessati.

In secondo luogo, è noto come l'introduzione del principio di **responsabilizzazione** (cd. *accountability*) trasformi la *compliance* privacy da adempimento normativo a sistema di gestione: le imprese sono chiamate a valutare, adeguare e dimostrare la conformità dei trattamenti che realizzano al Regolamento, nonché a mutare il proprio approccio alla protezione dei dati personali. L'attuazione di tale nuovo approccio presuppone un vero e proprio cambio culturale, cui Confindustria sta contribuendo, sensibilizzando le imprese sulle opportunità derivanti dall'applicazione delle nuove regole e supportandole in questa fase di transizione.

Tuttavia, con riferimento all'implementazione del GDPR da parte degli operatori italiani, si registra un **fenomeno a doppia velocità**:

- da una parte, le imprese più grandi e più strutturate, che sin da subito hanno iniziato a definire procedure e modelli di *compliance* e che, salve alcune difficoltà derivanti dal ritardo registrato nella definizione del quadro giuridico, sono pronte ad approfittare di questo salto di qualità;

- dall'altra, le imprese di medie e piccole dimensioni che, pur avendo dimostrato sin da subito un interesse nei confronti del nuovo quadro regolatorio, manifestano ancora molte difficoltà - operative ed economiche - nelle attività di *compliance* e che, pertanto, vanno sostenute.

È per tali ragioni, che Confindustria ha ribadito in tutte le sedi istituzionali l'invito che lo stesso GDPR porge alle Istituzioni europee e nazionali di ***considerare le esigenze specifiche delle micro, piccole e medie imprese*** **nell'applicazione delle nuove regole** (Considerando 13), al fine di alleggerire il più possibile il peso dei nuovi adempimenti e individuare soluzioni "sostenibili" da parte degli operatori più piccoli.

Di seguito, alcune osservazioni sullo schema di Decreto Legislativo.

Osservazioni sullo schema di Decreto Legislativo

Con riferimento alla **tecnica legislativa**, Confindustria ha apprezzato la scelta di abrogare espressamente le norme del Codice privacy non compatibili con l'impianto delineato dal Regolamento. Tale approccio, ragionevole e moderno, a nostro avviso, assicura un migliore coordinamento normativo, nonché una maggiore certezza giuridica, agevolando l'operatore nell'analisi e nell'integrazione delle norme Ue e nazionali.

A tal fine, significativa è anche la clausola di salvaguardia *ex* art. 22, co. 1 che, nell'orientare al GDPR l'interpretazione delle norme dell'ordinamento italiano punta espressamente a evitare controversie e antinomie in sede applicativa.

Sempre nell'ottica di guidare gli operatori nella fase di transizione normativa, risulta meritoria anche l'indicazione nella Relazione illustrativa del provvedimento delle norme del Codice privacy rilevanti ai fini delle ordinarie attività di gestione aziendale (es. la comunicazione dei dati infragruppo, il trattamento dei dati provenienti dai pubblici registri), che possono rientrare nel concetto di legittimo interesse e, quindi, considerarsi "*assorbite*" dal Regolamento.

Quanto al **merito**, assolutamente positiva è la norma che attribuisce al Garante privacy la previsione di **misure di semplificazione per le MPMI** (art. 22, co. 10). A nostro avviso, questa disposizione rafforza il *commitment* pubblico sul tema ed evidenzia l'attenzione del Legislatore nazionale all'esigenza di alleggerire il carico degli adempimenti sugli imprenditori di piccole dimensioni.

Altrettanto positiva è la possibilità riconosciuta a titolari e responsabili del trattamento di **attribuire a determinate persone fisiche specifici compiti o funzioni** connessi al trattamento dei dati personali (nuovo art. 2-*terdecies* del Codice privacy). Tale misura, infatti, consente agli operatori di - continuare a - strutturare la filiera privacy interna e di adattarla alle esigenze e alle dimensioni dell'organizzazione.

Apprezzabile è anche la previsione di una **disciplina transitoria**, volta a:

- assicurare il riordino, previa consultazione pubblica, delle autorizzazioni generali del Garante privacy (art. 21);
- mantenere l'operatività dei provvedimenti dell'Autorità compatibili con il GDPR (art. 22, co. 4). In più occasioni, Confindustria ha rappresentato come i provvedimenti dell'Autorità (si pensi, ad esempio, a: Provvedimento 1 marzo 2007, recante le Linee Guida per l'utilizzo della posta elettronica e internet; Provvedimento 27 novembre 2008, in materia di amministratore di sistema; Provvedimento 8 aprile 2010, in materia di trattamento di dati personali effettuato tramite sistemi di videosorveglianza; Provvedimento 4 ottobre 2011 sui sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro; Provvedimento 12 novembre 2014 in tema di biometria) costituiscano un punto di riferimento certo per le imprese titolari del trattamento e come, quindi, risulti fondamentale un'attività di ricognizione e adeguamento degli stessi al Regolamento, soprattutto rispetto agli adempimenti che il GDPR ha soppresso (es. notificazione, istanza di verifica preliminare), al fine di chiarire i presidi cui fare riferimento e confermare le soluzioni compatibili e consolidate;
- definire in maniera rapida i procedimenti - compresi quelli sanzionatori - davanti all'Autorità (artt. 18 e 19).

Quanto alla **conferma delle misure di maggiore interesse per le imprese**, si valuta positivamente il mantenimento di:

- il regime privacy previsto per i dati contenuti nei CV spontaneamente inviati (nuovo art. 111-*bis* del Codice privacy);
- l'autorizzazione normativa al trattamento dei dati "giudiziari" effettuato in attuazione di protocolli d'intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata. Sul punto, lo schema di decreto rinvia a un Decreto del Ministro della Giustizia da adottarsi entro 18 mesi (nuovo art. 2-*octies*, co. 6 del Codice privacy) e nelle more autorizza il trattamento direttamente (art. 22, co. 13). Tale previsione, compatibile con il GDPR che consente agli Stati membri di autorizzare *ex lege* il trattamento di dati giudiziari (art. 10 del GDPR) assume notevole rilevanza per l'implementazione del Protocollo di legalità che Confindustria ha stipulato con il Ministero dell'Interno al fine di rafforzare la collaborazione tra imprese e istituzioni nella lotta alle infiltrazioni della criminalità organizzata nell'economia.

Sebbene si auspicasse la mancata introduzione di ulteriori condizioni per il trattamento dei dati relativi alla salute, dei dati biometrici e dei dati genetici (art. 2-*septies*), si condivide la scelta di sottoporre a consultazione pubblica le misure di garanzia individuate dal Garante privacy.

Il **coinvolgimento dei soggetti interessati**, che si rinviene in altre norme dello schema di decreto (es. nuovo art. 2-*quater* del Codice privacy, in tema di regole deontologiche), costituisce una pratica assolutamente valida, che recepisce una

positiva esperienza registrata in materia a livello Ue con riferimento alle Linee Guida sul GDPR del Gruppo di lavoro articolo 29 per la protezione dei dati (cd. WP29).

Quanto ai profili che destano **preoccupazione**, si evidenzia in primo luogo quello **sanzionatorio**.

Con riferimento al fronte **amministrativo**, il GDPR ha rafforzato molto l'impianto sanzionatorio, prevedendo sanzioni amministrative pecuniarie elevate, che possono arrivare fino al 4% del fatturato mondiale totale annuo (ad esempio, in caso di inosservanza degli ordini del Garante privacy o di violazione dei principi di base del trattamento, dei diritti degli interessati, delle regole per il trasferimento dei dati in Paesi extra UE).

In base alla giurisprudenza della Corte europea dei diritti dell'uomo, sanzioni amministrative pecuniarie così elevate e incisive denotano una valenza afflittiva assimilabile, ai fini delle garanzie, a quella delle sanzioni penali.

Pertanto, in linea con quanto già previsto in altri settori in cui Autorità amministrative indipendenti irrogano rilevanti sanzioni amministrative (es. Consob, Banca d'Italia, IVASS), sarebbe opportuno stabilire che i procedimenti di controllo a carattere contenzioso e sanzionatori per violazione della normativa privacy siano *svolti nel rispetto dei principi della piena conoscenza degli atti istruttori, del contraddittorio, della verbalizzazione nonché della distinzione tra funzioni istruttorie e funzioni decisorie rispetto all'irrogazione della sanzione* (sul punto, v. art. 24, legge n. 262/2005).

Quanto all'**ambito penale**, a fronte della natura sussidiaria dei reati preposti alla tutela del dato personale *("salvo che il fatto non costituisca reato più grave")*, dello scarso ricorso negli anni agli stessi, del citato irrigidimento della responsabilità amministrativa operato dallo stesso GDPR e dal conseguente rischio di violare il principio del *ne bis in idem*, Confindustria auspicava e auspica ancora in un approccio di depenalizzazione che, peraltro, alcune prime versioni dello schema di decreto avevano adottato.

Tuttavia, lo schema di decreto interviene in materia penale, riscrivendo, tra l'altro, il reato del "trattamento illecito dei dati" *ex* art. 167 del Codice privacy e introducendo i nuovi reati di "comunicazione e diffusione illecita di dati personali riferibili a un rilevante numero di persone" e di "acquisizione fraudolenta di dati personali" (nuovi artt. 167-*bis* e 167-*ter* del Codice privacy). Quanto a questi ultimi nuovi reati, si sottolinea come entrambe le fattispecie, nel fare riferimento al generico concetto di "rilevante" numero di persone, rischino di violare il principio di tassatività in materia penale.

Ulteriore elemento di criticità è rappresentato dalla scelta di fissare a 16 anni la soglia minima di età ai fini della validità del **consenso espresso dal minore** al trattamento dei dati nell'ambito dei servizi della società dell'informazione. A nostro avviso sarebbe più coerente con la realtà fattuale e con una *policy* volta a supportare la digitalizzazione abbassare la soglia a 14 anni, come peraltro

proponevano alcune prime versioni dello schema di decreto. In particolare, il limite dei 16 anni rischia di scoraggiare proprio la creazione di servizi più adatti agli adolescenti sotto i 16 anni, creando così un disservizio e rendendo più difficoltoso l'accesso alla maggior parte dei servizi *online* (es. istruzione, *e-mail*, *e-commerce*, accesso a servizi di sostegno socio-psicologico).

Infine, si pone l'attenzione sulle norme contenute nella Legge di Bilancio 2018 (art. 1, commi da 1022 a 1023, legge n. 205/2017) in tema di trattamenti finalizzati al perseguimento di un interesse legittimo del titolare e realizzati con strumenti tecnologici. Confindustria condivide l'abrogazione di tali misure che, nel prevedere un controllo preliminare del Garante privacy, risultano incompatibili con il principio dell'*accountability* e l'impianto delineato dal GDPR. Tuttavia, con una norma interpretativa, lo schema di decreto mantiene l'applicazione di queste misure, nei limiti e con le modalità di cui all'art. 36 del GDPR, per i trattamenti dei dati di minori raccolti *online*. A fronte delle predette incompatibilità delle norme previste dalla Legge di Bilancio 2018, occorrerebbe valutare con maggiore attenzione l'opportunità della loro "reviviscenza", nonché la loro riconducibilità alla categoria dei trattamenti finalizzati all'esecuzione di un compito di interesse pubblico che, ai sensi dell'art. 36, co. 5 GDPR giustificano la previsione di un controllo abilitativo dell'Autorità.