centro nazionale
DI DOCUMENTAZIONE E ANALISI PER L'INFANZIA E L'ADOLESCENZA

Regolamento generale sulla protezione dei dati

Approfondimento

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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)

Dal **25 maggio 2018** si applica in tutti gli Stati membri dell'Unione europea il nuovo **Regolamento europeo generale sulla protezione dei dati** (chiamato più semplicemente *GDPR-General Data Protection Regulation*) che abroga la Direttiva 95/46/CE. In Italia, esso va a sostituire il Codice in materia di protezione dei dati personali, approvato con il Decreto legislativo n.196 del 30 giugno 2003. Sostanzialmente sono introdotte **regole più chiare in materia di informativa e di consenso** e sono definiti i limiti riguardanti il trattamento automatizzato dei dati personali. Vengono, inoltre, poste le basi per l'esercizio di **nuovi diritti** e stabiliti dei **criteri rigorosi** in caso di trasferimento dei dati al di fuori dell'Unione europea e per i casi di violazione dei dati personali. Il Regolamento è **direttamente applicabile** in tutti gli Stati membri dell'Unione europea, è **vincolante** e **non richiede una legge di recepimento nazionale**. Si applica integralmente anche a quelle imprese presenti su territori non facenti parte dell'Unione europea, le quali offrono servizi o prodotti a persone che si trovano invece sui territori degli Stati membri. È chiaro dunque che le aziende, ovunque stabilite, che abbiano a che fare con l'UE dovranno rispettare queste nuove regole.

È importante, innanzitutto, chiarire quali siano l'oggetto e le finalità del regolamento. Così come affermato all'**articolo 1**, **esso stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché le norme relative alla libera circolazione di tali**

dati. Sono dunque protetti i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. Non può esserci nell'Unione, in relazione alla loro libera circolazione, una limitazione o un divieto per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Agli **articoli 2 e 3** vengono definiti, rispettivamente, l'**ambito di applicazione materiale** e quello di **applicazione territoriale.** In riferimento al primo vediamo che il regolamento si applica al **trattamento automatizzato**, sia esso per **intero** o **parziale**, di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a esservi contenenuti. Relativamente al secondo ambito, si specificano i **tre casi** in cui che esso viene applicato: 1) trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione; 2) trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano sia l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; sia il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione; 3) trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Fatte le opportune precisazioni relative agli ambiti di applicazione, imprescindibili per comprendere la porta del nuovo regolamente, è fondamentale avere ben chiari i **principi applicabili al trattamento dei dati personali**, espressi all'**articolo 5**, che possiamo riassumere in: liceità, correttezza e trasparenza; limitazione, cioè raccolti solo per finalità determinate; minimizzazione dei dati, cioè adeguati e limitati a quanto necessario per le finalità per le quali sono trattati; esattezza; limitazione della conservazione, cioè conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore al conseguimento, salvo l'eccezione

dell'archiviazione più lunga nel pubblico interesse, delle finalità per le quali sono trattati; integrità e riservatezza, cioè trattati in modo tale da garantirne una sicurezza adeguata, attraverso valide misure tecniche e organizzative; responsabilizzazione, intesa come competenza del titolare al rispetto ai punti precedenti ed è in grado di comprovarli. Il **trattamento dei dati deve essere lecito** e all'**articolo 6** sono **precisate le condizioni**, in presenza di almeno una delle quali, può essere considerato tale.

Uno dei punti fondamentali è certamente rappresentato dal **consenso**, per il quale sono stabilite le condizioni nell'**articolo 7**, e alle sue modalità di espressione. Il consenso dovrà essere dato **preventivamente** e in maniera **inequivocabile**, anche quando debba essere espresso attraverso le modalità presenti nel Web, come, ad esempio, la selezione di una casella su un sito. Una precisazione va fatta relativamente ai **dati sensibili**, in presenza dei quali, il consenso deve essere **necessariamente esplicito**. Si vanno ad escludere in questo modo tutte le forme tacite, come ad esempio il silenzio, nonchè quelle che ottengono il consenso in seguito alla proposta fatta all'interessanto di una serie di opzioni già selezionate in precedenza. Il consenso potrà essere **revocato** in ogni momento, ma i trattamenti effettuati fino a quel momento dal titolare, sulla base del consenso espresso in precedenza, rimarranno comunque legittimi.

Per quanto riguarda i **minori**, vediamo che all'**articolo 8** del regolamento sono disciplinate le condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione. I fornitori di servizi Internet e i social media, dovranno richiedere il **consenso ai genitori o a chi esercita la responsabilità genitoriale** per trattare i dati personali dei **minori di 16 anni**, altrimenti il consenso non può essere considerato lecito. Tuttavia **si consente agli Stati membri di stabilire**, con una legge nazionale, un'**età inferiore** a tali fini **purché non inferiore ai 13 anni**. Il titolare del trattamento, in ogni modo ragionevole, deve adoperarsi per accertare che il consenso, nei casi di età inferiore a quella stabilità sia effettivamente dato dal titolare della responsabilità sul minore, in considerazione delle tecnologie disponibili. **L'attenzione particolare rivolta ai minori nel presente regolamento risulta essere di primaria importanza**. Si afferma, infatti, nelle considerazioni iniziali al **punto 38** che "***i minori meritano una specifica protezione relativamente ai loro dati personali,***

in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali *. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore".* Vediamo, inoltre, la previsione contenuta nell'**articolo 12** dell'obbligo di garantire che le informazioni fornite agli interessati siano concise, trasparenti e in linguaggio semplice sia soddisfatto ***"in particolare nel caso di informazioni destinate specificamente ai minori"***. Proprio in relazione a ciò, ricordiamo anche il **punto n. 5**8 delle già citate considerazioni iniziali, in cui si afferma che i minori meritano una protezione particolare "***quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa facilmente capire***".

Vanno posti in evidenza, inoltre, gli **articoli 13 e 14** riguardanti le **informazioni** da fornire rispettivamente nel caso in cui i dati personali siano raccolti presso l'interessato o nel caso in cui i dati personali non siano stati ottenuti presso l'interessato. I **contentuti dell'informativa** sono **elencati in modo tassativo** nei suddetti articoli e risultano essere più ampi rispetto al Codice precedente. In relazione alla seconda tipologia di raccolta, chiarisce l'articolo 14, il titolare del trattamento "*deve fornire entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati; nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali*".

L'**articolo 12**, stabilisce che il titolare del trattamento debba adottare **delle misure appropriate al fine di fornire all'interessato sia le comunicazioni**, delle quali si tratta in alcuni altri articoli del regolamento, **sia tutte le informazioni** alle quali fanno riferimenti gli articoli 13 e 14 esaminati

poco sopra. Esse, fornite **per iscritto** (o se richiesto dall'intereassato anche oralmente purchè sia comprovata l'identità dello stesso cona ltri mezzi) o con **altri mezzi** che possono essere anche di tipo elettronico, devono essere in forma concisa concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso in cui i destinatari delle informazioni siano dei minori - come già detto in precedenza. Il **termine** fissato per dare la risposta all'interessato è di **un mese** e può essere esteso **fino a tre mesi** in alcuni casi particolarmente complessi. Qualora ritenga la richiesta eccessiva o manifestamente infondata, spetta al titolare del trattamento l'onere di dimostralo.

Il **diritto di accesso** è invece disciplinato dall'**articolo 15**. Si stabilisce che l'interessato ha il diritto di ottenere la conferma, da parte del titolare, che sia in corso il trattamento dei suoi dati personali, nonchè ad ottenere l'accesso agli stessi e a tutte le informazioni specificamente indicate nel testo dell'articolo stesso. In caso di trasferimento dei dati ad un paese terzo o a un'organizzazione internazionale, deve essere garantita all'interessato la presenza di adeguate garanzie in relazione al trasferimento stesso. Una **copia** dei dati personali trattati deve essere data all'interessato.

Un punto di fondamentale importanza nel testo è, inoltre, l'**articolo 17** in cui si tratta il **diritto alla cancellazione**, anche detto *diritto all'oblio*. Come affermato chiaramente dal Garante per la protezione dei dati personali, si tratta di un *diritto alla cancellazione rafforzato* in capo all'interessato, poichè è previsto un **obbligo per i titolari del trattameento** – qualora abbiano reso pubblici i dati in questione, ad esempio attraverso un sito web - **di informare della richiesta di cancellazione**, attraverso l'adozione di misure ragionevoli e tenendo conto della tecnologia disponibile e dei costi di attuazione, **anche gli altri titolari che trattano i medesimi dati**, compresi qualsiasi link, copia o riproduzione degli stessi. Il **campo di applicazione** risulta essere **più esteso** rispetto a quello del vecchio "*Codice privacy*" e si ha diritto di ottenere la cancellazione dei dati personali in presenza dei seguenti **motivi**, elencati nel primo paragrafo dell'articolo 17: i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; l'interessato revoca, in conformità al regolamento stesso, il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento; l'interessato si oppone

leggittimamente al trattamento, secondo quanto previsto dall'articolo 21 del regolamento stesso e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; i dati personali sono stati trattati in maniera illecita; i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8 riguardante i minori.

Un importante diritto introdotto dal regolamento è la cosiddetta **portabilità dei dati**. All'**articolo 20** si stabilisce, infatti, che l'interessato ha il diritto di ricevere i dati personali che lo riguardano, già forniti a un titolare del trattamento, in un formato che sia strutturato e di uso comune nonchè leggibile da dispositivo automatico. Egli ha, inoltre, il diritto di **trasmetterli a un altro titolare** del trattamento senza alcun impedimento da parte del titolare precedente. Tutto ciò qualora il trattamento si basi sul consenso dato nei casi esplicitati nel testo dell'articolo stesso e qualora il trattamento sia effettuato con mezzi automatizzati – quindi non si applica agli archivi o registri cartacei.

Evidenziamo, inoltre, gli articoli che disciplinano la **sicurezza dei dati personali**. All' **articolo 32** si afferma che il titolare e il responsabile del trattamento devono mettere in atto **misure tecniche e organizzative** che siano realmente valide per garantire un **livello di sicurezza adeguato al rischio**. L' **articolo 33** stabilisce l'**obbligo di notifica alla competente autorità di controllo**, a carico del titolare del trattamento, nel caso di una violazione dei dati personali. La notifica deve essere fatta senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. L' **articolo 34** impone invece l'**obbligo per il titolare** del trattamento, senza ingiustificato ritardo, di una **comunicazione all'interessato in caso di violazione** dei dati dello stesso. Ciò quando la violazione può rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Il nuovo regolamento si concentra particolarmente sulla cosidetta ***accountability***, ossia sulla **responsabilizzazione dei titolari e dei responsabili del trattamento**. Ciò attraverso l'adozione di un insieme di **comportamenti idonei** a dimostrare l'adozione di misure che abbiano come fine quello di assicurare la **corretta applicazione del regolamento**. In generale l'intero Capo IV del regolamento è dedicato a questo e, sottolineiamo più in particolare, l' **articolo 25** che esprime il criterio cosiddetto "***data protection by defalut and by design***". In riferimento al primo si intende la tutela dei dati fin dalla fase di progettazione, sviluppo, selezione e utilizzo di applicazioni, servizi o prodotti che si basano sul trattamento di dati personali o che li trattano per svolgere le loro funzioni.

Mentre, con il secondo, si vuole indicare la tutela della vita privata *"per impostazione predefinita"*, cioè di default. Il titolare del trattamento, a tutela della protezione dei dati, dovrebbe adottare politiche interne e attuare misure tecniche e organizzative adeguate. Si chiarische infatti che, tenendo conto di vari fattori, *"sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati"*-. La stessa previsione, all'**articolo 37**, dell'obbligo di designazione di un **responsabile della protezione dei dati** riflette la volontà del legislatore europeo di attuare un approccio "responsabilizzante".

È importante, inoltre, porre l'accento sugli articoli **dal 40 al 43** nei quali si prevede l'adozione di **Codici di condotta** da parte di associazioni di categoria e altri soggetti, sottoposti all'approvazione dell'Autorità nazionale di protezione dei dati, che abbiano come obiettivo quello di contribuire alla corretta applicazione dei contenuti del Regolamento stesso *"in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese"*.

Quanto fin qui esposto rappresenta alcuni degli aspetti principali e innovativi del nuovo Regolamento. Certamente a livello di ordinamento nazionale, l'impatto delle nuove disposizioni

sarà forte e, in alcuni casi, di complessa interpretazione. In riferimento ai minori, per ciò che in particolare ci interessa, vedremo come il legislatore italiano deciderà di adeguare la normativa interna in relazione all'età minima del consenso al trattamento dei dati stabilita dal nuovo Regolamento, se deciderà di mantenere la soglia dei 16 anni o se, come consentito, deciderà di abbassarla. Sarà questo oggetto di ulteriori approfondimenti sul tema.

Carla Mura