



Approvato il nuovo regolamento generale per la protezione dei dati
personali nell'UE
Mariacristina Bottino

Il 14 aprile 2016 il Parlamento europeo ha [approvato](#), in seduta plenaria, il testo della [posizione](#) adottata in prima lettura dal Consiglio dell'UE sulla proposta di regolamento concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), nonché il testo della [posizione](#) adottata in prima lettura dal Consiglio sulla proposta di direttiva sul trattamento dei dati a fini di attività di contrasto ([comunicato stampa](#)).

L'approvazione di tali testi (disponibili ad oggi in sola lingua inglese) costituisce l'ultimo atto di un lungo *iter* legislativo che ha preso avvio nell'ormai lontano 25 gennaio 2012, quando la Commissione europea, nell'intento di rafforzare i diritti della *privacy online* e stimolare l'economia digitale europea, presentava un pacchetto di proposte legislative di riforma della [direttiva 95/46/CE](#) sulla protezione dei dati personali, pacchetto composto dalla [proposta di regolamento](#) generale sulla protezione dei dati nonché dalla [proposta di direttiva](#) sul trattamento dei dati a fini di attività di contrasto.

In particolare, l'approvazione del testo del regolamento in plenaria è stata preannunciata dalla [comunicazione](#) della Commissione europea e della [raccomandazione](#) della commissione Libertà Civili, Giustizia e Affari Interni del Parlamento europeo con le quali le due istituzioni hanno formalmente approvato i risultati dei negoziati e accettato la posizione del Consiglio.

Il nuovo regolamento, che entrerà in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale dell'UE e sarà applicabile nei 28 Stati membri dell'UE decorsi due anni da tale data, abroga la direttiva 95/46/CE, introducendo un *corpus* unico di norme, di diretta applicazione, valido per tutta l'UE.

Nelle more della pubblicazione in Gazzetta Ufficiale dell'UE del testo definitivo del regolamento e dell'accesso alla versione italiana dello stesso, si segnalano di seguito - senza alcuna pretesa di esaustività - alcune delle principali novità introdotte dal nuovo atto normativo, il cui articolato è il frutto di un lavoro di limatura certosino del testo della proposta della Commissione europea condotto in seno al trilogico interistituzionale.

Ebbene, qualche novità si registra nel contesto delle definizioni rilevanti ai fini



Approvato il nuovo regolamento generale per la protezione dei dati
personali nell'UE
Mariacristina Bottino

dell'interpretazione ed applicazione del regolamento. Tra queste, particolare rilievo rivestono le definizioni di "dati personali" e di "trattamento dei dati", che il legislatore UE parzialmente precisa e chiarisce rispetto alle corrispondenti definizioni di cui alla direttiva 95/46/CE. Viene altresì precisata la nozione di "consenso" quale presupposto imprescindibile della liceità del trattamento dei dati, chiarendo che lo stesso deve essere espresso in modo libero, specifico, informato, nonché inequivocabile (art. 4(11)). Confermato invece il divieto di trattamento di dati sensibili idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, le condizioni di salute e le abitudini sessuali, fermo restando le deroghe di cui all'art. 9 fondate su esigenze relative tanto alla necessità del trattamento, quanto la sua specifica finalità.

Il regolamento introduce inoltre un *set* di norme volte a rafforzare i diritti delle persone fisiche, nonché ridurre gli oneri amministrativi che gravano sulle imprese.

In tale prospettiva vanno lette innanzitutto le disposizioni intese ad assicurare all'interessato un accesso facilitato ai propri dati personali (art. 15), il diritto di revocare in qualsiasi momento il consenso al trattamento dei dati (art. 7), nonché il diritto alla ratifica (art. 16), il diritto - sia pure non privo di eccezioni - alla cancellazione (c.d. "diritto all'oblio"), dei dati oggetto di trattamento (art. 17), nonché alla limitazione (art. 18) del trattamento medesimo. Tra le norme più innovative a tutela degli individui si segnalano altresì quelle intese a riconoscere il diritto alla portabilità dei dati da un prestatore di servizi a un altro (art. 20), nonché il diritto di obiezione, anche riguardo all'uso dei dati personali a fini di "profilazione", intendendosi per tale «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare aspetti della personalità dell'interessato, in particolare per analizzare e prevedere aspetti riguardanti il rendimento professionale, la situazione economica, lo stato di salute, le preferenze personali o gli interessi, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti» (art. 4(4)).

Quanto ai benefici a favore delle imprese, una norma *ad hoc* (art. 25) impone ai responsabili del trattamento dei dati obblighi di protezione fin dalla progettazione e di protezione di *default* (c.d. *data protection by design and by default*), richiedendo - tenuto conto della



Approvato il nuovo regolamento generale per la protezione dei dati
personali nell'UE
Mariacristina Bottino

tecnologia disponibile e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, così come della probabilità e della gravità del rischio derivante dal trattamento per i diritti e le libertà delle persone fisiche - l'adozione di misure tecniche e organizzative adeguate all'attività del trattamento e dei suoi obiettivi, quali la minimizzazione e la pseudonimizzazione dei dati. Ciò, al fine di tutelare i diritti dell'interessato nonché garantire, *inter alia*, che siano trattati, di *default*, solo i dati personali necessari per ogni specifica finalità del trattamento.

Titolari o responsabili del trattamento dei dati hanno altresì l'obbligo di rendicontazione quando un trattamento presenta rischi specifici per i diritti e le libertà degli interessati. In tal caso, infatti, il regolamento prevede che, prima di procedere al trattamento dei dati, gli stessi effettuino una "valutazione d'impatto" (art. 35) del trattamento e procedano a una "consultazione preventiva" dell'autorità di controllo competente (art. 36). Viene abolito invece l'obbligo di notifica preventiva del trattamento dei dati personali alle autorità di controllo, già previsto dalla direttiva 95/46/CE. In base al nuovo regolamento, infatti, tale obbligo di notifica sorge solo successivamente alla constatazione di una violazione dei dati personali, suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, violazione che dovrà essere comunicata anche all'interessato, senza ingiustificato ritardo (art. 33).

Tra le novità più rilevanti in tema di controllo della corretta applicazione del regolamento a beneficio delle imprese, si segnala l'istituzione del c.d. sportello unico ("*one-stop-shop*"): il regolamento prevede, invero, per la prima volta (art. 56), che quando il responsabile o l'incaricato del trattamento ha sede in più Stati membri dell'UE, l'autorità di controllo competente a sorvegliare la corretta e coerente applicazione del regolamento sia l'autorità di controllo dello Stato membro in cui il responsabile o l'incaricato ha il proprio stabilimento principale (c.d. autorità di controllo "capofila"). Il nuovo regolamento contempla inoltre la creazione di un comitato europeo per la protezione dei dati (art. 68) composto dal responsabile delle autorità di controllo di ciascuno Stato membro e dal garante europeo della protezione dei dati. Chiamato a svolgere attività di indirizzo, monitoraggio, consultazione e supporto alle autorità nazionali competenti in materia di protezione dei dati,



Approvato il nuovo regolamento generale per la protezione dei dati
personali nell'UE
Mariacristina Bottino

al fine di garantire un'uniforme applicazione del regolamento, il comitato sostituisce il "Gruppo di Lavoro Articolo 29", istituito dalla direttiva 95/46/CE. I membri della Commissione europea, nonché il garante europeo della protezione dei dati possono partecipare, senza diritto di voto, alle riunioni del comitato.

Nell'ottica di rafforzare la sicurezza dei dati, il regolamento attribuisce alle autorità nazionali indipendenti di protezione dei dati poteri di controllo e sanzionatori più incisivi (artt. 77-84). Tali autorità potranno invero comminare, alle imprese che violano il regolamento, sanzioni pecuniarie corrispondenti ad importi fissi oppure commisurate al volume d'affari delle imprese coinvolte nella violazione del regolamento. Tali sanzioni, che dovranno essere effettive, proporzionate e persuasive, dovranno altresì tener conto della natura del trattamento dei dati in occasione del quale è stata commessa la violazione, del contesto in cui la violazione è avvenuta e dell'intenzionalità della condotta contraria alle disposizioni normative.

Infine, si segnala l'incoraggiamento all'elaborazione di codici di condotta (art. 40) destinati a contribuire alla corretta applicazione del regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese: le associazioni e gli altri organismi rappresentanti le categorie di responsabili del trattamento o incaricati del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione delle disposizioni del regolamento, sottoponendo il progetto di codice all'autorità di controllo competente, o all'organismo da questa accreditato, la quale esprimerà un parere ed approverà il progetto di codice qualora lo stesso rispetti i requisiti previsti dal regolamento.