

D.Lgs. n. 101/2018

## Privacy: il legislatore italiano si adegua al GDPR

Monica Lambrou - Avvocato

Con il Decreto legislativo 10 agosto 2018, n. 101 il legislatore ha finalmente provveduto ad adeguare la disciplina interna in materia di privacy, in seguito all'entrata in vigore del Regolamento Ue 2016/679 e delle relative novità. Come noto, la recente - e rivoluzionaria - normativa europea, immediatamente applicabile anche nell'ordinamento italiano a partire dal 25 maggio 2018, aveva introdotto una serie di nuovi e inediti principi per un corretto e trasparente trattamento dei dati personali, nonché, tra gli altri, previsto una serie di pesanti sanzioni a carico delle imprese che ne violassero le disposizioni.

Ebbene, con il definitivo riordino della normativa nazionale, dapprima totalmente fondata sulle prescrizioni di cui al Codice della Privacy (Decreto legislativo 30 giugno 2003, n. 196), le imprese non possono più ritardare l'adeguamento delle proprie *policy* interne nella gestione dei dati personali, come, peraltro, recentemente osservato dal dirigente del Garante per la protezione dei dati personali.

Il legislatore italiano parrebbe, in ogni caso, essere intervenuto non in modo sufficientemente tempestivo, posto che le prime versioni del Decreto di adeguamento risalgono ad un periodo di gran lunga precedente all'entrata in vigore del Regolamento europeo, a ciò conseguendo la generalizzata incertezza interpretativa che ha caratterizzato gli ultimi mesi.

Da una prima lettura dell'intervento legislativo, si nota, in primo luogo, l'astensione dalla scelta di abrogare definitivamente il vecchio Codice della Privacy. Tale eventualità aveva, invero, acquisito una discreta concretezza nei dibattiti e nelle prime versioni del Decreto. Una tecnica normativa che prevedesse un totale superamento della disciplina previgente avrebbe permesso, secondo taluno, il conseguimento di obiettivi di certezza e uniformità interpretativa - in una logi-

ca maggiormente razionale -, senza infirmare l'effettività della tutela giuridica.

In ogni caso - e pur in assenza di una completa abrogazione - può dirsi che il legislatore abbia operato un pregnante *restyling* del Codice nelle sue parti fondamentali. In particolare, sono oggetto di totale superamento (perché abrogate espressamente), tra le altre:

- le norme generali in tema di principi, definizioni e ambito di applicazione;
- le disposizioni sui diritti riconosciuti all'interessato e le relative modalità di esercizio;
- le regole generali sul trattamento dei dati (anche sensibili), sulle informative, sul consenso dell'interessato, sulle misure di sicurezza e sui soggetti che effettuino detto trattamento;
- le regole in materia di adempimenti (notificazione, obblighi di comunicazione, ecc.) e di trasferimento dei dati in Paesi terzi;
- talune norme specifiche in tema di trattamenti in ambito pubblico;
- talune norme specifiche in tema di trattamenti in ambito sanitario e di dati genetici;
- la quasi totalità delle disposizioni in materia di sanzioni.

### Il ruolo del Garante per la protezione dei dati personali

Analizzando nello specifico le novità introdotte dal D.Lgs. n. 101/2018 si segnala, in primo luogo, l'attribuzione di nuove e più ampie competenze al Garante per la protezione dei dati personali. L'Autorità, infatti, oltre ad essere onerata degli svariati compiti ad essa attribuiti dal Regolamento europeo, cui si devono, in particolare, atti di natura amministrativa e giurisdizionale dovrà, altresì, provvedere all'emanazione di provvedimenti specifici per il trattamento di categorie particolari di dati (genetici, biometrici e relativi alla salute) e ad individuare con cadenza almeno

# Approfondimenti

biennale specifiche misure di sicurezza in tal senso. È, per di più, demandata alla stessa autorità l'adozione di linee guida che promuovano, in favore delle micro, piccole e medie imprese, "modalità semplificate" di adempimento degli obblighi del titolare del trattamento (art. 154-bis, D.Lgs. n. 196/2003, come modificato dal D.Lgs. n. 101/2018).

Lo stesso Garante sarà, poi, chiamato ad operare di concerto con l'Autorità per le garanzie nelle comunicazioni (l'Agcom) per definire regole appropriate in materia di inserimento - e conseguente utilizzo - dei dati personali all'interno degli elenchi telefonici e, in linea generale, dovrà promuovere le regole deontologiche alla base dei trattamenti.

Peraltro, va detto che, a norma dell'art. 22, c. 4 la totalità dei provvedimenti già emessi dal Garante a decorrere dal 25 maggio 2018 "continuano ad applicarsi, in quanto compatibili con il... regolamento e con le disposizioni del... Decreto". A ciò si aggiunga, da ultimo, la configurazione, a norma degli artt. 140-bis, 141, 142, 143 del reclamo al Garante come forma di tutela alternativa rispetto al ricorso al Tribunale.

## Le sanzioni di natura amministrativa

Le novità più attese dai commentatori riguardavano le disposizioni in merito alle sanzioni da applicare in caso di violazioni. Come previsto, si registra un definitivo superamento di qualsivoglia sanzione amministrativa precedentemente disciplinata dal Codice del 2003. Per chi violi la normativa (interna o europea) sulla privacy, quindi, troverà applicazione esclusivamente il significativo apparato sanzionatorio di cui al Regolamento Ue 2016/679 e, quindi, si sottolinea, fino a euro 10.000.000 (ovvero fino al 2% del fatturato mondiale totale annuo per le imprese) ove la violazione riguardi: le condizioni applicabili al consenso dei minori, i trattamenti non richiedenti l'identificazione dell'interessato, l'intera disciplina dei titolari del trattamento e dei responsabili della protezione, le norme sulla sicurezza dei dati e sulla certificazione; fino a euro 20.000.000 (ovvero fino al 4% del fatturato mondiale totale annuo per le imprese) ove la violazione riguardi: i principi di base del trattamento, i diritti degli interessati, il trasferimento dei dati a destinatari di Paesi terzi o organizzazioni internazionali, l'inos-

servanza di un ordine o limitazione posto dal Garante per la protezione dei dati personali.

Tuttavia, con un'incerta prescrizione, il legislatore si preoccupa di specificare, all'art. 22, punto 13 del D.Lgs. n. 101/2018, come "per i primi otto mesi dalla data di entrata in vigore" del Decreto in oggetto "il Garante per la protezione dei dati personali" tenga conto, ai fini dell'applicazione delle sanzioni amministrative di cui sopra "della fase di prima applicazione delle disposizioni sanzionatorie". Il significato della norma ha sin da subito suscitato perplessità nelle letture degli interpreti. Si tratta di una sospensione del periodo di operatività delle sanzioni?

La genericità lessicale adottata e il carattere di auto-applicabilità del Regolamento europeo parrebbero privare di fondamento una simile interpretazione. Ad ogni modo, non v'è dubbio che la norma imponga al Garante, in fase di irrogazione e per il periodo in oggetto (sino al 19 maggio 2019), di prestare particolare attenzione nella valutazione delle circostanze del caso concreto e di optare per misure meno pregnanti o, eventualmente, graduare gli importi delle sanzioni pecuniarie sulla base delle possibili - ed iniziali - difficoltà di adeguamento ai nuovi meccanismi di gestione dei dati da parte delle imprese. L'Autorità di controllo parrebbe, con ciò, incentivata a livello legislativo - e almeno in questa fase - a preferire, ove possibile, l'adozione degli strumenti alla stessa offerti dall'art. 58, Reg. 2016/679, tra cui l'avvertimento, l'ammonimento, l'ingiunzione, l'imposizione di limitazioni, l'ordine di rettifica, cancellazione, limitazione, ecc.

## Le nuove fattispecie penali

Come noto, il Regolamento europeo ha demandato, sotto il profilo penale, agli Stati membri la valutazione circa l'opportunità di sanzionare talune condotte in materia di trattamento dei dati con l'introduzione di specifiche fattispecie di reato. Trattasi di una facoltà di cui il legislatore italiano, in coerenza con le scelte effettuate nel 2003, ha deciso di avvalersi, talvolta abrogando *in toto* e talvolta modificando le norme penali di cui al D.Lgs. n. 196/2003.

In particolare, nel continuare a disciplinare all'art. 167 l'ipotesi canonica del trattamento illecito di dati ("punito con la reclusione da sei mesi

a un anno e sei mesi”), il Decreto introduce nuovi e inediti reati.

Nello specifico, il nuovo art. 167-*bis* punisce la comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala. Allo stesso tempo, è punito con la reclusione da uno a quattro anni chiunque “*acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala*” (art. 167-*ter*, D.Lgs. n. 196/2003, introdotto dall’art. 15, D.Lgs. n. 101/2018). Il modificato art. 168, poi, oltre a continuare a sanzionare la falsità nelle dichiarazioni e notificazioni al Garante, perpetrata, appunto, per mezzo di false attestazioni di notizie e circostanze o produzione di atti e documenti innanzi all’Autorità di controllo, con la pena della reclusione da sei mesi a tre anni, punisce altresì (con la reclusione sino ad un anno) chiunque intenzionalmente cagioni “*un’interruzione*” o turbi “*la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti*”.

Si osserva, da ultimo, che in materia di rapporto di lavoro e, in particolare, di divieto di controlli a distanza e indagini sulle opinioni dei dipendenti, per espressa previsione dell’art. 171, D.Lgs. n. 196/2003 come modificato dall’art. 15, D.Lgs. n. 101/2018, in caso di violazioni continuerà a trovare applicazione la sanzione penale di cui all’art. 38, legge 20 maggio 1970, n. 300 (c.d. Statuto dei lavoratori) che consta in un’ammenda, ovvero nell’arresto da 15 giorni a un anno.

Sostanzialmente invariata rimane, altresì, la fattispecie di cui all’art. 170 sull’inosservanza di provvedimenti emessi dal Garante per la protezione dei dati personali.

Occorre, peraltro, sottolineare come, in forza dell’art. 24, Decreto, agli illeciti “depenalizzati” dallo stesso e commessi prima della sua entrata in vigore (19 settembre 2018) si applicano le sanzioni amministrative in luogo di quelle penali.

## Le novità in materia di gestione dei “curricula”

La gestione dei *curricula* inviati direttamente - e spontaneamente - dai candidati in favore delle imprese rappresenta un’operazione senz’altro delicata, in considerazione delle svariate tipologie di dati personali in essi contenuti. In tal senso, se

non può prescindersi in linea generale dalla configurazione di una forma di tutela anche per dette informazioni, ragioni di praticità e la necessità di rendere meno gravosi gli adempimenti già di per sé rilevanti posti in capo alle imprese, hanno spinto il legislatore alla previsione di disposizioni specifiche.

L’aspetto, in tal senso, più preoccupante riguardava la trasmissione dell’informativa e l’acquisizione del consenso, rese particolarmente difficoltose dalla volontarietà della comunicazione di dati da parte del candidato all’assunzione e dall’immediatezza della stessa. Orbene, a norma del nuovo art. 111-*bis*, introdotto dall’art. 9, D.Lgs. n. 101/2018, è prescritto che le innumerevoli informazioni di cui all’art. 13, Regolamento Ue 2016/679, ove appunto i *curricula* vengano “*spontaneamente trasmessi dagli interessati*” al fine dell’instaurazione di un rapporto di lavoro, possano essere fornite da parte del titolare “*al momento del primo contatto utile, successivo all’invio del curriculum medesimo*”. Peraltro, configurandosi in detta circostanza l’attributo della necessità del trattamento “*all’esecuzione di un contratto*” o “*all’esecuzione di misure precontrattuali*” di cui all’art. 6, par. 1, lett. b), non è dovuto alcun consenso specifico da parte dell’interessato.

## I diritti delle persone decedute

L’art. 2-*terdecies* interviene, poi, sulle modalità di esercizio dei diritti, in merito ai dati personali riguardanti persone decedute. La norma dispone, nello specifico, che i diritti garantiti dal Regolamento europeo agli artt. 15-22 (trattasi, in particolare, del diritto di accesso, del diritto di rettifica, oblio, portabilità, ecc.), in caso di decesso dell’interessato, possano “*essere esercitati da chi ha un interesse proprio, o agisce a tutela dell’interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione*”. Nonostante la genericità della disposizione, parrebbe potersi dedurre che, tra i soggetti richiamati dal Decreto, rientrino senza dubbio i prossimi congiunti del defunto, gli esecutori testamentari, nonché gli eredi legittimari pretermessi.

Detto intervento parrebbe giustificato, tra gli altri, dalla necessità di consentire agli eredi di accedere ai dati contenuti nelle piattaforme informatiche per procedere, a titolo esemplificativo,

# Approfondimenti

alla cancellazione, conversione ecc. dei profili personali. Tuttavia è sempre concessa all'interessato la facoltà di vietare il futuro esercizio dei diritti di cui sopra - quando ancora in vita e limitatamente ai servizi delle società di informazione - *“con dichiarazione scritta presentata direttamente al titolare del trattamento”* (art. 2-terdecies, comma 2).

## “Social media” e consenso del minore

Nel prevedere, all'art. 8, la liceità, per le società di informazione, del trattamento dei dati del minore di anni sedici soltanto con il consenso espresso del genitore, il GDPR aveva esplicitamente consentito agli Stati membri di prevedere una soglia di età inferiore (purché di almeno 13 anni). Ebbene, in tal senso il legislatore italiano si è avvalso della facoltà di abbassamento, statuendo all'art. 2-quinquies che *“il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento”*, posto che per età inferiori continua a risultare necessario che il consenso *“sia prestato da chi esercita la responsabilità genitoriale”*.

## Conclusioni

Molte erano le aspettative degli interpreti circa l'entrata in vigore del Decreto, alla luce, in parti-

colare, della genericità di talune disposizioni del Regolamento Ue e, soprattutto, del timore generato in capo alle imprese in merito all'irrogazione delle sanzioni.

All'indomani della pubblicazione, taluno non ha esitato, in proposito, a rilevare indici di scarsa qualità del prodotto legislativo; circostanza che sarebbe, peraltro, dimostrata dal comunicato di errata/corrige (G.U. n. 212 del 12 settembre 2018) pubblicato pochi giorni dopo il D.Lgs. n. 101/2018, con il quale si è provveduto a revisionare alcune disposizioni di cui all'art. 15, contenenti evidenti errori con riferimento all'indicazione dei commi da richiamare.

In ogni caso, a deludere buona parte degli interpreti è stata, altresì, la vaghezza e l'indeterminatezza in merito alle future ed eventuali semplificazioni per le piccole e medie imprese. La scelta di demandarne a successivi provvedimenti del Garante per la protezione dei dati personali l'individuazione porta con sé, infatti, numerose perplessità e risulta, al momento, inidonea a placare i timori dei c.d. “piccoli imprenditori”. Non resta, con ciò, che attendere le future pronunce del Garante per verificare la portata di dette misure, nonché la severità di cui intenderà avvalersi nell'irrogazione delle ingenti sanzioni previste dal Regolamento Ue 2016/679.