Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

Il decreto legislativo 101/2018 di modifica e coordinamento del Codice della privacy al GDPR: uno sguardo di insieme sul nuovo quadro normativo nazionale sulla tutela dei dati personali

di Alessandro del Ninno, professore e avvocato

E' stato pubblicato nella G.U. n. 205 del 4 Settembre 2018 il decreto legislativo 10 agosto 2018, n. 101 recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*".

Il decreto legislativo 101/2018 (che entra in vigore il 19 Settembre prossimo) novella e modifica il Codice della privacy (d.lgs. 196/2003) per coordinarne il contenuto regolatorio al già vigente (dallo scorso 25 maggio 2018) Regolamento Generale UE sulla protezione dei dati personali n. 679/2016 ("GDPR"). Inoltre, al di là della novella al Codice della privacy (attraverso abrogazioni, integrazioni e modifiche dell'articolato esistente) il decreto 101/2018 contiene ulteriori norme direttamente applicabili (importanti soprattutto le norme transitorie).

Il "nuovo" Codice della privacy si affianca al GDPR (occorrerà dunque in sede applicativa tenere conto di due importanti testi legislativi e dei relativi atti di implementazione connessi, essendo ovviamente quella del GDPR la disciplina privacy primaria e principale) e non va considerato un atto legislativo di recepimento nazionale del GDPR che - altrettanto ovviamente - essendo un regolamento comunitario è direttamente applicabile dal 25 Maggio scorso anche in Italia. Né il Codice della privacy apporta alcuna modifica al GDPR (una legge ordinaria non potrebbe modificare un regolamento comunitario, ad essa sovraordinato nel sistema delle fonti alle leggi ordinarie). Infine, andranno tenute presenti anche le residuali norme del decreto legislativo 101/2018 direttamente applicabili e non modificative o integrative del Codice della privacy in quanto tale (si pensi – solo per fare un esempio – all'articolo 22, Comma 5 del decreto 101/2018 recante norme sul cambiamento del nome e del cognome dei minorenni).

Il "nuovo" Codice della privacy rappresenta la normativa nazionale di coordinamento e di integrazione di quelle norme generali la cui regolamentazione di dettaglio appunto il GDPR ha lasciato agli Stati Membri ed ai Legislatori nazionali, al fine di specificare con regole ad hoc i presupposti di liceità del trattamento invece contenuti come principi generali nel GDPR: si pensi ai trattamenti di dati di particolare natura (ex "dati sensibili"), di dati relativi a reati e condanne penali (ex "dati giudiziari"), di dati biometrici, genetici e relativi

alla salute: il nuovo Codice della privacy quale risulta all'esito della novella operata dal decreto legislativo 101/2018 reca importanti prescrizioni, rispetto alle quali assume centralità il ruolo del Garante privacy che dovrà emanare non pochi provvedimenti attuativi. Inoltre, il GDPR ha lasciato altresì liberi gli Stati membri di dettare norme nazionali in ambiti ai quali il GDPR non si applica: ad esempio, il nuovo Codice della privacy continua a dettare una disciplina sul trattamento dei dati delle persone decedute (cfr. art. 2-*terdecies*), mentre è noto che il GDPR espressamente prevede che non si debba applicare a tali dati (cfr. il Considerando n. 27).

Anche nel settore del trattamento dei dati personali a fini di gestione del rapporto di lavoro, a fini di ricerca scientifica, storica e statistica, a fini di archiviazione e conservazione nel pubblico interesse e a fini giornalistici, in adempimento del Capo IX del GDPR (che ha demandato agli Stati Membri l'adozione di norme settoriali specifiche), il nuovo Codice della privacy detta norme nazionali ad hoc.

Nel presente contributo, si esamineranno - in una panoramica complessiva e in un'ottica pratico-operativa - le principali novità introdotte dal decreto 101/2018 e dal nuovo Codice della privacy novellato, elencate e commentate in "pillole" pratiche. Ciò anche per facilitare un approccio al nuovo Codice privacy che – per la tecnica redazionale adottata dal Legislatore (tecnica sempre più degradata nella prospettiva della chiarezza e comprensibilità delle norme) – si presenta di assai difficile lettura.

* * * * * *

In attuazione delle specifiche previsioni del GDPR il nuovo Codice della privacy come novellato dal decreto 101/2018 specifica: (a) i principi relativi al trattamento di dati relativi a condanne penali e reati e a connesse misure di sicurezza (gli ex "dati giudiziari"), prevedendo che il trattamento che avviene al di fuori del controllo della autorità pubblica sia lecito da solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati (l'articolo relativo - art. 2-*octies* del nuovo Codice - elenca una assai utile lista di casi esemplificativi di trattamenti ammessi). In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati nonché le relative garanzie saranno individuate con successivo decreto del Ministro della giustizia (che dunque è un ulteriore atto regolatorio che dovrà essere emanato); (b) le misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute, che possono essere oggetto di trattamento in presenza di una delle condizioni stabilite dall'art. 9 del GDPR e – in aggiunta - in conformità alle misure di garanzia disposte dal Garante con apposito e specifico provvedimento che dovrà essere emanato e aggiornato con cadenza biennale (cfr. art. 2-*septies* del nuovo Codice); (c) i casi di limitazione all'esercizio dei diritti che l'interessato può esercitare ai sensi degli articoli da 15 a 22 del GDPR (cfr. art. 2-*undecies* del Codice); le basi giuridiche per i soggetti pubblici che trattano dati di particolare natura (gli ex "dati sensibili) o debbano procedere al trattamento di dati in generale per motivi di interesse pubblico rilevante e connessi all'esercizio di pubblici poteri (cfr. articoli 2-*ter* e 2-*sexies* del nuovo Codice).

* * * * * *

E' interessante ricordare come nel nuovo Codice – all'articolo 2-*ter* - sono "recuperate" le definizioni previgenti – e del tutto assenti nell'articolo 4 del GDPR – di "comunicazione" e "diffusione" dei dati: per comunicazione si intende "*il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione*"; per "diffusione" si intende "*il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*" per esempio diffondere i dati mediante pubblicazione su bacheche o su Internet).

* * * * * *

Ridondante e foriera di difficoltà applicative appare poi la previsione di cui all'art. 2-*quaterdecies* del nuovo Codice che individua una nuova categoria – sconosciuta al GDPR – dei cosiddetti "*soggetti designati*". La norma dispone che il titolare o il responsabile del trattamento possono prevedere (dunque una facoltà e non un obbligo), sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità, individuando le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta. Una norma di cui francamente non si sentiva la necessità, soprattutto alla luce della chiara prescrizione dell'articolo 29 del GDPR rubricato "*Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento*" (*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento*). La norma appare più che altro un maldestro tentativo di preservare la designazione degli "incaricati del trattamento", figura quest'ultima prevista solo in Italia (dal vecchio articolo 30 del Codice della privacy, che prevedeva l'obbligo di nomina scritta delle persone fisiche operanti sotto l'autorità del titolare) e sconosciuta al resto della UE anche sotto il vigore della abrogata Direttiva sulla tutela dei dati personali.

* * * * * *

Assai significativa è poi la scelta del Legislatore italiano di confermare – nell'importante Titolo X ("*Comunicazioni Elettroniche*") la applicabilità, esclusivamente in materia di telemarketing, dell'*opt-in* (obbligo di consenso preventivo) anche per i trattamenti a tali esclusivi scopi dei dati delle persone giuridiche e delle aziende in quanto tali (in quanto "contraenti" e cioè, ai sensi del nuovo articolo 121 del Codice della privacy, "*parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate*"). Come è noto il

GDPR si applica ai soli dati delle persone fisiche, anche se ad esso si affiancherà il differente *ePrivacy Regulation* che nel corso del 2019 entrerà in vigore sostituendo la Direttiva 2002/58 sulla privacy nel settore delle comunicazioni elettroniche, prevedendo la specifica tutela dei dati delle persone giuridiche, inclusi i relativi trattamenti marketing. In tale prospettiva, si può affermare che il Legislatore italiano ha semplicemente anticipato ciò che l' *ePrivacy Regulation* comunque imporrà in materia di tutela dei dati delle persone giuridiche.

Per il resto, si può affermare che nel Titolo X restano sostanzialmente invariate – con alcuni aggiornamenti e integrazioni soprattutto in materia di sicurezza dei trattamenti (cfr. articoli 132-*ter* e 132-*quater* con i relativi obblighi imposti ai fornitori di reti e servizi di comunicazione elettronica) - le previgenti previsioni già contenute negli articoli da 121 a 132-*bis* del vecchio Codice.

* * * * * *

Così come d'altra parte, sono stati semplicemente coordinati al GDPR (prevedendone base giuridica di legittimità) e leggermente integrati tutti gli articoli del Codice previgenti che erano contenuti nella seconda parte, quella sui principi del trattamento in particolari settori (ambito sanitario, ambito pubblico, istruzione scolastica e universitaria; ricerca scientifica, storica o statistica, rapporti di lavoro, comparto assicurativo): anche con queste ulteriori prescrizioni i titolari e responsabili del trattamento interessati dovranno confrontarsi a partire dal 19 Settembre prossimo.

* * * * * *

In una fase in cui sta da tempo (dannosamente) proliferando un abusivo mercato di soggetti che si auto-dichiarano "certificatori" a vario titolo (di DPO, di conformità delle politiche del trattamento, di corsi di formazione "certificata", etc etc), appare norma di presidio l'art. 2-*septiesdecies* del nuovo Codice privacy che stabilisce che l'organismo nazionale di accreditamento è l'Ente unico nazionale di accreditamento, e cioè Accredia in quanto ente designato dal governo italiano, in applicazione del Regolamento europeo 765/2008, ad attestare la competenza, l'indipendenza e l'imparzialità degli organismi di certificazione. E' solo tale organismo (e in alternativa il Garante privacy, come previsto dal GDPR) che potrà accreditare organismi che dovranno dimostrare sia il possesso dei requisiti previsti dall'art. 43, comma 2, del GDPR che l'integrale rispetto dei criteri dettati dall'art. 42, comma 5, del GDPR (criteri esplicitati nelle *Linee Guida WP 261 sui criteri di accreditamento degli organismi di certificazione*) per ricevere il vero e proprio potere di certificazione a seguito di detto accreditamento.

* * * * * *

Rilevanti gli interventi sull'impianto sanzionatorio penale (che il GDPR, essendo materia riservata alla competenza nazionale, non poteva disciplinare ed ha rinviato, all'articolo 84, agli Stati membri): dopo che le prime bozze legislative del decreto di coordinamento avevano quasi del tutto depenalizzato i vecchi reati privacy contenuti nella

precedente versione del Codice della privacy, la scelta definitiva del Legislatore è stata di segno totalmente opposto: non solo sono stati confermati i reati già precedentemente noti e previsti dal Codice privacy (dal trattamento illecito di dati personali alla falsità nelle dichiarazioni al Garante; dalla inosservanza dei provvedimenti del Garante fino alle violazioni delle disposizioni in materia di controlli a distanza dei lavoratori), riordinando e rimodulando le relative sanzioni, ma sono stati altresì introdotte nel Codice nuove ipotesi di reato: la comunicazione e diffusione illecita di dati oggetto di trattamento su "larga scala" (art. 167-*bis*, per la cui nozione può farsi riferimento alle Linee Guida del Comitato Europeo WP 243); l'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala; l'interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante. L'unica ipotesi di reato abrogata è stata quella sulla omessa adozione delle misure di sicurezza, prima prevista all'articolo 168.

* * * * * *

Sul piano delle sanzioni amministrative, che come è noto sono materia ora direttamente disciplinata dal GDPR (con le nuove e ormai famose sanzioni amministrative pecuniarie, a seconda dei casi, fino a 10 o 20 milioni di Euro o, per le imprese, fino al 2 o 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore; e con i criteri di computo e applicazione previsti nelle Linee Guida attuative *WP 253 sulle sanzioni amministrative pecuniarie*), il decreto 101/2018 non si limita ad abrogare nel Codice della privacy quasi tutte le norme del Titolo III, Capo I sulle *Violazioni amministrative* (vengono abrogati gli articoli da 161 a 165) ma stabilisce anche – e questa è una indicazione rilevante – con la modifica dell'articolo 166 (l'unico articolo che rimane del Titolo III del Codice) quali violazioni amministrative delle nuove norme del novellato Codice della privacy devono essere sanzionate in base alle due diverse ipotesi previste dall'articolo 83, comma 4 del GDPR (fino a 10 milioni di Euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore) e 83, comma 5 (fino a 20 milioni di Euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore).

Sarà dunque sanzionata fino a 10 milioni di Euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, la violazione:

- dell'articolo 2-*quinquies*, comma 2, sul consenso del minore in relazione alla offerta di servizi della società dell'informazione, con particolare riferimento alla acquisizione del consenso del minore quattordicenne basato su informazioni non chiare, comprensibili o trasparenti);
- dell'articolo 2-*quinquiesdecies* relativo a trattamenti che presentano rischi elevati per l'esecuzione di un compito di interesse pubblico: la norma sanziona la violazione di eventuali provvedimenti di carattere generale adottati d'ufficio dal Garante per prescrivere misure e accorgimenti a garanzia dell'interessato che il titolare del trattamento in questi specifici casi è tenuto ad adottare;
- dell'articolo 92, comma 1 sui dati contenuti nelle cartelle cliniche (la norma prescrive che nei casi in cui strutture, pubbliche e private, che erogano prestazioni sanitarie e

socio-sanitarie redigono e conservano una cartella clinica in conformità alla disciplina applicabile, esse devono adottare opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri);

- dell'articolo 93, comma 1 ((la norma prescrive che ai fini della dichiarazione di nascita il certificato di assistenza al parto è sempre sostituito da una semplice attestazione contenente i soli dati richiesti nei registri di nascita);
- dell'articolo 123, comma 4 (sulla oscurazione delle ultime tre cifre dei numeri telefonici chiamati nella fatturazione al cliente);
- dell'articolo 128 (la norma prescrive che un fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve consentire a ciascun contraente, gratuitamente e mediante una funzione semplice, di poter bloccare il trasferimento automatico delle chiamate verso il proprio terminale effettuato da terzi);
- dell'articolo 129, comma 2 (sulla violazione del divieto di utilizzo – per l'abbonato che non ha dato il preventivo ed esplicito consenso - dei dati tratti dagli elenchi telefonici pubblici per finalità di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale);
- del nuovo articolo 132-ter, rubricato "Sicurezza del trattamento"e che prevede che il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve adottare, ai sensi dell'articolo 32 del GDPR, anche attraverso altri soggetti a cui sia affidata l'erogazione del servizio, misure tecniche e organizzative adeguate al rischio esistente;
- dell'articolo 110 sui trattamenti in materia di ricerca medica, biomedica ed epidemiologica (che non richiedono il consenso solo se autorizzati da una norma di legge o solo se il programma di ricerca è stato sottoposto a consultazione preventiva del Garante).

Sarà invece sanzionata fino a 20 milioni di Euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, la violazione:

- dell'articolo 2-*ter* che individua la base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
- dell'articolo 2-*quinquies*, comma 1 (sui limiti di età a quattordici anni per ottenere un valido consenso del minore per l'offerta di servizi della società dell'informazione e sull'obbligo, nel caso di minori infra-quattordicenni, di ottenere l'autorizzazione genitoriale);
- dell'articolo 2-*sexies* sul trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante;
- dell'articolo 2-*septies*, comma 7, sull'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati;
- dell'articolo 2-*ocities* recante i principi relativi al trattamento di dati relativi a condanne penali e reati;
- dell'articolo 2-*terdecies* recante i diritti sui dati delle persone decedute
- dell'articolo 52, commi 4 e 5, sul divieto di diffondere i dati di cui l'interessato ha chiesto l'oscuramento nelle sentenze giudiziarie o se i dati dei provvedimenti giudiziari si riferiscono a minori;
- di tutti gli articoli del Codice in materia di trattamento dei dati personali in ambito sanitario, sia pubblico che privato (dovranno essere particolarmente attenti i

professionisti del settore sanitario a quanto previsto dagli articoli da 75 a 82 del nuovo Codice della privacy);

- dell'articolo 92, comma 2, in caso di violazione del divieto di dar corso ad eventuali richieste di presa visione o di rilascio di copia della cartella clinica e dell´acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall´interessato;
- dell'articolo 93, commi 2 e 3, in caso di violazione del divieto di rilasciare certificati di assistenza al parto comprensivi dei dati della madre che abbia chiesto di non essere nominata;
- dell'articolo 96 (novellato), sul trattamento dei dati degli studenti nel comparto sia scolastico che universitario (particolare attenzione dovranno dunque prestare i dirigenti scolastici e le Università, vista la sanzione fino a 20 milioni di Euro);
- di tutti gli articoli del Codice sui trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;
- dell'articolo 110-*bis* sul trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici (norma che prevede la obbligatoria autorizzazione del Garante);
- dell'articolo 111, nel caso di violazione del (futuro) codice contenente le regole deontologiche per trattamenti nell'ambito del rapporto di lavoro che il Garante dovrà promuovere;
- dell'articolo 111-*bis* che prevede che nei casi di ricezione dei curricula spontaneamente
- trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro si debba comunque fornire la informativa privacy al momento del primo contatto utile, successivo all'invio del curriculum medesimo (la previsione della sanzione in questo caso appare a chi scrive del tutto esorbitante e ingiustificata);
- dell'articolo 116, comma 1, che prevede che gli istituti di patronato e di assistenza sociale, nell´ambito del mandato conferito dall´interessato, possono accedere alle banche di dati degli enti eroganti le prestazioni con il consenso manifestato dall'interessato medesimo;
- dell'articolo 120, comma 2, in materia di trattamenti nel comparto assicurativo, con particolare riferimento all'accesso e comunicazione dei dati della banca dati nazionale dei sinistri;
- di quasi tutte le norme del Titolo X sulle Comunicazioni elettroniche (articoli da 121 a 134-*quater*), inclusi i noti articoli sul telemarketing (art. 130, che richiede a tali fini il consenso preventivo sia di persone fisiche che delle persone giuridiche "contraenti") e sulla *data retention* (art. 132) dei dati di traffico telefonico (24 mesi) e telematico (12 mesi) cui sono obbligati gli operatori di comunicazione elettronica per esigenze di prevenzione e accertamento dei reati;
- dell'articolo 157, in caso di violazione dell'obbligo del titolare o del responsabile di riscontrare la richiesta di informazioni o di esibizione di documenti trasmessa dal Garante;
- delle future regole deontologiche che recheranno ulteriori misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute e per i trattamenti necessari per adempiere un obbligo legale al quale è soggetto il titolare del trattamento o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

* * * * * *

Importanti anche le norme transitorie contenute all'articolo 18 del decreto 101/2018 (dunque non nel Codice della privacy novellato) che consentono di chiudere in via agevolata i procedimenti sanzionatori pendenti alla data di entrata in vigore del decreto, così come le altre norme transitorie di cui all'art. 22 e 24 del decreto.

L'articolo 22, comma 13 del decreto 101/2018 contiene altresì una norma che dispone che per i primi otto mesi dalla data di entrata in vigore del decreto, il Garante per la protezione dei dati personali terrà conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del GDPR, della fase di prima applicazione delle disposizioni sanzionatorie. Il che - al contrario di quanto erroneamente pubblicizzato circa una presunta quanto infondata sospensione per otto mesi della applicazione di sanzioni in caso di violazioni - non implica affatto che l'Autorità non comminerà sanzioni per otto mesi (e d'altra parte è recente la pubblicazione sul sito del Garante privacy del piano ispettivo per il secondo semestre 2018, che interesserà gestori di grandi database, aziende di telemarketing e Istituti di credito). Significa solo che l'Autorità comminerà le sanzioni totalmente e fin da subito, ma applicherà con stringenti criteri i meccanismi di computo della sanzione (anche in base a quanto previsto dalle apposite Linee Guida europee *WP 253 sulle sanzioni amministrative previste dal GDPR*) oppure - in alternativa ed ove possibile (ad esempio per i titolari persone fisiche) - applicherà il nuovo potere di ammonimento (una sorta di richiamo) previsto come novità dal GDPR, senza applicare sanzioni amministrative pecuniarie (che come noto hanno una portata senza precedenti e che possono raggiungere nel massimo i 20 milioni di Euro o fino al 4% del fatturato mondiale di gruppo).

* * * * * *

Il decreto 101/2018 fa salvi tutti i provvedimenti emanati dall'Autorità Garante dal 1997 (cfr. art. 22, comma 4 del decreto) , in base al criterio della loro compatibilità con il GDPR e con le stesso decreto 101 (e vi saranno non poche difficoltà applicative e contrasti, poichè ciò che un titolare del trattamento potrebbe ritenere - all'interno di quei provvedimenti - non compatibile con il GDPR, disapplicandoli, potrebbe essere invece ritenuto dal Garante - in sede ispettiva - compatibile, dandosi luogo a sanzioni).

In base a quanto previsto dall'articolo 20 del decreto 101, restano provvisoriamente vigenti e applicabili anche i codici di deontologia e buona condotta (gli Allegati da A.1 a A.7 al Codice della privacy); ciò fino al controllo della loro compatibilità con il GDPR che il Garante dovrà effettuare entro 90 giorni dalla data di entrata in vigore del decreto (il 19 Settembre prossimo) o – per quanto riguarda i soli codici A.5, sulle centrali rischi private; A.6 per i trattamenti di dati personali effettuati per svolgere investigazioni difensive e A.7 per il trattamento dei dati personali effettuato a fini di informazione commerciale - fino alla definizione delle nuove procedure di adozione di codici di condotta (ridefiniti dall'art. 16 "Regole deontologiche") ai sensi dell'art. 40 del GDPR. Sono invece abrogati gli Allegati B (

recante il ben noto Disciplinare tecnico sulle misure minime di sicurezza, che non esistono più nel GDPR, prevedendo l'articolo 32 del Regolamento europeo le sole misure idonee) e l'Allegato C sui trattamenti non occasionali effettuati in ambito giudiziario e per finalità di polizia.

Si è scelto poi di garantire la continuità facendo salvi per un periodo transitorio anche le Autorizzazioni Generali (già il Garante con il Provvedimento in tema di Autorizzazioni generali del Garante per la protezione dei dati personali - 19 luglio 2018 ne ha transitoriamente prorogato la validità), che ai sensi dell'articolo 21 del decreto 101 saranno oggetto di successivo riesame.

* * * * * *

In considerazione delle esigenze di semplificazione delle micro, piccole e medie imprese, si è previsto che il Garante promuova modalità semplificate di adempimento degli obblighi del titolare del trattamento attraverso l'emanazione di specifiche Linee Guida (è un nuovo potere dell'Autorità previsto dall'articolo 154-*bis* del nuovo Codice della privacy).

* * * * * *

I minori che hanno compiuto quattordici anni potranno esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione (es: iscrizione a social media, offerte on line, etc). Per quanto riguarda i minori di 14 anni, invece, resta in piedi il requisito del consenso del soggetto esercente la potestà genitoriale. E' quanto prevede l'art. 2-*quinquies* del nuovo Codice della privacy, in attuazione dell'articolo 8 GDPR.

Conclusioni.

Il "nuovo" Codice della privacy (profondamente "snellito" nel numero degli articoli) non conclude comunque il complesso e complicato insieme di regole e norme a tutela dei dati personali: spetterà infatti all'Autorità Garante per la protezione dei dati personali emanare nel prossimo futuro ancora una serie di regole deontologiche sul trattamento di dati in particolari settori, oltre ad una serie di altri provvedimenti di ulteriore regolamentazione specifica. Tutti gli operatori dovranno quindi procedere con una doppia prospettiva per garantirsi la piena (e assolutamente non semplice da conseguire) conformità a tutta la applicabile normativa sulla protezione dei dati: un occhio dovrà essere in primo luogo sempre vigile sul GDPR (e sulle corpose Linee Guida esecutive già emanate dai Garanti UE nel biennio 2016-2018); l'altro dovrà rivolgersi al Codice della privacy. E ciò, nell'attesa delle ulteriori regole nazionali che nel futuro – tra deontologia, codici settoriali e provvedimenti del Garante – andranno ad arricchire il già affollatissimo panorama delle regole privacy.