Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

I recenti interventi normativi del Legislatore italiano nel settore della tutela dei dati personali tra dubbi di compatibilità e conflitti pratici con le norme del Regolamento Generale UE sulla data protection.
Le nuove norme privacy della Legge di Bilancio 2018

del Prof. Avv. Alessandro del Ninno

Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

Indice

§ 1. Introduzione: i recenti interventi del Legislatore italiano sul quadro normativo in materia di protezione dei dati. Legge Europea n. 167/2017, Legge di delegazione europea n. 163/2017 e Legge di Bilancio 2018 n. 205/2017.

Stanno facendo discutere – e non poco – i recenti interventi del Governo italiano, chiamato – come gli altri Stati membri della UE – a coordinare il quadro normativo nazionale in materia di protezione dei dati personali con la diretta applicabilità – a far data dal 25 Maggio 2018 – del Regolamento Generale UE sulla protezione dei dati personali n. 679/2016 (di seguito, "RGPD"). Gli argomenti di discussione vertono soprattutto su due aspetti: la scelta del tipo di intervento legislativo e i contenuti normativi di recente emanati, questi ultimi di davvero dubbia compatibilità, per taluni aspetti, con il Regolamento UE (va ricordato, nella gerarchia delle fonti, il primato dei regolamenti comunitari sulle leggi statali, da tempo acclarato sia dalla Corte Costituzionale che dalla Corte di Giustizia della UE, nel senso della capacità dei regolamenti comunitari di abrogare leggi statali anteriori e di resistere all'abrogazione da parte di leggi nazionali successive, da disapplicare in caso di contrasto).

Con riferimento al primo aspetto, e cioè la scelta del tipo di intervento legislativo adottato dal Legislatore italiano, va segnalato come molti Stati membri abbiano già da tempo compiuto il delicato lavoro di modifica e integrazione, emanando nuove leggi privacy nazionali organicamente coordinate al RGPD (la Germania è addirittura il primo Stato ad avere, fin dal 5 Luglio 2017, una normativa privacy rinnovata e coordinata al Regolamento, avendo adottato il "*Bundesdatenschutzgesetz*"; il Regno Unito – che pure uscirà dalla UE - ha approvato il nuovo *Data Protection Act* coordinato al RGPD, etc) . Nonostante non sia necessaria una norma interna di recepimento del Regolamento UE, direttamente applicabile negli ordinamenti nazionali, sono comunque molti i casi in cui lo stesso RGPD demanda alla legislazione nazionale il compito di precisare ulteriormente le condizioni specifiche per i trattamenti dei dati. Solo per fare alcuni esempi: l'art. 8 sulle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione, che prevede che gli Stati Membri possono stabilire – rispetto ai 16 anni ivi previsti – un'età diversa inferiore (purchè non sotto i 13 anni) per rendere validamente prestato il consenso; oppure l'art. 9 sul trattamento di categorie particolari di dati (che includo gli ex dati sensibili), che prevede all'ultimo comma la possibilità per gli Stati Membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute; fino ad arrivare all'art. 88 del RGPD che prevede che gli Stati membri possono prescrivere, con legge o tramite contratti collettivi (anche aziendali, ai sensi del Considerando 155), norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro. E si potrebbero fare molti altri esempi, ma non è questa la sede per un'analisi del genere, che porterebbe comunque alla conclusione di un quadro normativo UE sulla *data protection* che negli anni si diversificherà e frammenterà, a livello di norme nazionali, con buona pace delle intenzioni iniziali di introdurre un quadro normativo unitario che invece non sarà affatto – all'atto pratico e in contrasto proprio con gli obiettivi del Regolamento – omogeneo e privo di conflitti.

E l'Italia? A che punto è con tale delicato lavoro di coordinamento normativo tra normativa privacy esistente e RGPD? L'approccio legislativo attuato è stato quanto di più scoordinato e privo di visione programmatica e unitaria si potesse immaginare. Da un lato – difatti – vi è l'articolo 13 (rubricato "*Delega al Governo 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*") della c.d. Legge di Delegazione europea 2016-2017 (L. 25 ottobre 2017, n. 163 *Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea*); dall'altro abbiamo una serie di interventi episodici (verrebbe da dire quasi improvvisati) contenuti nell'art. 28 (rubricato "*Modifiche al codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196*") della c.d. Legge Europea 2017 (L. 20 novembre 2017, n. 167 - *Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione*

europea) e nei commi da 1020 a 1025 della successiva Legge 27 Dicembre 2017, n. 205, (c.d. *Legge di Bilancio 2018*) che saranno oggetto di specifica analisi e commento nel prosieguo della presente trattazione.
Con riferimento alle due leggi di attuazione degli obblighi di appartenenza alla UE, gli interventi di modifica e coordinamento del quadro nazionale privacy attuati in due distinte leggi (appunto la Legge di *Delegazione europea 2016-2017* e la *Legge Europea 2017*) derivano dal fatto che con la legge 234/2012 quella che prima era nota come la *Legge Comunitaria*, cioè lo strumento con cui il nostro Paese recepiva le norme giuridiche dell'Unione europea, è stata scissa in due distinti provvedimenti: la legge di delegazione europea e la legge europea (allo scopo di velocizzare i tempi di approvazione ed evitare l'avvio di procedure di infrazione). La legge di delegazione europea conferisce le deleghe legislative al Governo per far recepire nell'ordinamento italiano le direttive e gli altri atti dell'Unione europea. La legge europea, invece, contiene disposizioni modificative o abrogative di norme statali in contrasto con gli obblighi UE. Se la legge di delegazione europea (presentata entro il 28 febbraio di ogni anno) è finalizzata ad implementare nell'ordinamento nazionale le nuove norme UE, la legge europea mira invece a modificare – quando ritenuto necessario - precedenti normative, in conformità alle norme UE.

Dunque, l'art. 13 della Legge di Delegazione europea 2016-2017 ha delegato il Governo ad emanare (entro la data del 21 Maggio 2018, a quattro giorni dalla diretta applicabilità del RGPD…) "*uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679*", mediante:

- abrogazione specifica ed espressa delle norme del Codice della privacy incompatibili con le nuove regole del RGPD;
- modifica e integrazione del Codice della privacy limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel RGPD (cioè i casi di rinvio a più specifiche misure da prevedersi con norme nazionali in attuazione RGPD); modifica del Codice anche per quanto concerne il sistema sanzionatorio penale e amministrativo vigente, onde adeguarlo alle disposizioni del RGPD (che non prevede, ad esempio, le sanzioni penali) con previsione di sanzioni penali e amministrative "*efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse*";
- coordinamento delle disposizioni vigenti in materia di protezione dei dati personali contenute in altre leggi diverse dal Codice della privacy con le disposizioni del GDPR.

L'articolo 13 precisa anche che il tutto potrà avvenire prevedendo altresì nei decreti delegati – "*ove opportuno*" - il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal RGDP (norma, questa, di particolare interesse e portata innovativa, conferendo al Garante una sorta di "potere normativo delegato", anche nella fondamentale e necessaria prospettiva della attesa indicazione da parte dell'Autorità privacy italiana di ciò che resterà in vigore e di ciò che invece sarà abrogato del vasto panorama di Provvedimenti Generali, Linee Guida, codici deontologici, Autorizzazioni generali, etc emanate in venti anni dal Garante).

In sostanza, nonostante l'errato messaggio diffuso in questi mesi di un Codice della privacy abrogato dal RGPD (che invece, ai sensi dell'art. 94, abroga semplicemente la Direttiva del 1995 sulla protezione dei dati personali), all'esito dell'esercizio della delega ci troveremo con un quadro normativo privacy nazionale (limitandoci al solo rango legislativo primario) costituito dal Codice della privacy emendato attraverso abrogazioni, integrazioni e introduzione di nuove norme di coordinamento; dalle norme del RGPD direttamente applicabili; dalle altre leggi esterne settoriali che prevedono norme sul trattamento dei dati personali: un quadro - cui aggiungere tutti gli atti amministrativo-regolatori del Garante - all'interno del quale non sarà affatto semplice muoversi.

L'articolo 28 della Legge europea 2017 n. 167/2017 ha invece introdotto le seguenti modifiche al Codice della privacy:

- ha aggiunto all'articolo 29 (sul responsabile del trattamento) un comma 4-*bis* (che di fatto recepisce - in parte - modalità di nomina, caratteristiche soggettive e ruolo della figura del responsabile del trattamento come tratteggiata dall'articolo 28 del RGPD) e modificato il comma 5 per coordinare gli obblighi del responsabile e i rapporti tra titolare e responsabile al nuovo comma 4-*bis*; l'intervento normativo in questione è apparso del tutto scomposto e quasi improvvisato, sorprendente nel suo non essere assolutamente né atteso nè urgente o al momento necessario (anche perché non coordinato con la delega più generale di cui all'art. 13 della legge di delegazione europea 167/2017), determinando altresì all'atto pratico una anticipazione al 12 Dicembre 2017, data di entrata in vigore delle modifiche, della efficacia di taluni obblighi previsti e prescritti dal RGPD sul responsabile del trattamento (rispetto alla data di efficacia del RGPD del 25 maggio 2018);
- ha aggiunto il nuovo articolo 110-*bis* sul riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici (nuova norma che pure sta sollevando forti polemiche: per alcuni – infatti - poiché codifica la possibilità per le multinazionali di settore di accedere per scopi di ricerca ai dati sanitari dei cittadini – ancorchè soggetti a minimizzazione ed anonimizzati e previa procedura di autorizzazione del Garante - senza che questi siano informati o prestino il consenso; per altri perché – vietando tale procedura per la ricerca sui dati genetici – restringerebbe – in una diversa prospettiva – le possibilità di avanzamento della ricerca scientifica medesima).

Il presente articolo affronterà in particolare la portata pratica del terzo e più recente intervento normativo di "coordinamento-recepimento" (non richiesto e di dubbia "costituzionalità") del RGPD: quello attuato dal Legislatore italiano con la Legge di Bilancio 2018 e le cui norme sono applicabili a far data dal 1° gennaio 2018.

§ 2. Gli obblighi privacy introdotti dai commi da 1020 a 1025 della Legge di Bilancio 2018: un quadro di insieme all'insegna della assoluta disorganicità dell'intervento normativo.

Se nel panorama normativo italiano già gli interventi di coordinamento tra quadro giuridico privacy italiano e RGPD attuati dalla Legge di delegazione europea e dalla Legge Europea hanno determinato una inopinata confusione a causa della mancanza – *sic* ! – di coordinamento e di visione organica degli interventi necessari, con la Legge di Bilancio 2018, in vigore dallo scorso 1° gennaio 2018, il Legislatore italiano ha ulteriormente peggiorato il quadro (di disorganicità), poiché ha introdotto novità che – per quanto si dirà – appaiono essere addirittura in contrasto con il (se non in violazione del) RGPD.
Nel prosieguo si procederà ad un commento pratico di ciascuno dei cinque commi; in sede preliminare – tuttavia – non si può non formulare un assai severo e negativo giudizio complessivo su tale intervento nel settore della tutela dei dati personali – inopinato quanto scoordinato – attuato dal Legislatore. Basti osservare, in via generale, quanto segue.

In primo luogo, la ormai inveterata e grave abitudine della tecnica redazionale delle leggi fondamentali della Repubblica: leggi *monstre* di un solo articolo e centinaia di commi scoordinati, senza neanche più l'ausilio delle rubriche degli articoli, o delle Sezioni, dei Capi, dei Titoli a guida dell'opera interpretativa degli operatori chiamati ad applicare le norme. Una tecnica del genere è – tra l'altro - di davvero dubbia costituzionalità: la Costituzione prevede all'art. 72 che l'approvazione di ogni legge avvenga «*articolo per articolo e con votazione finale*»; la stessa Presidenza della Repubblica ha richiamato più volte il Parlamento sul punto: ad esempio, fin dal 2004 l'allora Presidente Carlo Azeglio Ciampi scrisse in un messaggio di rinvio di una legge alle Camere: "*A tale proposito, ritengo che questa possa essere la sede propria per richiamare l'attenzione del Parlamento su un modo di legiferare, invalso da tempo, che non appare coerente con la ratio delle norme costituzionali che disciplinano il procedimento legislativo e, segnatamente, con l'articolo 72 della Costituzione. La Costituzione esige che i parlamentari votino provvedimenti suddivisi per partizioni*

omogenee, così da esprimersi con razionalità, evitando di dover dire sì o no a caotici assembramenti di disposizioni del tutto scoordinate, slegate, incoerenti. Il voto finale obbligatorio serve altresì ad evitare che l'approvazione di articoli contraddittori (politicamente, anche se non giuridicamente) determini l'adozione di una legge disomogenea».

In secondo luogo, i commi da 1020 a 1025 della Legge di Bilancio rappresentano un (asserito) coordinamento con il RGPD del tutto *esterno* rispetto alle fonti normative vigenti, nel senso che segue. Mentre la Legge di delegazione europea ha previsto l'emanazione di specifici decreti volti a modificare e coordinare il Codice della privacy con il RGPD e l'art. 28 della legge Europea ha comunque novellato direttamente il Codice della privacy integrandone l'articolato – si è dunque trattato di due interventi normativi forieri di effetti, per così dire, *interni* al Codice della privacy - gli scoordinati commi da 1020 a 1025 della Legge di Bilancio 2018 restano e resteranno invece limitati e "rinchiusi" dentro tale fonte normativa, non incidendo affatto in senso modificativo o integrativo sul Codice della privacy né coordinandosi in altro modo con esso. L'attuale e incredibilmente disorganico effetto (a meno di future correzioni auspicabili in sede di esercizio della delega di cui all'art. 13 della Legge di delegazione europea) è che si dovranno leggere le future norme delegate di coordinamento e/o il Codice della privacy come eventualmente modificato e coordinato con il RGPD, insieme ai commi in esame.

In terzo luogo, non si può non notare addirittura una serie di gravi imprecisioni linguistiche e di terminologia tecnico-giuridica nella redazione dei commi in esame: di tali lacune si darà conto in sede di commento dei singoli commi.

§ 2.1 Segue - Commento al comma 1020: dalle imprecisioni linguistiche all'incomprensibile delega di tutela che snatura la funzione del Garante privacy.

Il comma 1020 della Legge di Bilancio 2018 così recita:
"*Al fine di adeguare l'ordinamento interno al 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, di seguito denominato « regolamento RGPD », il Garante per la protezione dei dati personali assicura la tutela dei diritti fondamentali e delle libertà dei cittadini*".

Tale comma è una testimonianza di quanto sia scaduta e impoverita la qualità e la tecnica di scrittura delle norme di legge in questo Paese. Prima di analizzare la portata giuridica della norma, la si commenterà dalla prospettiva meramente linguistica: quale è il significato in lingua italiana? Intanto il Legislatore addirittura specifica e definisce tautologicamente il regolamento come regolamento…. L'acronimo "RGPD" sta per "*Regolamento Generale sulla Protezione dei Dati*"; il Legislatore specifica che si riferisce al RGPD come "*regolamento RGPD*", che dunque sta per "*regolamento Regolamento Generale sulla Protezione Dei Dati*"….

In secondo luogo, la portata concettuale (sempre in lingua italiana) del comma 1020 è la seguente: in tanto l'ordinamento italiano può adeguarsi al RGPD (e tale finalità può essere perseguita solo) in quanto il Garante per la protezione dei dati personali assicuri la tutela dei diritti fondamentali e delle libertà dei cittadini. Incredibilmente (e stavolta anche da un punto di vista giuridico) la norma (del tutto inutile quanto a portata pratica, ma gravissima da un punto di vista legale e delle conseguenze di interpretazione giuridica) snatura la funzione del Garante, obbligandolo ad "assicurare" *la tutela dei diritti fondamentali e delle libertà dei cittadini*" (come se fosse un Legislatore o un Tribunale della Repubblica). Addirittura in funzione dell'intero coordinamento dell'ordinamento interno al "*regolamento RGPD*"…. A ben vedere, neanche l'attuale articolo 154 del Codice della privacy si spinge a tanto, prevedendo tra i compiti e il ruolo istituzionale del Garante (che è una autorità amministrativa indipendente) quelli di presidio e controllo del

rispetto della disciplina applicabile ai trattamenti di dati; anzi è il Garante che deve - ai sensi dell'art. 154 - "*segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti*", non è certo tale Authority che può/deve provvedere in via diretta alla loro tutela, come sembrerebbe da una semplice lettura della norma! E neanche gli articoli 57 e 58 del GDPR si spingono – nell'elencare i compiti e i poteri delle autorità nazionali di controllo – a delegare loro una funzione di tutela diretta dei diritti e delle libertà dei cittadini con riferimento al trattamento dei dati personali. Anche l'art. 51 RGPD ("*Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione*") ricollega allo "*Stato Membro*" e non alle autorità di controllo il "*fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento*", e lo stesso articolo 57 RGPD delega alle autorità di controllo il primario compito di sorvegliare e assicurare "*l'applicazione del Regolamento*", che è compito ben diverso da quello di attuare in via diretta "*la tutela dei diritti fondamentali e delle libertà dei cittadini*".

§ 2.2 Segue - Commento al comma 1021: l'obbligo (inesistente nel RGPD) di garantire l'interoperabilità dei formati dei dati. Un nuovo format documentale che ricorda il modello di notificazione del trattamento al Garante privacy.

Il comma 1021 della Legge di Bilancio 2018 così recita:
"Ai fini di cui al comma 1020, il Garante per la protezione dei dati personali, con proprio provvedimento da adottare entro due mesi dalla data di entrata in vigore della presente legge:
a) disciplina le modalita' attraverso le quali il Garante stesso monitora l'applicazione del regolamento RGPD e vigila sulla sua applicazione;
b) disciplina le modalita' di verifica, anche attraverso l'acquisizione di informazioni dai titolari dei dati personali trattati per via automatizzata o tramite tecnologie digitali, della presenza di adeguate infrastrutture per l'interoperabilità dei formati con cui i dati sono messi a disposizione dei soggetti interessati, sia ai fini della portabilità dei dati ai sensi dell'articolo 20 del regolamento RGPD, sia ai fini dell'adeguamento tempestivo alle disposizioni del regolamento stesso;
c) predispone un modello di informativa da compilare a cura dei titolari di dati personali che effettuano un trattamento fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati;
d) definisce linee-guida o buone prassi in materia di trattamento dei dati personali fondato sull'interesse legittimo del titolare".

Tale comma, prevede che *"ai fini di cui al comma 1020"* (cioè, dunque, al fine di adeguare l'ordinamento interno al RGPD e far sì in concreto che il Garante assicuri *"la tutela dei diritti fondamentali e delle libertà dei cittadini"*…) l'Autorità Garante per la protezione dei dati personali adotti entro il 1° Marzo 2018 (cioè entro due mesi dalla data di entrata in vigore della Legge di Bilancio 2018) un "*proprio provvedimento*" per disciplinare e definire una pletora diversificata e disomogenea di scopi, attività e modelli documentali: dalle modalità di monitoraggio su come (l'intero) RGPD viene applicato alle verifiche sull'adempimento degli obblighi dei titolari del trattamento di garantire agli interessati la portabilità dei dati personali da un titolare all'altro (nuovo diritto degli interessati previsto dall'art. 20 RGPD); dalla redazione di nuovi modelli documentali alla redazione di linee guida o buone prassi, etc. In sostanza, tale comma vorrebbe introdurre le disposizioni esecutive e di attuazione dei principi del comma 1020.
In primo luogo, dalla lettura del comma, non si comprende se il Garante debba provvedere con un provvedimento *omnibus* o con più provvedimenti settoriali: la norma non menziona "*uno o più provvedimenti*" ma sembrerebbe indicare un provvedimento unitario: anche il limitato lasso di tempo conferito all'Autorità per la adozione – solo 60 giorni – sembrerebbe non compatibile con l'adozione di più provvedimenti singoli, corrispondenti ad esempio ai contenuti di ciascuna delle lettere da (a) a (d) del

comma in esame. Con riferimento poi alla lettera (a) del comma 1021, non si comprende se il Garante possa adempiere aggiornando alla luce del RGPD i propri Regolamenti interni (es: i regolamenti 1/2007 - che agli articoli 15 e 16 reca appunto le modalità su come il Garante vigila e controlla il rispetto delle norme a tutela della protezione dei dati - e 2/2007) o se debba adottare un provvedimento *ad hoc.*

La lettera (b) del comma 1021 dispone poi che il Garante privacy, con proprio provvedimento, detti le regole per verificare se i "*titolari dei dati personali*" (*rectius*: "*titolari del trattamento",* incredibilmente ed erroneamente definiti "*titolari dei dati personali*", figura mai esistita e non esistente, a dimostrazione della "sciatteria redazionale" del Legislatore da un punto di vista tecnico-giuridico..) abbiano adeguate infrastrutture per garantire l'interoperabilità dei formati con cui i dati (esclusivamente) trattati per via automatizzata o tramite tecnologie digitali sono messi a disposizione dei soggetti interessati. E ciò nella duplice prospettiva (1) di attuazione del nuovo diritto alla portabilità dei dati come previsto dall'art. 20 RGPD; e dell'incomprensibile fine di (2) "*adeguamento tempestivo alle disposizioni del regolamento stesso"* (il realtà il RGPD fa riferimento alla "*interoperabilità dei formati*" solo nel Considerando 68, ove si legge che sarebbe "*opportuno incoraggiare i titolari del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati*"; in altri termini non vi sono disposizioni obbligatorie del RGPD in materia di interoperabilità dei formati cui "*adeguarsi tempestivamente*"…). Nel proprio provvedimento il Garante potrà anche disciplinare le modalità di acquisizione di informazioni utili ai fini citati presso i titolari: cioè che in realtà è già previsto e regolato dagli articoli 157 ("*Richiesta di informazioni e di esibizione di documenti*") e 158 ("*Accertamenti*") del Codice della privacy, oltre che dall'art. 58, comma 1, lettera (a) del RGPD ("*Ogni autorità di controllo ha il potere di ingiungere al titolare del trattamento ….. di fornirle ogni informazione di cui necessiti ….").*

La lettera (b) del comma 1021 appare incompatibile e in conflitto con il RGPD, il quale – come detto – non prescrive alcun obbligo per i titolari di dotarsi di "*infrastrutture per l'interoperabilità dei formati*"; né sarebbe sanzionabile quel titolare che ne fosse sprovvisto all'esito delle "*verifiche*" condotte in materia dal Garante in base alle modalità previste nel "*proprio provvedimento*". Il Legislatore italiano pare tra l'altro dimenticare che in materia di portabilità esistono e sono in vigore le specifiche Linee Guida adottate dai Garanti privacy UE in esecuzione dell'art. 20 del RGPD (WP 242 – *Linee Guida sul diritto alla portabilità dei dati* del 13 Dicembre 2016, aggiornate in 5 aprile 2017). Tali Linee Guida (con le quali il futuro provvedimento del Garante ai sensi del comma 1021 dovrebbe comunque coordinarsi, con non pochi problemi) prevedono esattamente il contrario allorchè specificano l'insussistenza – allo stato – di formali obblighi legali (invece indirettamente posti dal comma 1021) di dotarsi di "*adeguate infrastrutture per l'interoperabilità dei formati con cui i dati sono messi a disposizione dei soggetti interessati*. Al massimo, le Linee Guida europee "invitano", "suggeriscono" come buona prassi, auspicano come opportuno scenario industriale futuro quello di addivenire alla competa compatibilità e interoperabilità di formati, ma non prescrivono alo stato alcuno specifico obbligo tecnico-giuridico:

- *… il Considerando 68 RGPD promuove lo sviluppo di formati interoperabili da parte dei titolari così da consentire la portabilità dei dati, ma non configura un obbligo in capo ai titolari stessi di introdurre o mantenere sistemi di trattamento tecnicamente compatibili…;*
- *… l'aspettativa è che il titolare trasmetta i dati personali in un formato interoperabile, ma ciò non configura alcun obbligo in capo agli altri titolari di supportare tale formato: occorrerà solo prestare particolare attenzione al formato dei dati trasmessi in modo da garantire che i dati siano riutilizzabili dall'interessato o da un diverso titolare con un minimo sforzo…;*
- *… si dovrebbero invitare i titolari del trattamento a garantire l'interoperabilità dei formati con cui i dati vengono messi a disposizione in ottemperanza a una richiesta di portabilità.*

Per completezza espositiva , si ricorda che l'articolo 20 RGPD introduce il nuovo diritto alla portabilità dei dati. Tale diritto consente all'interessato di ricevere i dati personali in precedenza forniti a un titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli a un altro titolare del trattamento senza impedimenti. Il nuovo diritto alla portabilità – soggetto a specifiche condizioni (soprattutto per quanto concerne il trasferimento dei dati da un titolare all'altro) - intende promuovere il controllo degli interessati sui propri dati personali, facilitando la circolazione, la copia o la trasmissione dei dati da un ambiente informatico all'altro (che si tratti dei propri sistemi, dei sistemi di soggetti terzi fidati, o di quelli di un diverso titolare del trattamento).

La lettera (c) del comma 1021 dispone che il Garante privacy, con proprio provvedimento, predisponga *"un modello di informativa da compilare a cura dei titolari di dati personali che effettuano un trattamento fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati".* Tale disposizione prevede dunque un nuovo modello documentale standard, collegato ad una procedura specificata dai successivi commi 1022 e 1023: quella della verifica della sussistenza dell'interesse legittimo del titolare del trattamento quale base giuridica di trattamenti che prevedono *"l'uso di nuove tecnologie o di strumenti automatizzati*".
Prima di commentare la portata della norma, non si può non rilevare nuovamente quella che abbiamo definito più sopra "sciatteria redazionale" del Legislatore da un punto di vista linguistico e tecnico-giuridico: dalla ripetuta menzione del "*titolare dei dati personali*" (in luogo di "titolare del trattamento") alla definizione del nuovo modello come "*informativa*" (che nulla ha a che vedere con l'atto con il quale i titolari del trattamento forniscono agli interessati le informazioni su finalità, modalità, sicurezza dei trattamenti dei loro dati), che servirà solo ad aumentare la confusione.

In realtà questo nuovo modello che il Garante dovrà predisporre nella sua struttura e nei contenuti, sembra avvicinarsi – per finalità - al modello (esistente) della notificazione dei trattamenti (istituto abrogato con l'entrata in vigore del RGPD dal prossimo 25 Maggio 2018): come nel modello di notificazione dei trattamenti, infatti, il nuovo format dovrà consentire al titolare di specificare al Garante (ma non ai terzi: il modello infatti non confluirà in un Registro ma resterà a livello di interlocuzione interna tra titolare e Garante) "*l'oggetto, le finalità e* (il non meglio specificato, n.d.r.) *contesto del trattamento*". Differisce però dal modello di notificazione perché non ha carattere generale (per lo meno con riferimento alle categorie di trattamenti elencati dall'art. 37 del Codice della privacy e per i quali la notificazione è restata obbligatoria), ma si applica esclusivamente a trattamenti:

- per i quali il titolare del trattamento si richiami all'interesse legittimo come base giuridica del trattamento (quindi, ad esempio, non va compilato alcun modello di "*informativa*"se il trattamento si basa sul consenso dell'interessato, o sull'adempimento di obblighi normativi, etc);
- che siano effettuati mediante l'uso di nuove tecnologie o di strumenti automatizzati (se i mezzi del trattamento sono esclusivamente manuali, non vi è obbligo alcuno; va specificato che per "nuove tecnologie" si intende anche la introduzione – nel contesto organizzativo di un certo titolare del trattamento – di tecnologie mai impiegate prima da quel titolare, anche se non sono "nuove" nel senso di precedente inesistenza sui mercati tecnologici).

Occorre allora illustrare – per comprendere la portata pratica e applicativa della norma (e anche dei successivi commi 1022 e 1023) – cosa si intende per trattamento fondato sull'interesse legittimo del titolare del trattamento, e ciò sia alla luce del Codice della privacy che del RGPD. Sia Il Codice della privacy che il RGPD non forniscono in realtà una definizione giuridica di "*interesse legittimo*" del titolare del trattamento: tale istituto è solo considerato quale base giuridica alternativa alle altre (il consenso dell'interessato, l'esecuzione di un contratto, l'adempimento di obblighi di legge, etc) in grado di fondare un lecito trattamento di dati personali ove non prevalgano i diritti e le libertà fondamentali dell'interessato.
In assenza di precise definizioni normative, ci aiuta a comprendere meglio l'istituto e il concetto lo specifico *Parere WP 217 del 9 Aprile 2014, n. 6 sulla nozione di legittimo interesse del titolare del trattamento* adottato dal Gruppo dei Garanti UE. In base a tale parere, per essere considerato "legittimo", (quale base

giuridica lecita del trattamento) l'"interesse" del titolare deve basarsi su tutte le seguenti e contestuali condizioni (da comprovare):

1. deve essere legale, cioè previsto da una norma di legge nazionale o europea;
2. deve essere concreto (dunque non una astratta enunciazione di principio di un generico interesse a procedere ad un certo trattamento);
3. deve essere – di conseguenza - documentabile e sufficientemente chiaro da poter essere illustrato e giustificato dal titolare in maniera articolata, onde consentire di svolgere una comparazione pratica tra detto interesse e i diritti e le libertà degli interessati (per verificare quale prevalga);
4. deve essere reale, attuale e non speculativo;
5. il correlato trattamento di dati deve essere realmente e concretamente necessario per perseguire l'interesse legittimo del titolare e quest'ultimo deve considerare se non esistano modalità e mezzi meno invasivi che gli consentano di perseguire comunque le finalità del trattamento e realizzare l'interesse;
6. i diritti e le libertà degli interessati devono risultare non prevalenti sull'interesse legittimo del titolare del trattamento, all'esito di uno specifico *balance test,* e cioè una comparazione in ogni specifico caso/trattamento tra il proprio interesse e i diritti e libertà fondamentali degli interessati; il titolare deve condurre (e documentare ai sensi anche dell'*accountability* del RGPD) tale *balance test* tenendo presente: la natura dell'interesse (es: diritto fondamentale, interesse pubblico, etc), il possibile pregiudizio del titolare del trattamento o di terzi ove non fosse possibile procedere al trattamento; la natura dei dati, lo status dell'interessato (es: minore, lavoratore dipendente, etc), le modalità del trattamento (es: su larga scala, profilazione, comunicazione ad elevato numero di destinatari, etc), la natura dei diritti e delle libertà che nello specifico sarebbero coinvolte dal trattamento;
7. vanno considerate le aspettative dell'interessato;
8. vanno valutati comparativamente gli impatti del trattamento sulla sfera degli interessati in rapporto ai benefici derivanti al titolare dallo svolgimento del trattamento.

Ai sensi della vigente disciplina di cui al Codice della privacy, l'istituto dell'interesse legittimo del titolare del trattamento è menzionato in un solo caso: quello dell'art. 24 ("*Casi nei quali può essere effettuato il trattamento senza consenso*"), comma 1, lettera (g). Tale norma dispone che non è necessario acquisire il consenso dell'interessato quando il trattamento "*con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei princìpi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato*".

In altri termini, è possibile procedere al trattamento senza acquisire il consenso dell'interessato (consenso che nella filosofia attuale è il pilastro fondamentale del sistema legale di *data protection*, mentre assume minore importanza nella filosofia del RGPD) solo ove il Garante (e non il titolare del trattamento), all'esito di una procedura di verifica – caso per caso – abbia formalmente stabilito "*sulla base dei princìpi sanciti dalla legge"* che non prevalgono *"i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato*" e dunque il trattamento può essere svolto basandolo (in alternativa al consenso) sull'interesse legittimo del titolare. In pratica, il titolare presenta al Garante una specifica *istanza di riconoscimento di interesse legittimo ai sensi dell'art. 24, comma 1, lettera (g) del Codice della privacy* (spesso unitamente all'interpello o *prior checking* ex art. 17 della Codice della privacy) che dà avvio ad un procedimento amministrativo che si conclude con un pronunciamento (di riconoscimento o diniego) dell'interesse legittimo per lo specifico trattamento sottoposto a valutazione dell'Autorità da parte del titolare.

Al contrario, con il RGPD, dal 25 maggio 2018 decadrà la procedura appena descritta per il riconoscimento di interesse legittimo: sarà il titolare del trattamento – ovviamente in base ai principi di responsabilizzazione e di *accountability* – a svolgere in proprio le valutazioni (di cui appunto assume la responsabilità) sulla sussistenza dell'interesse legittimo e la comparazione con i diritti e le libertà degli interessati coinvolti. Il titolare del trattamento cioè conduce un *assessment* sul proprio legittimo interesse e ne documenta l'esito (come anche indicato dal Parere 6/2014 sopra citato), senza essere obbligato a

presentare istanze di sorta all'autorità privacy. Nel condurre tale valutazione il titolare del trattamento può utilizzare la guida contenuta nel Considerando 47 del RGPD:
"*I legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Ad esempio, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali*".
Tra l'altro, alcuni Considerando del RGPD elencano e menzionano casi di legittimo interesse del titolare presentato già come prevalente sui diritti e le libertà è degli interessati (come se fosse stato condotto a monte dal Legislatore UE il relativo *assessment*):

- costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di prevenzione delle frodi;
- i titolari del trattamento facenti parte di un gruppo imprenditoriale possono avere un interesse legittimo a trasmettere dati personali all'interno del gruppo imprenditoriale a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti (è il trattamento per *finalità amministrativo-contabili* di cui all'attuale art. 24 e 34 del Codice della privacy, che difatti non richiede il consenso degli interessati);
- costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione.

L'articolo 6 RGPD ("*Liceità del trattamento*"), alla lettera (f) del comma 1, individua tra le basi giuridiche di liceità del trattamento quella appunto dell'interesse legittimo: il trattamento è lecito solo "*se necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore*".

L'interesse legittimo del titolare del trattamento è poi menzionato nell'ambito di un altro importante nuovo istituto introdotto dal RGPD: quello della *valutazione di impatto preventiva* di cui all'art. 35. In base a tale disposizione, quando un trattamento prevede l'uso di nuove tecnologie e considerati la natura, l'oggetto, il contesto e le finalità del trattamento può presentare un rischio *elevato* per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve effettuare, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (c.d. *privacy impact assessment* o DPIA). Oltre agli altri elementi, "*la valutazione contiene almeno una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento*". Ecco dunque in che senso il RGPD stabilisce un rapporto tra DPIA e valutazione dell'interesse legittimo.
Solo se il titolare del trattamento, all'esito delle sue preventive valutazioni, ritenga di non aver identificato o attenuato sufficientemente il rischio, allora dovrà rivolgersi all'autorità di controllo (in una sorta di consultazione consulenziale obbligatoria) che fornirà, entro un termine di otto settimane (prorogabile di altre sei) dal ricevimento della richiesta di consultazione, un parere scritto.
Dunque il legislatore italiano, nel comma 1021, lettera (c), appare aver confuso con la procedura Valutazione di Impatto Preventivo del RGPD l'istituto dell'interesse legittimo come base giuridica del trattamento, come meglio si dirà in sede di commento dei commi 1022 e 1023.

La lettera (d) del comma 1021 prevede infine che con proprio provvedimento il Garante definisca linee-guida o buone prassi in materia di trattamento dei dati personali fondato sull'interesse legittimo del titolare. A parte che oramai – nella prospettiva europea del RGPD – linee guida o buone prassi devono essere definite di concerto tra le varie autorità privacy UE riunite nel Comitato Europeo per la protezione dei dati di cui all'art. 68 RGPD, ancora una volta il Legislatore italiano appare aver scordato che linee guida in materia già esistono (la opinion 6/2014 sul legittimo interesse) o saranno emanate a livello UE in attuazione del RGPD, dunque non si comprende l'utilità pratica di una tale disposizione, che potrebbe creare conflitti con atti già esistenti.

§ 2.4 Segue - Commento ai commi 1022 e 1023: la reintroduzione dell'obbligo di presentare istanza al Garante privacy per il riconoscimento dell'interesse legittimo. Tra confusione e conflitti con la valutazione di impatto preventiva prevista dal RGPD.

I commi 1022 e 1023 introducono una nuova procedura di notifica/comunicazione tra titolare del trattamento e Autorità Garante per la protezione dei dati personali, delineata come segue:

1022. Il titolare di dati personali, individuato ai sensi dell'articolo 4, numero 7), del regolamento RGPD, ove effettui un trattamento fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati, deve darne tempestiva comunicazione al Garante per la protezione dei dati personali. A tale fine, prima di procedere al trattamento, il titolare dei dati invia al Garante un'informativa relativa all'oggetto, alle finalità e al contesto del trattamento, utilizzando il modello di cui al comma 1021, lettera c). Trascorsi quindici giorni lavorativi dall'invio dell'informativa, in assenza di risposta da parte del Garante, il titolare può procedere al trattamento.

1023. Il Garante per la protezione dei dati personali effettua un'istruttoria sulla base dell'informativa ricevuta dal titolare ai sensi del comma 1022 e, ove ravvisi il rischio che dal trattamento derivi una lesione dei diritti e delle libertà dei soggetti interessati, dispone la moratoria del trattamento per un periodo massimo di trenta giorni. In tale periodo, il Garante può chiedere al titolare ulteriori informazioni e integrazioni, da rendere tempestivamente, e, qualora ritenga che dal trattamento derivi comunque una lesione dei diritti e delle libertà del soggetto interessato, dispone l'inibitoria all'utilizzo dei dati.

Il Legislatore italiano compie una incredibile confusione, ispirandosi - da un lato – alla DPIA, la procedura di valutazione di impatto preventiva (ed eventuale successiva interlocuzione con l'autorità di controllo) ai sensi degli articoli 35 e 36 del RGPD, ma - dall'altro - introduce nell'ordinamento italiano una nuova obbligatoria procedura che nulla ha a che vedere con la DPIA e semmai ha l'effetto pratico di reintrodurre obblighi che sarebbero abrogati con l'entrata in vigore del RGPD: in parte una sorta di notificazione del trattamento, in parte l'obbligo di sottoporre comunque alla valutazione dell'Authority la sussistenza di un interesse legittimo del titolare del trattamento, proprio come ora avviene ai sensi della già indicata procedura prevista dall'art. 24, comma 1, lettera (g) del Codice della privacy.

Procedendo a comparare le caratteristiche delle due procedure (la DPIA e le interlocuzioni con l'autorità di controllo ai sensi degli articoli 35 e 36 RGPD e la notifica/comunicazione ai sensi dei commi 1022 e 1023 della Legge di Bilancio 2018), si potrà comprendere la situazione di grave confusione e conflitto applicativo:

L'art. 35 del RGPD – come visto – prevede che quando il trattamento si basa sull'utilizzo di nuove tecnologie e considerati la natura, l'oggetto, il contesto e le finalità del trattamento può presentare un rischio *elevato* per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve effettuare, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali, procedendo al relativo *assessment* del rischio. L'obbligo di DPIA non è generalizzato: valutazioni e relativo *assessment* vanno effettuati solo se il rischio è *elevato*. In tale fase non vi è alcun obbligo di notificare/comunicare alcunchè all'autorità di controllo, né è implicato l'interesse legittimo come base giuridica del trattamento.

Al contrario, il comma 1022 della Legge di Bilancio obbliga il titolare (nuovamente definito grossolanamente "*titolare dei dati personali*", con inutile quanto pedissequo riferimento all'articolo 4, numero 7), del "*regolamento RGPD*") che proceda ad un trattamento mediante utilizzo di nuove tecnologie o strumenti automatizzati e giuridicamente fondato sul proprio interesse legittimo a darne tempestiva comunicazione al Garante per la protezione dei dati personali utilizzando il modello di "*informativa*" per illustrare oggetto, finalità e contesto del trattamento (in tale prospettiva alcuni primi commentatori hanno parlato di reintroduzione dell'obbligo di notificazione del trattamento, anche se in realtà è più corretto rapportare l'obbligo procedurale di cui ai commi 1022 e 1023 agli attuali istituti di interpello, istanze di riconoscimento di interesse legittimo o richieste residuali di autorizzazione al Garante). Trascorsi quindici giorni lavorativi dall'invio dell'informativa (non è dato sapere in quali modalità pratiche, se si utilizzerà ad esempio la stessa piattaforma *web* attuale per l'invio al Garante del modello di notificazione sottoscritto con firma digitale), in assenza di risposta da parte del Garante, il titolare potrà procedere al trattamento.

In sostanza, rispetto all'art. 35 RGPD, la procedura del comma 1022 introduce un obbligo di immediata interlocuzione con l'autorità di controllo (che invece l'art. 36 RGPD prevede sia obbligatoriamente coinvolta solo se il titolare del trattamento, all'esito dalla valutazione di impatto preventiva, ritenga di non essere in grado di gestire l'elevato rischio per l'interessato). Inoltre, mentre la DPIA va condotta in caso di impiego di nuove tecnologie, la procedura del comma 1022 amplia i presupposti: non solo l'utilizzo di nuove tecnologie, ma anche il più ordinario impiego di qualsiasi strumento automatizzato nel trattamento obbliga il titolare (che persegua un proprio interesse legittimo) a informare il Garante, e, inoltre, ciò indipendentemente dall'impatto e dal rischio (anche non *elevato*) che il trattamento possa comportare sulla sfera dell'interessato. Più limitato appare invece il presupposto giuridico: mentre la DPIA è obbligatoria indipendentemente dalla base giuridica del trattamento (che può essere rappresentato dal consenso dell'interessato, dall'obbligo di adempimento di un contratto, dalla necessità di rispettare norme di legge, etc) e solo ove il rischio sia *elevato*, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, la procedura di comunicazione al Garante di cui al comma 1022 è obbligatoria solo se il trattamento è basato sull'interesse legittimo del titolare del trattamento. Anzi: è proprio la valutazione dell'interesse legittimo che costituisce oggetto e finalità dell'intervento del Garante.

Diversi anche i gli effetti e gli esiti delle due procedure: intanto, in base alla procedura del comma 1022, il mero invio della *informativa* al Garante fa decorrere in automatico un periodo di quindici giorni alla scadenza del quale – in assenza di risposta – il titolare può procedere al trattamento. Non si tratta di un meccanismo di silenzio–assenso, in quanto, in base al successivo comma 1023, il Garante può poi sospendere e definitivamente bloccare il trattamento. Difatti, l'Autorità effettua una istruttoria sulla base dell'informativa ricevuta dal titolare e ove ravvisi il rischio che dal trattamento derivi una lesione dei diritti e delle libertà dei soggetti interessati in prima battuta dispone la moratoria del trattamento per un periodo massimo di trenta giorni (con gli immaginabili danni che ciò può comportare al titolare del trattamento che abbia nelle more avviato il trattamento dopo i quindici giorni…). In tale periodo, il Garante può chiedere al titolare ulteriori informazioni e integrazioni, da rendere tempestivamente, e, qualora ritenga che dal trattamento derivi comunque una lesione dei diritti e delle libertà del soggetto interessato, dispone l'inibitoria (definitiva) all'utilizzo dei dati. Manca inoltre del tutto la disciplina dell'esito positivo della istruttoria: non è dato comprendere cosa accada qualora il Garante ritenga che dal trattamento non derivi alcuna lesione dei diritti e delle libertà del soggetto interessato: vi è formale comunicazione/autorizzazione al titolare del trattamento con specifico provvedimento? Deve ritenersi di sì: lo si deduce indirettamente dal successivo comma 1024 che obbliga il Garante nella relazione annuale al parlamento a dare conto "*dei provvedimenti conseguentemente adottati*". Nella procedura introdotta dai commi 1022 e 1023 non vi è infine alcun ruolo "positivo" di consulenza e assistenza al titolare del trattamento da parte del Garante, ruolo invece specificatamente costruito dal Legislatore UE con l'art. 36 RGPD. In base a tale disposizione, difatti, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, l'autorità di controllo – lungi dal sospendere, bloccare, etc – rilascia un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento, con il quale – presumibilmente – fornisce indicazioni, misure e

cautele aggiuntive per l'*assessment* di quell'*elevato* rischio che preliminarmente il titolare del trattamento non aveva ritenuto di poter autonomamente porre in essere.

§ 2.5 Segue - Commento ai commi 1024 e 1025: la "pubblicità" della nuova procedura nella relazione annuale al Parlamento.

Il Legislatore italiano attribuisce una tale (poco comprensibile) importanza alla procedura di cui ai commi 1022 e 1023 da prevedere uno specifico obbligo istituzionale in capo all'Autorità: ai sensi del comma 1024, difatti, il Garante per la protezione dei dati personali "*dà conto dell'attivita' svolta ai sensi del comma 1023 e dei provvedimenti conseguentemente adottati nella relazione annuale*". Dunque per ogni informativa e comunicazione ricevuta da qualsiasi titolare del trattamento ai sensi del comma 1022, l'Autorità dovrà specificamente illustrare nella relazione annuale non solo i contenuti dell'istruttoria svolta caso per caso, ma anche il relativo esito e provvedimento singolarmente adottati. Con tutto l'onere amministrativo che ciò potrà comportare, ove – presumibilmente – saranno assai elevate le comunicazioni obbligatorie dei titolari del trattamento. Francamente non si comprende la finalità di una tale disposizione: è come se nella relazione annuale trovasse posto una sorta di Registro Generale dei trattamenti basati sull'interesse legittimo…
Ai fini dell'attuazione dei commi 1020, 1021, 1022, 1023 e 1024, infine, il comma 1025 autorizza una spesa annuale di 2 milioni di euro annui a decorrere dall'anno 2018.

§ 3. Conclusioni.

E' talmente incongruente, disorganico e confusionario l'intervento attuato con i commi da 1020 a 1025 della Legge di Bilancio 2018 da rendere auspicabile che l'esercizio delle delega generale prevista dall'art. 13 della Legge di delegazione europea per il coordinamento al RGPD della normativa italiana sulla *data protection* – a partire dal Codice della privacy – porti a modificare i commi sopra analizzati, risolvendo criticità e conflitti che l'inopinata normativa ha determinato. Ciò sarebbe possibile nella parte in cui l'art. 13 prevede il coordinamento delle disposizioni vigenti in materia di protezione dei dati personali contenute in altre leggi diverse dal Codice della privacy con le disposizioni del GDPR.
Tra l'altro, come notazione conclusiva, si noti che in caso di violazione degli obblighi di comunicazione posti ai titolari del trattamento ai sensi del comma 1022, non vi sarebbe alcuna specifica sanzione, a meno di non volere rendere interpretativamente ed analogicamente applicabile l'art. 164 del Codice della privacy (chiunque omette di fornire le informazioni… è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro).