COMMISSIONE SPECIALE PER L'ESAME DEGLI ATTI URGENTI PRESENTATI DAL GOVERNO (SENATO)

COMMISSIONE SPECIALE PER L'ESAME DEGLI ATTI DEL GOVERNO (CAMERA)

AUDIZIONE DELL'AVV. GIANLUCA DE CRISTOFARO NELL'AMBITO DELL'ESAME DELL'ATTO DEL GOVERNO N. 22

Schema di Decreto Legislativo recante disposizione per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

7 giugno 2018

Palazzo Carpegna

Via degli Staderari, 4 – Roma

LCA STUDIO LEGALE
www.lcalex.it

MILANO
Via della Moscova 18
20121 Milano
T +39 02 7788751
F +39 02 76018478
milano@lcalex.it

GENOVA
Via Fieschi 3/13
16121 Genova
T +39 010 5956039
F +39 010 5370804
genova@lcalex.it

TREVISO
Via Sile 41
31056 Roncade (TV)
T +39 0422 789511
F +39 0422 789666
treviso@lcalex.it

DUBAI
IAA Middle East Legal Consultants LLP
Liberty House, Office 514, DIFC
P.O.Box 506949 Dubai
T +971 4 3860090 - F +971 4 3860091
dubai@lcalex.it

member of ASLA

Illustri Senatori e Deputati,

Vi ringrazio, innanzitutto, per l'invito a queste audizioni che mi consente di condividere alcuni spunti critici e suggerimenti sullo schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679.

Vorrei muovere dalla premessa che il compito affidato al legislatore italiano è, forse più che in altri casi, estremamente difficile. Innanzitutto, perché il GDPR - in alcuni aspetti specifici e nel suo impianto generale - ha dato il via ad una "rivoluzione copernicana" del settore della protezione dati personali e a un cambio culturale. In secondo luogo, perché l'obiettivo del GDPR è, come noto, quello di bilanciare la tutela del diritto alla protezione dei dati personali con il principio della libera circolazione degli stessi.

Il legislatore nazionale (insieme a quello comunitario) ha, quindi, l'onere di trovare il punto di equilibrio tra le due esigenze anzidette.

Come già evidenziato da altri (penso, ad esempio, al Senatore Caliendo), l'imposizione di limiti eccessivi alla libera circolazione dei dati, rischia di avere effetti dannosi sulla capacità concorrenziale di un determinato paese rispetto ad altri che decidano di non imporre limiti ulteriori a quelli previsti dal GDPR.

E questo è, a mio avviso, il più rilevante punto di attenzione davanti a un mondo ormai sempre meno locale/nazionale (su questo aspetto tornerò anche nel prosieguo).

La seconda (e ultima) premessa è che i rilievi di cui sotto traggono origine dall'esperienza maturata in questo ultimo anno e mezzo in cui, con i miei colleghi, ho accompagnato passo-passo le imprese nel percorso di adeguamento al GDPR.

Peraltro, assistendo, oltre a piccole-medie imprese e grandi imprese italiane, anche filiali italiane di multinazionali straniere, sono stato coinvolto in processi di adeguamento *cross-border* e ho quindi avuto contezza di come gli altri Paesi stanno approcciando (dal punto di vista delle imprese) e interpretando (dal punto di vista del legislatore e dell'autorità di controllo) il GDPR.

E qui ripeto ancora una volta quanto sia importante evitare di porre limiti (o guarentigie) ulteriori o eccessive – rispetto a quelle imposte dagli altri paesi - che possano mettere in difficoltà le nostre imprese oppure rendere meno *appealing* il nostro Paese da parte delle multinazionali straniere.

Il mio primo punto è, quindi, legato al potere prescrittivo/autorizzativo che su alcuni aspetti lo schema di decreto pare demandare al Garante. Pensiamo, ad esempio, alle autorizzazioni generali per il trattamento delle categorie particolari di dati (già dati sensibili).

Il mio timore è:

- da un lato, che attribuire un ampio potere al Garante finisca per entrare in contrasto con i principi del GDPR e, soprattutto, con quello dell'*accountability*;
- dall'altro che i provvedimenti prescrittivi/autorizzativi del Garante possano – almeno in una prima fase – bloccare l'operatività delle imprese (in attesa dell'autorizzazione/del provvedimento) e prevedere quei limiti eccessivi di cui parlavo sopra, e ciò perché è troppo facile incorrere nel rischio di trovarsi legati a principi espressi in provvedimenti del passato che oggi, però, non dovrebbero più trovare applicazione.

Sotto quest'ultimo aspetto molti consulenti italiani fanno ancora fatica ad abbandonare quel famoso termine massimo di 24 mesi per i trattamenti per finalità di marketing previsto da un provvedimento del 2005 sulle carte fedeltà.

Quanto sto dicendo potrebbe anche sembrare in contrasto con gli interessi delle imprese (e, indirettamente, di noi consulenti) ad avere regole chiare o un perimetro "certo" in cui muoversi.

Ma è il GDPR che, con l'ormai noto principio di *accountability*, affida alle imprese l'onere di "responsabilizzarsi" individuando misure adeguate e di porre in essere, ove necessario, un bilanciamento tra interessi, in qualche misura, contrapposti.

Peraltro, come detto, il GDPR richiede un cambio culturale; e attribuire al Garante un ampio potere prescrittivo/autorizzativo (che finisce per dire – od ordinare - alle imprese cosa fare) non contribuisce certamente ad accelerare il processo verso questo cambio di cultura.

Gli interventi del Garante dovrebbero avere carattere interpretativo/integrativo del GDPR e del rinnovato Codice Privacy ed essere quindi limitati - tutt'al più - a provvedimenti di indirizzo, a linee-guida volte ad evitare che l'*accountability* diventi un arbitrio o si risolva in un'incertezza giuridica di fondo.

Meglio attendere un po' di più, e avere un Codice Privacy che insieme al GDPR possa considerarsi autosufficiente, piuttosto che modificare il Decreto Legislativo prima ma demandando al Garante tutta una serie di interventi, come anche quelli di semplificazione. L'esperienza di questi anni lo ha insegnato: il Garante non ha le risorse, per attivarsi tempestivamente, e forse nemmeno la volontà, di modificare i propri orientamenti per meglio seguire l'evolversi della società.

Insomma, la mia idea è che **per consentire il cambio culturale e garantire l'uniformità giuridica a livello Europeo, è necessario in generale limitare l'intervento nazionale** (sia del Garante che del legislatore) **ai profili strettamente necessari all'attuazione della disciplina europea, evitando di introdurre limiti ulteriori/eccessivi**.

L'intervento, sia del legislatore, sia del Garante, dovrebbe essere indirizzato a chiarire e a semplificare gli adempimenti a carico dei titolari.

***

Premesso quanto sopra, di seguito alcuni rilievi specifici:

1. Art. 22, comma 5: viene mantenuta l'applicazione dell'art. 1, commi da 1022 a 1023, della legge 27 dicembre 2017, n. 205, che prevede specifici obblighi a carico dei titolari che intendano svolgere un trattamento dati fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati, limitandola ai trattamenti dati relativi a minori ed ai dati raccolti *online*.

   Tale previsione, prevedendo un controllo preliminare del Garante, si pone, a mio avviso, in contrasto con il principio di accountability e con il considerando 89 del GDPR, oltre che con l'obiettivo, già più volte richiamato, di garantire l'uniformità giuridica nell'UE.

   Assistendo nel percorso di adeguamento al GDPR multinazionali straniere che offrono prodotti e servizi ai minori in tutta Europa ci si rende conto che l'impresa dovrebbe bloccare l'attività, limitatamente all'Italia, in attesa del controllo preliminare del Garante.

2. Art. 2-*quinquies*: sul tema minori, condivido il parere reso dal Garante il 22 maggio 2018, laddove suggerisce di abbassare l'età per la prestazione di un valido consenso ai sensi della normativa in materia di protezione dati personali a 14 anni: e ciò sia perché tutti sappiamo che i bambini imparano ad usare *smartphone* e *tablet* a un'età ben più giovane (ed è irrealistico credere di poter subordinare l'accesso a *social network* all'acquisizione del consenso dei genitori), sia perché in questo modo ci si allineerebbe alla Legge 29 maggio 2017 n. 71 recante "*Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*".

3. Art. 2-*quaterdecies*: lo schema prevede che il Garante possa emanare d'ufficio provvedimenti di per prescrivere misure e accorgimenti da applicare a garanzia dell'interessato nei trattamenti svolti per l'esecuzione di un compito di pubblico interesse che presentano un rischio particolarmente elevato.
   Non vedo il motivo per cui attribuire al Garante questo potere e non lasciare, nuovamente, all'impresa/titolare il compito di svolgere una valutazione del rischio. E ciò sempre in virtù del principio di "responsabilizzazione" e sulla base delle considerazioni di cui sopra.

4. Art. 2-*terdecies*: nonostante la norma sembra voler eliminare o rendere facoltativa la nomina dei "vecchi" incaricati (figura tutta italiana che ha sempre costituito più un onere per le imprese che una forma di tutela per gli interessati), una interpretazione letterale e/o restrittiva della stessa potrebbe finire per aggravare gli adempimenti previsti a carico dell'impresa/titolare. La norma parla, infatti, di "autorizzare al trattamento" (v. secondo comma). Sarebbe opportuno che la norma prevedesse – espressamente – che tra "le modalità più opportune che il titolare può adottare ci fosse anche l'autorizzazione verbale o implicita nel proprio contratto di lavoro sulla base delle mansioni assegnate al dipendente.

Come detto sopra, anche in questo caso, non prevedere alcunché in integrazione a quanto previsto dall'art. 29 del GDPR – lasciando all'impresa/titolare decidere sulla propria organizzazione interna - potrebbe essere la scelta più appropriata, a condizione che si decida di "cambiare rotta" rispetto al passato, abbandonando l'idea che le formalità e la burocratizzazione portino a una maggiore tutela degli interessati.

5. Art. 18, comma 1: il termine per la definizione dei procedimenti sanzionatori da parte del Garante dovrebbe essere individuato nella data di effettiva applicazione del GDPR, ossia il 25 maggio 2018.

6. Art. 22, comma 4: Nonostante abbia suggerito più volte che la strada dovrebbe essere quella di ridurre al minimo l'intervento del Garante, l'auspicio è che venga, comunque, chiarito il prima possibile quali provvedimenti del Garante - la cui efficacia è stata confermata nella misura in cui sono compatibili con il GDPR e con il Codice Privacy - rimarranno in vigore. Sarebbe preferibile evitare che il Garante possa (o debba) emettere delle nuove autorizzazioni generali.

7. Art. 11: non è chiara la *ratio* dell'abrogazione dei provvedimenti del Garante sui *cookies* che consentono modalità semplificate di fornitura dell'informativa, quantomeno fino all'approvazione dell'*e-privacy regulation*.

8. Art. 2-ter: la norma fornisce una definizione di "comunicazione" (non fornita, invece, direttamente dal GDPR – v. art. 3). Andrebbe specificato se tale definizione è applicabile esclusivamente ai trattamenti descritti dall'art. 2-ter.

9. Definizione di "interessato": già da diversi anni, le persone giuridiche sono state formalmente escluse della definizione di "interessato". All'inizio, si è gridato alla semplificazione: salvo, poi, rendersi conto che, di fatto ed inevitabilmente, gli interessati continuano a comprendere anche le persone giuridiche.
   Tralasciando il fatto che il trattamento dei dati di una persona giuridica comporta sempre il trattamento dei dati almeno di una persona fisica (*i.e.*, il legale rappresentante), il Garante non ha mancato di precisare che **(i)** gli indirizzi email riferibili ai dipendenti, seppur aventi dominio aziendale, sono e restano dati personali, e che **(ii)** le disposizioni del capo 1 del titolo X del Codice Privacy si applicano anche alle persone giuridiche. Il chiaro risultato è che le società che offrono servizi B2B hanno, di fatto, gli stessi obblighi delle società attive nel settore B2C, e devono necessariamente fornire un'informativa ad ogni contatto (persona fisica) della propria controparte contrattuale (persona giuridica) con il quale si interfacciano. Irrealistico, a dir poco, pensare che tale obbligo sia onorabile.
   Prevedere chiaramente che fornire l'informativa alla controparte contrattuale basti anche ad informarne il personale che sarà coinvolto nel rapporto contrattuale, significherebbe ridurre

le tutele per gli interessati? No: significherebbe renderle più effettive, perché l'obbligo a carico dei titolari sarebbe eseguibile e verrebbe sicuramente eseguito (essendo semplificato). Il legislatore ha, ora, l'occasione di introdurre una deroga espressa, che si ritiene utile precisare essere omnicomprensiva ed estesa, quindi, al marketing.
Anche la definizione di "contraente", che comprende nell'attuale versione dello schema di decreto legislativo le persone giuridiche, potrebbe essere oggetto di eventuali semplificazioni.

10. Dati personali di terzi: alcune professioni, come quelle consulenziali, possono comportare la ricezione e il trattamento di dati di soggetti terzi, come la controparte del cliente o ancora i dipendenti del cliente. Si auspica che venga espressamente introdotta una deroga dall'obbligo di informare tali terzi del trattamento dei dati, non solo come misura di semplificazione, ma anche per assicurare il rispetto degli obblighi di riservatezza derivanti dall'incarico professionale.

11. Registro delle opposizioni: premesso che la legge 11 gennaio 2018 n. 5 rinvia, per le definizioni, all'art. 4 dell'attuale d.lgs. 196/2003 che sarà abrogato, stando all'attuale versione del disegno di legge, la legge n. 5/2018 impone a ogni titolare di verificare mensilmente il registro delle opposizioni, verificando che nessun interessato abbia revocato "implicitamente" il consenso al marketing telefonico iscrivendosi al registro dopo la prestazione del consenso stesso. Si tratta di un onere estremamente gravoso.
Peraltro, non è chiaro se il riferimento al consenso a cui si riferisce la legge n. 5/2018 debba essere inteso in senso restrittivo, o se l'adempimento debba invece estendersi anche al marketing telefonico che trova legittimazione in altre basi giuridiche, come ad esempio il legittimo interesse.
Nonostante i temi di cui sopra non siano oggetto di specifiche previsioni dello schema di decreto legislativo, qualora non ci fossero temi di "eccesso di delega", sarebbe opportuno cogliere l'occasione per intervenire.

12. Soft spam e art. 130 Codice Privacy: il decreto legislativo potrebbe cogliere l'occasione per coordinare l'eccezione c.d. soft spam con l'art. 6 del GDPR. Qual è la base giuridica di un trattamento che trova la propria legittimazione in una deroga legislativa espressa? Ad oggi si è quasi obbligati a ricorrere al legittimo interesse: ma sarebbe apprezzabile che il legislatore lo precisasse, del caso esentando i titolari dall'onere di eseguire un bilanciamento già fatto dal legislatore.

***

Ringraziando nuovamente per l'opportunità.

Roma, 7 giugno 2018

Avv. Gianluca De Cristofaro