ASSOTELECOMUNICAZIONI
ASSTEL

ADERENTE A CONFINDUSTRIA E CONFINDUSTRIA DIGITALE

Documento di Audizione di Assotelecomunicazioni-Asstel sullo schema di decreto legislativo A.G. n. 22 – "adeguamento normativa nazionale circa la protezione delle persone fisiche con riguardo al trattamento dei dati personali"

Commissioni Speciali congiunte

Roma, 31 maggio 2018

Sommario

A cura di Marzia Minozzi

Responsabile Normativa e Regolamentazione

Assotelecomunicazioni-Asstel

Premessa: presentazione di Assotelecomunicazioni-Asstel e oggetto dell'audizione

Asstel è l'Associazione di categoria che, nel sistema di Confindustria, rappresenta le imprese della tecnologia dell'informazione esercenti servizi di telecomunicazione fissa e mobile, attive nell'assistenza e gestione della clientela, che forniscono apparati e servizi di gestione, manutenzione ed esercizio di impianti e reti di telecomunicazione, caratterizzate dallo sviluppo e implementazione di servizi per soluzioni tecnologiche applicate anche alle telecomunicazioni e di servizi per contenuti digitali e multimediali.
Le imprese rappresentate da Asstel occupano circa 130.000 addetti.
Assotelecomunicazioni-Asstel è socio fondatore di Confindustria Digitale.
Il tema in discussione riguarda aspetti estremamente sensibili del business rappresentato da Asstel e ringraziamo quindi sentitamente della possibilità concessaci di intervenire in questa sede.

Le Considerazioni di Asstel sullo schema di d. lgs. in discussione

L'Associazione rinvia al contributo espresso da Confindustria per le considerazioni di carattere più generale ed esprime qui l'apprezzamento per l'adeguamento ordinato del quadro normativo nazionale rispetto a quello predisposto dal Regolamento Europeo realizzato con il decreto legislativo in commento.
Si coglie altresì l'occasione per rimarcare che la tempistica di elaborazione e perfezionamento del decreto avrebbe invece dovuto seguire ben altro calendario: Confindustria Digitale ed Asstel hanno sollecitato, verso le istituzioni competenti ma senza esito, l'attuale discussione sin dalla pubblicazione, nel 2016, del Regolamento Generale per la Protezione dei Dati Personali nella Gazzetta Ufficiale delle Comunità Europee (anche GDPR); un più sollecito adeguamento del quadro normativo nazionale a tutela della protezione dei dati a quanto definito dal Regolamento sarebbe stato ottimale per consentire alle imprese di operare in condizioni di certezza nello svolgimento di tutte le analisi ed azioni necessarie per assicurare la conformità dei propri comportamenti a quanto previsto dal Regolamento entro il termine del 25 maggio u.s..

Ricordiamo infatti che la "rivoluzione copernicana" rispetto al tema della tutela dei dati personali introdotta dal Regolamento, che ha responsabilizzato fortemente i titolari dei trattamenti rispetto ad un precedente approccio più formale, ha richiesto un enorme sforzo di compliance alle imprese.

Segnaliamo che per quanto riguarda le imprese di telecomunicazioni tale sforzo potrebbe non terminare con l'adeguamento al GDPR, dato che è in iter comunitario un altro Regolamento, cosiddetto e-privacy, che andrà nuovamente ad incidere sulla tutela dei dati personali nell'esercizio delle reti e servizi di comunicazione elettronica. Segnaliamo tale circostanza perché rischia di vanificare, almeno parzialmente, nel breve periodo azioni di compliance messe in atto e accrescere – senza un beneficio correlato – i costi improduttivi a carico delle imprese.

La discussione sul Regolamento e-privacy è ancora in corso, quindi la considerazione appena esposta non ha ricadute dirette giuridiche e testuali sullo schema di decreto legislativo in discussione se non per quanto diremo nel seguito sul tema delle sanzioni, tuttavia sembra opportuno segnalare questo elemento in vista degli sviluppi futuri delle misure di attuazione del GDPR e della definizione del nuovo Regolamento e-privacy e della posizione nazionale nel negoziato comunitario.

In particolare, si segnala la necessità la necessità che le due norme (GDPR ed e-Privacy) garantiscano un necessario sistema di coordinamento funzionale al fine di evitare il rischio di pericolose sovrapposizioni di sanzioni.

La relazione del GDPR con l'e-privacy

Fino all'attesa adozione del nuovo Regolamento Europeo[1] e-Privacy, resterà in vigore la Direttiva e-Privacy (2002/58/CE e s.m.i.) relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e continueranno quindi ad essere in vigore le norme recepite all'interno del titolo X del nostro Codice Privacy (ovvero dall'art. 121 all'articolo 134 del Codice Privacy), che vengono armonizzate con il GDPR dal d. lgs. in discussione.

L'istanza a questo riguardo è quindi quella di limitarsi all'adeguamento minimo al GDPR, in vista dell'arrivo del Regolamento e-privacy, e di adoperarsi per evitare quanto più possibile sovrapposizioni tra i due Regolamenti.

[1] Proposta di regolamento COM(2017) 10, presentata dalla Commissione Europea il 10 gennaio 2017

Un ultimo appunto a questo riguardo è relativo alla necessità di assicurare un campo da gioco livellato agli attori del digitale: questo sarà possibile solo attenendosi quanto più possibile al Regolamento Generale per la Protezione dei Dati anche nella definizione della disciplina dell'e-privacy, che deve avere un contenuto assolutamente minimale.

Esprimiamo quindi un generale apprezzamento per l'impostazione del d. lgs., che abroga e modifica selettivamente quegli articoli del Codice per la protezione dati personali su cui ha inciso il GDPR e segnaliamo pochi punti specifici che suscitano preoccupazione.

La conservazione dei dati di traffico

Lo schema di Decreto, nel confermare la disposizione introdotta con la c.d. Legge europea 2017[2] prolungherebbe definitivamente fino a 72 mesi il termine di conservazione dei dati di traffico telefonico e telematico, nonché dei dati relativi alle chiamate senza risposta, per esigenze di indagine nel contrasto al terrorismo e di accertamento e repressione di reati di particolare gravità[3] cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale".
A questo riguardo, l'Associazione condivide integralmente le riserve espresse dal Garante per la Protezione dei Dati personali.
In conformità a quanto statuito dalla giurisprudenza europea[4], si osserva che la conferma di un arco temporale di conservazione così ampio determina rilevanti criticità in ordine al mancato rispetto del principio di proporzionalità tra esigenze investigative e le eventuali limitazioni del diritto alla protezione dati degli interessati.
Lo stesso Garante privacy, nel citato parere suggerisce di stralciare la norma in questione, altresì abrogando espressamente le connesse disposizioni contenute nella Legge europea 2017.

[2] L'articolo 11, comma 1, lett. i), numero 3, conferma la deroga all'articolo 132, commi 1 ed 1-bis del Codice, introdotta dall'articolo 24 della legge 20 novembre 2017, n. 167, recante "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017".
[3] Ai sensi degli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale sono: delitti di criminalità mafiosa o commessi con finalità di terrorismo, omicidio, estorsione aggravata, sequestro di persona a scopo di estorsione, armi ed esplosivi ad eccezione di alcune ipotesi, associazione finalizzata al traffico di stupefacenti, ecc
[4] Cfr. Corte di giustizia Ue con le sentenze Digital Rights Ireland (resa in data 8 aprile 2014 nelle cause riunite C-293/12 e C-594/12,) e Tele2 e Watson (resa il 21 dicembre 2016, nelle cause riunite C 203/15 e C 698/15).

Dal punto di vista degli Operatori di telecomunicazioni si sottolinea che la disposizione in questione impone oneri di attuazione quantificabili in decine di milioni di EURO a carico degli attori del mercato, oneri che non troverebbero compensazione in alcuna voce, alla luce dell'orientamento recentemente espresso dal Ministero della Giustizia di escludere tali oneri dal ristoro dei costi per le prestazioni obbligatorie, con effetti negativi sui conti degli Operatori e sull'attrattività degli Investimenti nel nostro Paese, non solo per l'ammontare ma soprattutto per la disparità di trattamento rispetto ad altri Paesi dell'Unione Europea.

La definizione dell'età del consenso

L'articolo 8 del GDPR tutela il minore da chi si rivolge direttamente a lui per offrire servizi della società dell'informazione che richiedono, prescrivendo che tali atti, per essere legittimamente posti in essere, richiedono il suo consenso informato. Consenso che, per i minori di 16 anni deve essere ottenuto da chi esercita la potestà genitoriale, fatta salva per ciascun Stato membro la possibilità di diminuire il limite previsto fino a 13 anni.

La Commissione incaricata di redigere la bozza di decreto legislativo di recepimento del GDPR, nello schema presentato al Ministro della Giustizia per l'attuazione della delega relativa all'adeguamento della legge italiana al GDPR, aveva suggerito di fissare in 14 anni l'età minima per l'accesso a tali servizi nei casi previsti dall'art.8.

L'articolo 2-quinquies dell'ultima versione del Decreto in circolazione reintroduce tuttavia il limite dei 16 anni per prestare un valido consenso al trattamento dei propri dati in tale ambito.

Sul punto, l'Associazione ritiene pienamente condivisibile il parere del Garante del 22 maggio 2018 n. 312 (anche "Parere"), secondo cui il limite prescritto non appare coerente con altre disposizioni dell'ordinamento che individuano a quattordici anni il limite di età consentito per esercitare determinate azioni giuridiche; diverse disposizioni del nostro Ordinamento consentono al minore infra sedicenne di esercitare i diritti previsti a propria tutela: si ricorda il caso delle disposizioni sul cyberbullismo[5] o del consenso ai fini di un'adozione[6].

[5] v. art. 2, c. 1, l. n. 71 del 2017
[6] art. 7, c. 2, l. n. 184 del 1983

Prevedere un limite più stringente per iscriversi, ad esempio, ad un social network non sarebbe coerente con tali precedenti e avrebbe anche effetti negativi rispetto proprio alla tutela dei minori; infatti, aumentare l'età del consenso:

- incoraggerà i minori a mentire sulla loro età, scoraggiando al contempo la creazione di contenuti e servizi previsti per un età inferiore ai 16 anni;
- creerà ulteriori problemi agli adolescenti che utilizzano internet, dal momento che si rischia di privarli dell'accesso alla maggior parte dei servizi online. Infatti, le definizioni di "trattamento" e "dati personali" introdotte dal Regolamento sono talmente ampie che includono tutto ciò che i minori fanno online, dall'acquisto di un regalo di natale per i loro genitori alle ricerche per un progetto scolastico, le email mandate agli amici o l'accesso a servizi di sostegno socio-psicologico. Inoltre, nel caso di minori che provengono da famiglie meno istruite e meno abituate al digitale, requisiti addizionali di controllo parentale potrebbero ottenere l'effetto opposto rispetto ad un obiettivo di maggiore tutela, impendendo loro di accedere ai servizi online legali;
- impedirà ai giovani di utilizzare Internet per scopi educativi, quando diverse ricerche dimostrano l'impatto positivo della didattica tramite servizi digitali, senza parlare del ruolo importante giocato dalla scuola nella formazione ad una navigazione sicura. Inoltre, imporre il consenso dei genitori prima che un insegnante possa utilizzare risorse formative online a scuola potrebbe avere un impatto negativo sui metodi didattici moderni.

Come dimostrato dalla lettera aperta inviata ai membri del Parlamento Europeo da una serie di associazioni, tra cui Telefono Azzurro per l'Italia, il Family Online Safety Institute e il Diana Award per il Regno Unito; Cyberhus per la Danimarca; Spunout per l'Irlanda, la maggior parte delle associazioni europee a tutela dei minori è contraria all'innalzamento dell'età del consenso a 16 anni per l'accesso ai servizi online[7].

Si noti, peraltro, che molti Paesi già si stanno orientando per esercitare tale deroga, fissando in molti casi l'età minima a 13/14 anni. E' il caso di Bulgaria, Cipro, Estonia, Irlanda, Portogallo, Slovenia, Belgio, Repubblica Ceca, Danimarca, Finlandia, Lettonia, Polonia, Spagna, Svezia e Regno Unito. Si suggerisce pertanto la fissazione a 14 anni quali il limite di età per la prestazione del consenso,

[7] http://www.antibullyingpro.com/blog/2015/12/11/letter-expressing-concern-to-the-draft-general-data-protection-regulation-13to16#sthash.excOK7cQ.dpuf,

coerentemente con le altre disposizioni dell'ordinamento volte a prevedere regimi di maggior tutela per i minori.

L'art. 132 ed il tema dell'impianto sanzionatorio per il Titolo X.

Le modifiche apportate dallo Schema di decreto legislativo all'articolo 132 sostanzialmente mirano a mantenere norme previgenti che non sono presenti nel GDPR; l'assetto risultante appare quindi conservativo dell'assetto attuale: non è particolarmente problematico, ma rappresenta un'occasione di semplificazione mancata ed è quello in cui si concentra maggiormente il rischio di andare in sovrapposizione con ulteriori sviluppi della normativa a protezione dei dati personali nelle comunicazioni elettroniche.

Si ripropone quindi la necessità di non apportare modifiche al Codice nella sezione servizi di comunicazioni elettroniche se non strettamente necessarie per garantire coerenza al GDPR.

In particolare la preoccupazione riguarda l'impianto sanzionatorio, su cui eventuali modifiche dovrebbeo essere adottate solo dopo l'approvazione del Regolamento e-Privacy, in modo da garantire alle imprese di telecomunicazioni un quadro normativo coerente, certo e prevedibile.

Si fa riferimento al fatto che nel set regolatorio risultante dal combinato disposto dello schema di d. lgs, e GDPR sarebbero assistite dalle sanzioni amministrative previste dal Regolamento tutte le violazioni riferibili al Titolo X del Codice, che non fa invece parte del Regolamento stesso: un esito divergente da quanto disposto dal GDPR e che sarà, appunto, aggiornato solo a valle della definizione del Regolamento e-privacy. Questa criticità è molto rilevante per le imprese di telecomunicazioni e andrebbe sanata nella versione definitiva del decreto legislativo in discussione, escludendo il riferimento agli articoli dal 122 al 132 dal testo dell'attuale art. 166 dello schema di d. lgs. e prevedendo il mantenimento, per il Titolo X del Codice per la protezione dati personali, del sistema sanzionatorio attuale.