AUDIZIONE DELL'ASSOCIAZIONE ITALIANA INTERNET PROVIDER

DOTT. GIULIANO CLAUDIO PERITORE – PRESIDENTE
ING. PAOLO NUTI - CONSIGLIERE

AUDIZIONI INFORMALI NELL'AMBITO DEL

DISEGNO DI LEGGE N. 2553
MODIFICHE AL CODICE DELLE COMUNICAZIONI ELETTRONICHE, DI CUI AL DECRETO LEGISLATIVO 1° AGOSTO 2003, N. 259, IN MATERIA DI OBBLIGO DI ATTIVAZIONE DEL SERVIZIO DI SAFETY CHECK

E DEL DISEGNO DI LEGGE N. 2575
DELEGA AL GOVERNO PER GARANTIRE IL CONSEGUIMENTO DELLA TRACCIABILITA' DELL'IDENTITA' DEGLI AUTORI DI CONTENUTI NELLE PIATTAFORME DI RETI SOCIALI

8^ COMMISSIONE DEL SENATO DELLA REPUBBLICA
28 GIUGNO 2017

PALAZZO CARPEGNA
VIA DEGLI STADERARI, 4 – ROMA

ASSOCIAZIONE ITALIANA INTERNET PROVIDER
c/o Studio Legale Valli & Ass. – Via del Governo Vecchio, 20 - 00186 Roma
Cod. Fis.: 97166260154 – P. IVA: 07549520968
Sito Web: www.aiip.it
E-mail: info@aiip.it
PEC: aiip.pec@unicert.it

AUDIZIONE DELL'ASSOCIAZIONE ITALIANA INTERNET PROVIDER

DOTT. GIULIANO CLAUDIO PERITORE – PRESIDENTE
ING. PAOLO NUTI - CONSIGLIERE

L'Associazione Italiana Internet Provider (AIIP) - che rappresenta circa cinquanta imprese abilitate a fornire al pubblico servizi di comunicazione elettronica, tra i quali, i servizi di accesso a internet ed altri servizi a banda larga e ultralarga – desidera innanzitutto ringraziare la Commissione per averle concesso l'opportunità di esprimere il proprio punto di vista sul **Disegno di legge n. 2553 (***Modifiche al Codice delle comunicazioni elettroniche, di cui al Decreto Legislativo 1° agosto 2003, n. 259, in materia di obbligo di attivazione del servizio di Safety Check*) e sul **Disegno di legge n. 2575** (*Delega al Governo per garantire il conseguimento della tracciabilità dell'identità degli autori di contenuti nelle piattaforme di reti sociali*).

Quanto al **DDL 2553**, in materia di Safety Check, è opinione di AIIP che il provvedimento debba rivolgersi quasi esclusivamente ad operatori di telefonia mobile stabiliti in Italia, o comunque dotati di un rappresentante legale in Italia.

Sotto il profilo pratico, l'operatore di telefonia mobile dispone infatti non solo di tecnologie di localizzazione del terminale mobile (telefono, *smartphone, tablet*) ma anche della possibilità di inviare messaggi al singolo terminale non solo sotto forma di SMS, ma anche, su un canale dedicato alle "notifiche" (p.e. "*la tua ricarica scade tra 2 giorni e sarà rinnovata automaticamente se disponi del credito sufficiente*").

La evidente delicatezza e criticità del Safety Check, infatti, sconsiglia di consentire a entità non soggette alla giurisdizione italiana e/o comunitaria di poter interagire direttamente con la popolazione. Un soggetto extra comunitario che ottenesse un titolo giuridico per inviare messaggi in situazioni di emergenza non sarebbe immediatamente perseguibile in Italia in caso di "falsi allarmi"

ASSOCIAZIONE ITALIANA INTERNET PROVIDER
c/o Studio Legale Valli & Ass. – Via del Governo Vecchio, 20 - 00186 Roma
Cod. Fis.: 97166260154 – P. IVA: 07549520968
Sito Web: www.aiip.it
E-mail: info@aiip.it
PEC: aiip.pec@unicert.it

generati da errori o da azioni dolose (anche di terzi, in caso di accesso abusivo ai sistemi di gestione del *Safety Check*).

Quale che sia la scelta del legislatore, ad ogni modo, è fondamentale che il *Safety Check* sia sottoposto all'adozione di stringenti misure di sicurezza e di effettivi controlli sul loro rispetto, in modo da minimizzare il rischio di utilizzi impropri e/o illegali del servizio in questione.

Sotto questo profilo vale tuttavia la pena di sottolineare che vi sono alcune "applicazioni" per *smartphone* prodotte e/o gestite anche da soggetti di diritto italiano che già oggi inviano notifiche anche su base geografica del tipo "*è in arrivo una nuova perturbazione*", "*c'e un terremoto nella zona di…*" o "*non perdere stasera la prima puntata del nuovo sceneggiato*" e che potrebbero utilmente essere cooptati nel servizio di allarme preventivo

Sotto il profilo dell'invio massivo di messaggi vocali, sia su rete fissa che mobile, che in prima battuta può sembrare utile a raggiungere la parte residua di popolazione che non utilizza tecnologie mobili, vale la pena di sottolineare che tale ipotesi rischia di non raggiungere l'obiettivo a causa della improvvisa saturazione dei canali trasmissivi dedicati alla voce che non sono dimensionati per sostenere una contemporaneità del 100%, saturazione di risorse che dovrebbero rimanere il più possibile disponibili agli utenti specialmente in situazione emergenziale.

Da ultimo, dobbiamo osservare, sia pure con rammarico, che I fornitori di servizi di accesso ad Internet possono dare un contributo esclusivamente "passivo" come canale trasmissivo dei servizi "OTT" (con le criticità giurisdizionali sopra menzionate) ma, salvo una residuale pubblicazione di allerte sulla propria "*home page*", non dispongono di tecnologie adatte all'invio di notifiche in quanto l'attivazione di tecniche di "*captive portal*" o di "*DNS poisoning*" rischia incidere negativamente sulla capacità dell'utente di accedere alle "*app*" e ai servizi "*social*" cui si collega abitualmente, se non addirittura di intralciare l'accesso ad Internet dei soccorritori, oltre a configurarsi come indebita intromissione in quella che dovrebbe essere, per definizione, un'agnostica trasmissione dati dell'utente.

@iip Associazione Italiana INTERNET Provider
ASSOCIAZIONE ITALIANA INTERNET PROVIDER
c/o Studio Legale Valli & Ass. – Via del Governo Vecchio, 20 - 00186 Roma
Cod. Fis.: 97166260154 – P. IVA: 07549520968
Sito Web: www.aiip.it
E-mail: info@aiip.it
PEC: aiip.pec@unicert.it

Quanto al **DDL 2575**, AIIP esprime la propria soddisfazione per il fatto che, finalmente, una proposta normativa recepisce con chiarezza il dettato di cui all'art. 27 comma I della Costituzione secondo il quale la responsabilità (penale) è personale.

I cittadini devono essere consapevoli che sono sottoposti alla legge e che rispondono in prima persona delle loro azioni anche quando utilizzano servizi di comunicazione elettronica.

Nello stesso tempo, essi devono sentirsi sicuri che le conseguenze dei loro comportamenti saranno valutate dalla magistratura (con tutte le garanzie giuridiche previste dalla Costituzione e dalle Leggi) e non da soggetti privati, come gli Internet Provider, che non possono e non devono rivestire il ruolo di "sceriffi della Rete".

Spiace solo che questo Disegno di Legge, che finalmente affronta in modo corretto il problema della responsabilità personale del “cittadino della rete” abbia solo tre firmatari, mentre, su un provvedimento di grande civiltà, sarebbe auspicabile una piena condivisione di tutte le forze politiche.

Evidentemente si tratta di un provvedimento impopolare, non gradito a quella parte della popolazione che, sentendosi protetta dall’ anonimato compie reati di varia gravità e lancia pietre sotto forma di parole. Sappiamo che, nei casi più gravi, si riesce spesso a risalire all’autore dell’illecito, ma qui siamo di fronte ad un problema di civiltà, perché l’impunità per alcuni ha sinora avuto come contraltare la censura per tutti.

AIIP ritiene che l'applicazione dei principi costituzionali in materia di responsabilità richieda l'effettiva adozione del cosiddetto "anonimato protetto", peraltro già previsto dal Regolamento generale sulla protezione dei dati personali all'articolo 4 comma I n. 5, in modo da bilanciare il diritto dei cittadini ad esprimersi liberamente, con il dovere di accettare le conseguenze delle loro azioni.

Di conseguenza, AIIP ritiene che un provvedimento normativo diretto a rendere consapevole il cittadino delle sue responsabilità nell'uso di servizi di comunicazione elettronica dovrebbe prevedere innanzi tutto l'attivazione, da parte degli *Over The Top* (i cosiddetti OTT), di sistemi di identificazione forte dei propri utenti.

@iip Associazione Italiana INTERNET Provider
ASSOCIAZIONE ITALIANA INTERNET PROVIDER
c/o Studio Legale Valli & Ass. – Via del Governo Vecchio, 20 - 00186 Roma
Cod. Fis.: 97166260154 – P. IVA: 07549520968
Sito Web: www.aiip.it
E-mail: info@aiip.it
PEC: aiip.pec@unicert.it

Mentre, infatti, gli operatori di accesso già identificano in modo certo i propri clienti, questo non accade necessariamente per gli OTT e in particolare per quelli che offrono servizi non a pagamento.

Sarebbe inoltre opportuno integrare le disposizioni del codice di procedura penale in materia di mezzi per la ricerca della prova informatica, prevedendo modalità che agevolino la richiesta e acquisizione di dati e informazioni presso gli operatori da parte dell'autorità giudiziaria.

Attualmente, infatti, il Codice di procedura penale prevede che anche la semplice acquisizione di file di log - fondamentali ai fini dell'identificazione del potenziale autore di un illecito - e degli altri dati di traffico sia documentata in verbali cartacei che costringono gli ufficiali di polizia giudiziaria a recarsi presso la sede dell'operatore e ad acquisire materialmente i dati in questione. Ci sono casi nei quali la polizia giudiziaria ha ottenuto via fax le informazioni di interesse, ma la giurisprudenza ha ritenuto irrituale questa modalità di acquisizione.

La numerosità e la complessità delle indagini relative ad abusi che coinvolgono servizi di comunicazione elettronica richiedono che, nel rispetto del diritto di difesa, l'autorità giudiziaria possa ricorrere a procedure più snelle e totalmente dematerializzate che consentirebbero maggiore efficienza e abbattimento di costi.

Sarebbe inoltre opportuno che il provvedimento di cui al DDL in commento si applicasse in generale a tutti i servizi Over The Top e non solo ai Social Network. Escludere piattaforme di "*e-commerce*", condivisione e pubblicazione di contenuti, messaggistica e in generale ciò che costituisce l'ecosistema digitale sarebbe una discriminazione che altera le dinamiche di mercato e riduce l'efficacia del provvedimento.

Inoltre, l'attuale normativa relativa alla conservazione dei dati di traffico si rivolge esclusivamente ai fornitori di servizi di comunicazione e non agli OTT. L'adeguamento di questa normativa suggerito dall'iniziativa legislativa, dovrebbe riguardare proprio gli OTT, attualmente non assoggettati al Codice delle Comunicazioni, e detentori di enormi moli di dati, e non introdurre ulteriori oneri verso i fornitori di servizi di comunicazione elettronica che già custodiscono, con un meccanismo rodato, i dati di traffico dei loro utenti necessari alle indagini.

@iip Associazione Italiana INTERNET Provider
ASSOCIAZIONE ITALIANA INTERNET PROVIDER
c/o Studio Legale Valli & Ass. – Via del Governo Vecchio, 20 - 00186 Roma
Cod. Fis.: 97166260154 – P. IVA: 07549520968
Sito Web: www.aiip.it
E-mail: info@aiip.it
PEC: aiip.pec@unicert.it

Ricordiamo a questo proposito, che il valore economico sviluppato dalla analisi con tecnologie tipiche dei "*big data*" sta spingendo I grandi OTT verso un modello economico sempre più simile l'uno all'altro: I portali di vendita si trasformano in portali di aste e distribuzioni di contenuti, i "social" si trasformano in produttori di contenuti e coì via. Non dimentichiamo poi che tutti questi servizi OTT sviluppano valore economico analizzando grandi masse di dati aggregati e per ciò stesso *formalmente anonimi*.

La sostanza però è in realtà molto diversa, perché o attraverso le modalità di pagamento o attraverso autenticazione a due fattori tramite telefono cellulare, praticamente tutte queste profilazioni possono diventare direttamente o indirettamente nominative.

@iip Associazione Italiana INTERNET Provider
ASSOCIAZIONE ITALIANA INTERNET PROVIDER
c/o Studio Legale Valli & Ass. – Via del Governo Vecchio, 20 - 00186 Roma
Cod. Fis.: 97166260154 – P. IVA: 07549520968
Sito Web: www.aiip.it
E-mail: info@aiip.it
PEC: aiip.pec@unicert.it