Senato della Repubblica

8ª Commissione (Lavori pubblici, comunicazioni)

Audizione del Presidente
Prof. Angelo Marcello Cardani

Esame dei disegni 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 n. 2575 (*Delega al Governo per garantire il conseguimento della tracciabilità dell'identità degli autori di contenuti nelle piattaforme di reti sociali*)

Mercoledì 23 maggio 2017
ore 14:00

Palazzo Carpegna
Via degli Staderari, 4 - Roma

Signor Presidente, Onorevoli Senatori,

ringrazio la Commissione per aver invitato in Audizione l'Istituzione da me rappresentata, e per l'opportunità che mi viene data di partecipare al dibattito in merito ai disegni di legge n. 2553 e n. 2575. Entrambi i testi investono temi di interesse per l'Autorità per le Garanzie nelle Comunicazioni.

1. **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*)**

L'iniziativa legislativa in esame propone alcune integrazioni e modifiche al Codice delle comunicazioni elettroniche (di seguito "Codice") al fine di generalizzare l'utilizzo della funzione di *safety check*. Tale funzione viene definita come "*un servizio di trasmissione dati monodirezionale verso utente che, in caso di emergenze connesse a calamità naturali o eventi di natura terroristica sul territorio nazionale, garantisce alle persone presenti in una determinata area geografica la possibilità di ricevere messaggi di emergenza e istruzioni di sicurezza*" (cfr. articolo 2 del ddl).

Si rappresenta, in via preliminare, la necessità che l'insieme delle proposte avanzate nel disegno di legge, con riguardo in particolare alle modifiche al Codice delle comunicazioni elettroniche relative all'ambito definitorio, agli obiettivi dell'attività di regolazione e ai nuovi obblighi previsti in capo ai soggetti regolati dal Codice medesimo, sia attentamente valutata sotto il profilo della coerenza con il diritto comunitario, che costituisce la "legislazione primaria" cui l'ordinamento nazionale deve sempre riferirsi.

Ciò detto, onde assicurare il servizio in esame, il ddl apporta una prima novità al Codice introducendo un ulteriore obiettivo rispetto a quelli che il Ministero dello sviluppo economico e l'Autorità sono già tenuti a realizzare. In particolare, si dispone che il Ministero e l'Autorità, nell'ambito delle rispettive competenze, promuovano gli interessi dei cittadini anche "*garantendo l'attivazione della funzione di safety check* […]" (cfr. articolo 4 del ddl).

La seconda novità riguarda, invece, le condizioni alle quali è sottoposto il rilascio dell'autorizzazione generale. Stando a quanto previsto dal ddl tra queste condizioni figurerà anche l'attivazione della funzione di *safety check* (cfr. articolo 9 del ddl). Quindi, gli operatori che intendono ottenere il rilascio dell'autorizzazione generale per la fornitura di reti o servizi di comunicazione elettronica dovranno garantire l'attivazione della funzione di *safety check*, così come definita dal ddl.

La funzione di *safety check*

Stando alla suddetta definizione prevista dall'articolo 2 del ddl, la funzione di *safety check* consiste in un trasferimento di dati monodirezionale verso utente. Sul punto appare opportuno un ulteriore sforzo definitorio finalizzato a chiarire meglio cosa debba intendersi per sistema monodirezionale verso utente per evitare l'insorgere di problemi interpretativi in sede di attuazione delle nuove disposizioni del Codice delle comunicazioni elettroniche. In particolare, sulla base di quanto affermato nella relazione illustrativa, sembrerebbe che il sistema debba implicare un ruolo attivo degli utenti, potendo essi "*rispondere con modalità semplici ed immediate*" al messaggio di

allerta. La definizione contenuta nell'art. 2 del disegno di legge in esame, invece, sembra far riferimento ad una funzione di *safety check* in cui il ruolo attivo è attribuito esclusivamente alle autorità pubbliche, chiamate ad inviare messaggi a carattere informativo agli utenti. In altri termini, non appare chiaro se la funzione in parola debba anche consentire agli utenti di rispondere a questi messaggi (come sembrerebbe emergere dalla relazione illustrativa), ad esempio fornendo conferma o meno del coinvolgimento diretto nell'evento, pur essendo nei pressi dell'area interessata. Ove si ritenesse necessario che il sistema di *safety check* debba prevedere anche questa modalità, bisognerebbe darne esplicita indicazione nell'articolato del ddl, dotando in tal caso la normativa degli strumenti minimi di tutela idonei ad impedire la diffusione di falsi allarmi e l'uso fraudolento o ingannevole della funzione.

Non si tratta del solo problema che riteniamo di porre all'attenzione sotto il profilo definitorio e delle specifiche tecniche del servizio, cosi come prospettato nel disegno di legge. Pur condividendo l'idea di conferire ad un successivo DPCM il compito di definire in dettaglio caratteristiche, modalità di prestazione e contenuti del servizio, crediamo che uno sforzo ulteriore debba essere compiuto già nel disegno di legge, sia in particolare nella individuazione della Autorità pubblica che sovraintende al servizio, sia anche sui vincoli cogenti che gravano in capo agli operatori che gestiscono reti di comunicazione elettronica, nonché infine sugli oneri e le competenze che l'articolato ripartisce tra i vari soggetti coinvolti.

La relazione illustrativa dà ampio spazio al sistema di *safety check* utilizzato da Facebook, che utilizza in larga misura l'interazione e la diretta collaborazione dei singoli utenti. Non è del tutto chiaro se l'intenzione dei proponenti è di ispirare il servizio a tale modello. Per un verso, infatti, se ne illustrano in dettaglio le caratteristiche, per altro verso sembra discostarsene laddove l'articolato pare escludere una funzione attiva dell'utente, privilegiando l'idea di un messaggio monodirezionale ispirato dall'Autorità pubblica che presiede al servizio. Si tratta di un aspetto che merita un chiarimento.

La questione delle modalità di espletazione del servizio non è secondaria in quanto, come vedremo meglio anche in seguito, un servizio prestato "sopra" le canoniche reti di comunicazione elettronica coinvolgerebbe fatalmente soggetti (i cosiddetti per l'appunto Over The Top OTT- segnatamente le grandi piattaforme digitali fornitrici di servizi ed *app*) non disciplinati, allo stato, dal Codice delle comunicazioni elettroniche, e servizi allo stato essi stessi estranei all'ambito di intervento del Codice medesimo.

Destinatari dell'obbligo

Dalla relazione illustrativa sembra emergere che l'obbligo di predisporre un sistema di *safety check* riguardi solo le imprese che offrono servizi di comunicazione mobile.

Nel testo della relazione si legge infatti che "*Il presente disegno di legge è volto ad integrare la disciplina prevista dal codice al fine di introdurre l'obbligo per tutte le reti di telefonia e internet in concessione di mettere a disposizione un canale safety*

check, mediante il quale gli operatori lanciano l'allerta verso i cellulari agganciati alle celle in una data area".

Poiché il servizio si pone l'importante obiettivo di mettere in sicurezza i cittadini nel corso di vari tipi di emergenze, in casi estremi salvando loro la vita, occorrerebbe, tuttavia, garantire il raggiungimento del maggior numero di cittadini nel più breve tempo possibile. A tale scopo, potrebbe essere necessario estendere l'obbligo anche agli operatori di rete fissa in modo che il messaggio di allerta (che nel caso di specie assumerebbe la forma di un messaggio vocale eventualmente preregistrato) possa raggiungere anche coloro che (per ragioni di scelta o per circostanze eccezionali) non dispongono di un dispositivo mobile. Inoltre, l'uso di un canale di comunicazione su rete fissa dovrebbe aumentare le possibilità di raggiungere i cittadini anche quando altri canali sono fuori servizio a causa dell'emergenza in atto.

Andrebbe meglio chiarito, infine, se tra le finalità del ddl ci sia anche quella di prevedere la possibilità che il servizio possa essere prestato tramite una specifica applicazione dedicata e, in tal caso, se debba trattarsi di una "*app* istituzionale". Si tratta di un tema il cui dettaglio tecnico non può che essere affrontato, eventualmente, in sede applicativa, ma su cui il testo della norma dovrebbe fornire una indicazione più esplicita. Naturalmente nella consapevolezza che le applicazioni in discorso (ossia i servizi comunemente conosciuti come "*app*"), di natura istituzionale o direttamente fornita da un *social network*, ove non avesse mero carattere di ausilio ai cittadini, senza vincoli di prestazione per gli operatori, richiederebbe un quadro regolatorio *ad hoc*

atteso che, come è noto, il Codice delle comunicazioni elettroniche non estende la sua disciplina ai cd. OTT.

Conclusioni

Il ddl *safety check* è una proposta che non può che trovare il favore dell'Autorità, in particolare laddove opportunamente chiariti gli aspetti che si ritiene di aver posto in luce. Immagino, infatti, che ci sia tempo e spazio per ulteriori riflessioni, in particolare all'esito dell'audizione delle altre Autorità pubbliche portatrici di specifiche competenze tecniche in materia.

2. 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*)

Il disegno di legge n. 2575, costituito da un solo articolo, contiene la delega al Governo ad adottare, entro dodici mesi dalla sua entrata in vigore, "(…) *uno o più decreti legislativi finalizzati al conseguimento della tracciabilità dell'identità degli autori di contenuti nelle piattaforme di reti sociali, anche al fine dell'intervento da parte delle autorità competenti in caso di reati commessi mediante internet (…) su proposta del Ministro della giustizia, di concerto con i Ministri dell'interno, delle infrastrutture e dei trasporti e dello sviluppo economico, sentito il Garante per la protezione dei dati personali (…)*".

A tale scopo, si propone l'introduzione di sistemi, di servizi tecnologici e di una idonea regolamentazione per rendere possibile la tracciabilità dell'identità degli autori di contenuti nelle piattaforme di reti sociali da parte delle Autorità competenti in caso di reati commessi mediante la Rete.

La premessa, scrivono i proponenti nella relazione, è che "*una certa notizia, una volta immessa nel circuito telematico, si diffonde rapidamente con modalità definite virali e diventa reperibile, a volte addirittura non tracciabile, a distanza di anni*".

Prevedere, quindi, sistemi e servizi tecnologici, nonché una adeguata regolamentazione che permettano la tracciabilità dell'attività dell'utente-autore è ormai priorità sia dal punto di vista sociale che normativo.

I possibili sistemi di identificazione si basano da un lato sull'identità che il soggetto comunica al *social network* al momento dell'iscrizione, dall'altro, sulla tracciabilità della connessione. La veridicità di detti dati non è verificata attraverso l'invio di documenti, ma, eventualmente, attraverso l'incrocio delle informazioni fornite e mediante la verifica dei contenuti caricati su altre piattaforme. Si tratta di un meccanismo che, oltre a sollevare perplessità sotto il profilo della proporzionalità, appare anche piuttosto complesso sotto il profilo procedurale.

L'identificazione attraverso la tracciabilità della connessione può incontrare numerose difficoltà tecniche: ogni dispositivo connesso è identificato da un proprio indirizzo IP, che consente, infatti, di conoscere solo il dispositivo da cui origina una connessione e risalire al soggetto che ne ha la responsabilità amministrativa, ma non all'effettivo

utilizzatore in un dato momento. Ciò è quanto può riscontrarsi, ad esempio, nella contestazione delle infrazioni al Codice della Strada, dove la targa di un veicolo consente di risalire al proprietario dello stesso, ma non permette di identificare il conducente, se non per presunzioni o espresse dichiarazioni di responsabilità da far pervenire alle competenti autorità.

In definitiva, un controllo preventivo sulla tracciabilità dell'utilizzo delle piattaforme in Internet, oltre che macchinoso, rischia di risultare sproporzionato nei riguardi dei cittadini, senza peraltro fornire adeguate certezze in ordine al conseguimento dei pur virtuosi obiettivi perseguiti. Per non dire che - secondo i dati a disposizione - molte delle condotte che il ddl intende perseguire sono perpetrate da giovani, in molti casi minorenni. Questa circostanza richiederebbe di spostare l'attenzione sugli aspetti legati alla formazione e al corretto sviluppo della personalità, piuttosto che su quelli meramente repressivi. Nel nuovo contesto tecnologico, l'istruzione scolastica andrebbe profondamente riformata, assicurando un adeguato livello di cultura digitale agli insegnanti e garantendo, in tal modo, la formazione digitale dei giovani, intesa non solo come padronanza delle tecnologie, ma, soprattutto, come piena consapevolezza della complessità dei linguaggi digitali e delle insidie connesse all'uso di tali linguaggi.

Le misure in parola, infine, andrebbero valutate senza trascurare le esigenze di tutela dei dati personali perseguite dal nostro ordinamento. Ne ha parlato in questa sede in modo puntuale ed approfondito il Presidente Soro. La proporzionalità tra le finalità perseguite ed i mezzi messi in campo per conseguirle deve essere in questo caso la sola

bussola. Al ddl è richiesto, al riguardo, uno sforzo di più accurata delimitazione dei suoi obiettivi, per evitare l'indeterminatezza dei fini e il rischio di una raccolta di dati invasiva e generalizzata.

Numerosi sono infatti i rischi per la protezione dei dati che derivano dall'impiego sempre più generalizzato di tecniche che consentono l'interazione e l'interconnessione di *device* di uso quotidiano, quali *smartphone*, *tablet* e pc, per non dire delle potenzialità ultra invasive degli strumenti di più recente ingresso nel mercato, come i dispositivi indossabili, di automazione domestica e di geolocalizzazione.

Ne risultano spesso vantaggi e semplificazioni d'uso che, tuttavia, comportano la raccolta, la registrazione e l'elaborazione di una grande quantità di informazioni relative a utenti spesso inconsapevoli.

Questi dati consentono non solo di costruire profili dettagliati delle persone, basati sui loro comportamenti, abitudini, gusti e perfino sul loro stato di salute, ma di effettuare anche un monitoraggio particolarmente invasivo sulla loro vita privata e di mettere in atto potenziali condizionamenti della loro libertà, peraltro basandosi su informazioni delle quali non è neppure possibile garantire l'affidabilità o il trattamento nel rispetto di rigorose misure di sicurezza.

Si tratta di questioni le cui implicazioni, afferenti prevalentemente al profilo della tutela della *privacy*, prescindono in larga misura dall'ambito di intervento dell'Autorità che presiedo. Ma che tuttavia non possiamo non vedere e valutare, come Agcom, allorchè appaiono suscettibili di orientare opinioni e comportamenti, o determinare condotte

economiche in contrasto con i principi di tutela dei consumatori e di parità di *chance* tra i soggetti che operano sul mercato. Al riguardo, sentiamo forte l'esigenza di un corretto bilanciamento tra la necessità di assicurare il più pieno dispiegarsi della libertà di pensiero dei cittadini e il dovere di garantire, al contempo, condizioni di tutela e sicurezza adeguate a tutti coloro che navigano sulla Rete.

Un profilo di stretto interesse per Agcom - che prescinde largamente dal *focus* del ddl in esame - è piuttosto quello del corretto utilizzo dei dati da parte delle grandi piattaforme digitali che li raccolgono e detengono. É quanto stiamo approfondendo con i nostri studi su "Big data" in via di conclusione proprio in queste settimane. Le modalità di utilizzo dei dati assumono particolare rilievo quando riguardano i minori.

Al momento non esistono norme che attribuiscano all'Autorità esplicite competenze in materia di tutela dei minori e dei diritti fondamentali della persona sulla rete Internet; è per questo che vorrei approfittare della mia presenza in questa sede per sensibilizzare il legislatore affinché valuti questa possibilità. Mi preme segnalare che, anche in assenza di esplicite competenze in materia, l'Autorità ha ritenuto opportuno istituire un Osservatorio permanente delle garanzie per i minori e dei diritti fondamentali della persona su Internet, con l'intento di monitorare la crescente diffusione di fenomeni quali l'istigazione all'odio, le minacce, le molestie, il bullismo, l'*hate speech* e la diffusione di contenuti deplorevoli.

Intendiamo aprire l'Osservatorio a soggetti esterni (Università, Istituti di ricerca, operatori del settore, esperti di pedagogia, giuristi, rappresentanti delle famiglie) e

veicolare su un apposito sito web tutte le segnalazioni ed iniziative intraprese da soggetti esterni.

A partire da quest'anno, inoltre, presenteremo un rapporto al Parlamento sull'attività dell'Osservatorio rafforzando un legame che, grazie alla sensibilità della Presidente Laura Boldrini, ha già consentito la realizzazione di un importante Workshop tenutosi alla Camera lo scorso 9 febbraio e al quale hanno partecipato i più qualificati esponenti dei settori della comunicazione, degli operatori, dei *social network* e delle istituzioni di questo Paese, dando un contributo fondamentale alla giornata del *Safer Internet Day*.

Un'ulteriore iniziativa è il Libro bianco tv e minori, giunto alla sua seconda edizione, in cui si sono affrontati i temi connessi all'utilizzo di internet e dei social media.

In conclusione, mentre ribadiamo da un lato la nostra disponibilità a collaborare con le Autorità sul piano nazionale e internazionale per mettere in atto misure di prevenzione e repressione, siamo altrettanto convinti che l'investimento di maggiore efficacia sia sul fronte dell'educazione a cui debbono collaborare tanto gli operatori privati quanto il Ministero dell'Istruzione, le scuole pubbliche e private.

A tal proposito, si evidenzia che l'Agcom siede al tavolo dell'Advisory Board del Miur che comprende gli attori chiave, a livello nazionale, in grado di promuovere un utilizzo consapevole delle tecnologie digitali.

Si intende raggiungere questo obiettivo attraverso una sinergia di interventi che veda i Garanti, ognuno nell'ambito delle proprie competenze, far squadra e progettare insieme un piano di educazione/formazione rivolto ai giovani ed agli stessi educatori.

L'educazione è il pilastro fondamentale per permettere a tutti, non solo ai più giovani, di sviluppare senso critico e utilizzare al meglio la Rete evitando i "tranelli" che ci possono essere.

Solo un livello elevato di formazione e di educazione digitale renderà tutti noi maggiormente in grado di beneficiare appieno delle potenzialità delle tecnologie digitali, essendo, al tempo stesso, consumatori e cittadini responsabili.

Ringraziando per l'attenzione, confido con questo mio intervento di aver fornito un utile contributo al vostro lavoro. L'Autorità resta a disposizione per approfondimenti o richieste di chiarimenti.