



DISEGNO DI LEGGE

**d’iniziativa dei senatori PAGANO, GIAMMANCO, BERNINI, MALAN,
DAMIANI, FLORIS, VITALI, AIMI e CANGINI**

COMUNICATO ALLA PRESIDENZA IL 24 OTTOBRE 2018

Modifica al decreto legislativo 9 aprile 2003, n. 70, recante attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell’informazione nel mercato interno, con particolare riferimento al commercio elettronico, in materia di identificazione dei destinatari dei servizi

ONOREVOLI SENATORI. – L'evolversi delle nuove tecnologie e il prepotente ingresso dei *social network* nell'ambito della comunicazione hanno determinato un'espansione significativa della libertà di espressione. Conseguentemente anche i luoghi tipici di commissione dei reati si sono però espansi, andando ad interessare anche l'ambito dei cosiddetti *social network*, nonché, più genericamente, di tutti gli *hosting provider*, vale a dire i fornitori di servizi di memorizzazione permanente.

La materia è senz'altro molto delicata, poiché va a toccare l'ambito della libertà tutelata all'articolo 21 della Costituzione, libertà che costituisce base imprescindibile per ogni solida democrazia.

Il presente disegno di legge si pone proprio l'obiettivo di garantire tale diritto, non andando in alcun modo a intaccare quello che è il diritto di espressione del pensiero, ma semplicemente a far sì che le vittime di reati quali ad esempio la diffamazione e le minacce, commesse a mezzo *internet*, siano agevolmente tutelate.

La difficoltà enorme che incontrano le Forze dell'ordine è infatti quella di risalire al proprietario del «profilo» attraverso il quale è stato commesso il reato, facendo sì che la vittima si trovi senza tutela, una tutela che è garantita dalla nostra Costituzione, ai sensi dell'articolo 24.

Attraverso questa misura, gli *hosting provider* potranno più agevolmente fornire alle Forze dell'ordine i dati anagrafici collegati al profilo per cui si ipotizza il reato.

Osservando più nello specifico i profili costituzionali che vengono in gioco, basandosi su un'interpretazione testuale dell'articolo 21 della Costituzione, si evince che

tutti hanno diritto a manifestare il proprio pensiero. In questo modo, la Costituzione sembra condizionare l'esercizio della libertà di espressione al fatto che esso si dia «a volto scoperto», ossia alla circostanza che ogni manifestazione di pensiero sia riconducibile a un soggetto che ne risponderà in caso di lesione di altri interessi (come nel caso di diffamazione). L'anonimato nell'espressione del pensiero infatti ha ragione di esistere nei regimi illiberali, non certo in uno Stato democratico dove è la norma fondante stessa a garantire la libera espressione del pensiero con ogni mezzo. Al contrario, identificare con le proprie generalità gli utenti, come previsto dal presente disegno di legge, consente di renderli responsabili in caso di violazioni commesse per il mezzo dei rispettivi *account*, che potrebbero corrispondere a *nickname* o pseudonimi e quindi essere difficilmente rintracciabili. L'identificazione potrebbe svolgersi secondo modalità analoghe a quelle che caratterizzano le procedure di verifica degli *account* di personalità note o di rilevanza pubblica, così da non impattare eccessivamente sull'esercizio della libertà di iniziativa economica di attori privati che dovrebbero inevitabilmente dedicare risorse tecniche e umane alla gestione di questi processi. Proprio per questo è stato previsto un termine ampio, gennaio 2020, per adeguarsi alla normativa in questione.

Si è scelto poi di prevedere una sanzione amministrativa, sulla base del fatto che i pilastri che definiscono il regime di responsabilità sono due e si fondano sull'assenza di controllo e di responsabilità editoriale da parte dei fornitori di servizi: essi non «conoscono», né creano o modificano i contenuti immessi dai destinatari dei loro servizi.

Per esempio, se attraverso l'uso di *internet* è commesso un illecito, il fornitore di servizi di connettività vi è generalmente estraneo. Così essi non esercitano una sorveglianza sui contenuti o sulle attività degli utenti in rete. Di conseguenza questi soggetti non sono responsabili per illeciti commessi a mezzo dei loro servizi. La responsabilità di questi operatori sussiste solo quando abbiano notizia, tramite segnalazioni dell'autorità giudiziaria o amministrativa o notifiche degli utenti sufficientemente circostanziate, di contenuti illeciti e non provvedano tempestivamente alla loro rimozione. L'assunto è dunque che gli *internet service provider* siano del tutto neutrali, passivi e svolgano un servizio di natura tecnica che non comporta alcun controllo sui contenuti, né alcuna sorveglianza sugli stessi (che sarebbe, di fatto, impraticabile, dato il numero elevatissimo di contenuti). Inoltre se questi operatori, specialmente i prestatori di servizi di memorizzazione permanente, fossero gravati da un obbligo di sorveglianza, essi sarebbero equiparati a dei censori privati, in grado di imporre una linea di pensiero o politica, mettendo così a rischio la libertà della rete.

Infine l'utilizzo di dati personali per finalità di identificazione dell'utente responsabile di una condotta illecita sui *social network* non apre certamente a forme di giustizia privata che risentirebbero di modalità difficilmente compatibili con la tutela dei dati personali. Occorre che il dato relativo all'identità di un utente sia comunicato alle autorità di pubblica sicurezza che conducono indagini nell'ambito di procedimenti penali per reati commessi sulle piattaforme *social*, non già divulgati pubblicamente. Quest'ultimo risultato sarebbe peraltro in contrasto con le disposizioni vigenti nel regolamento europeo per la protezione dei dati personali (GDPR (*General Data Protection Regulation*) - regolamento (UE) 2016/679), in quanto comporterebbe una loro divulga-

zione. Si segnala peraltro la recente proposta di regolamento «*e-Evidence*» adottata dalla Commissione europea che mira a costruire un sistema di acquisizione di prove elettroniche dai prestatori di servizi (compresi i *social network*) che siano stabiliti o conservino i dati in altri Paesi. Così l'autorità di uno Stato membro che indaghi su un determinato reato potrà chiedere a un operatore stabilito in un altro Stato europeo o in un Paese terzo di produrre dati destinati all'utilizzo come prove nel procedimento incardinato presso l'autorità di emissione della richiesta. È quindi abbastanza evidente come in ambito europeo ci si stia muovendo per far sì che *internet* non sia più una cosiddetta area franca, ma che, sempre nel rispetto delle libertà, vada regolarizzato il suo utilizzo affinché, al fine di favorire un diritto, non se ne vadano a comprimere altri. Il bilanciamento dei diritti è infatti alla base delle democrazie moderne. Un'ultima, importante considerazione va fatta poi in merito alla scelta di non istituire ulteriori appositi reati commessi a mezzo *web*. Occorre infatti sottolineare come le fattispecie dei reati che è possibile commettere a mezzo *web* siano già presenti nell'ordinamento e come non sia assolutamente necessario, ma semmai ridondante in un sistema che necessita di semplificazione, prevedere delle ulteriori specifiche ipotesi. Al contrario gli strumenti mancanti sono quelli relativi al supporto alle indagini delle autorità, strumenti che andranno senz'altro creati e raggruppati, si spera, in un vero e proprio codice che vada a normare e definire la complessa materia, senza andare mai ad intaccare, occorre ribadirlo, il contenuto dell'articolo 21 della Costituzione.

A tal fine, il presente disegno di legge, composto di un solo articolo, introduce l'articolo 16-*bis* nel decreto legislativo 9 aprile 2003, n. 70, recante attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione

nel mercato interno, con particolare riferimento al commercio elettronico, volto a prevedere l'obbligo per i fornitori di servizi di memorizzazione permanente di richiedere al-

l'atto di iscrizione del destinatario del servizio un documento d'identità in corso di validità, stabilendo la relativa sanzione in caso di non osservanza.

DISEGNO DI LEGGE

Art. 1.

1. Al decreto legislativo 9 aprile 2003, n. 70, dopo l'articolo 16 è inserito il seguente:

«Art. 16-bis. - (*Obblighi di identificazione*). - 1. I fornitori di servizi di memorizzazione permanente hanno l'obbligo di richiedere, all'atto di iscrizione del destinatario del servizio, un documento d'identità in corso di validità.

2. L'inosservanza dell'obbligo di cui al comma 1 comporta l'irrogazione di una sanzione amministrativa pecuniaria da 500 a 10.000 euro.

3. Le sanzioni amministrative pecuniarie di cui al comma 2 sono applicate dall'Autorità per le garanzie nelle comunicazioni con provvedimento motivato, previa contestazione degli addebiti agli interessati, da effettuare entro un mese dall'accertamento.

4. Le disposizioni del presente articolo si applicano a decorrere dal 1° gennaio 2020».

€ 1,00