CAMERA DEI DEPUTATI N. **4791**

PROPOSTA DI LEGGE

d'iniziativa del deputato QUINTARELLI

Disposizioni per la tutela dell'identità degli utilizzatori della rete *internet* e delega al Governo per la disciplina della fornitura e dell'impiego di identità digitali protette

Presentata il 18 dicembre 2017

Onorevoli Colleghi ! — Il tema delle notizie false, cosiddette bufale, *on line* e di come esse interferiscano nella vita *on line* dei cittadini sta riempiendo le cronache, tanto che la Commissione europea sta discutendo con intermediari, mezzi di informazione, motori di ricerca e organizzazioni della società civile al fine di progettare soluzioni per affrontare la diffusione di notizie false. L'obiettivo è definire le responsabilità degli attori, nel rispetto della libertà di espressione, del pluralismo dei *media* e del diritto dei cittadini a informazioni diverse e affidabili.

Nel complesso, le notizie false rappresentano un concetto indefinito che comprende diversi tipi di travisamento o distorsione della realtà sotto forma di notizie (in formato testo, audio o video). È tuttavia possibile fare una distinzione ampia tra informazioni false che contengono elementi illegali ai sensi delle leggi europee o nazionali e notizie false che non rientrano nell'ambito di tali leggi.

Una risposta politica globale deve riflettere i ruoli specifici dei diversi attori (piattaforme sociali, mezzi di informazione e utenti) e definire le loro responsabilità alla luce di una serie di princìpi guida, che includono, come già evidenziato, la libertà di espressione, il pluralismo dei *media* e il diritto dei cittadini a informazioni diverse e affidabili.

Più in generale, sempre più spesso emerge nella rete *internet* la delicatezza dell'equilibrio tra la necessità di poter perseguire alcuni reati e la garanzia della libertà di espressione rispetto al rischio di censura.

Molto si sta facendo per gestire il fenomeno intervenendo in modo efficace sia nella fase di pre-moderazione che nelle fasi successive alla pubblicazione, soprattutto con la rimozione di incentivi economici unitamente a meccanismi che introducono

un attrito nella diffusione per limitare la viralità intervenendo anche con algoritmi basati sulla reputazione delle fonti.

Il concetto di reputazione, ovvero di fiducia attribuita a un soggetto, è uno dei pilastri centrali della società in tutti i suoi aspetti relazionali, dall'economia alla politica. Ci si deve quindi interrogare in che misura una funzione così critica possa essere appannaggio di una piccola comunità di appassionati o di professionisti e sulla possibilità che questi possano essere a loro volta catturati o influenzati da interessi esterni.

In economia le agenzie di *rating* svolgono un ruolo per molti versi analogo ai gruppi di *fact checking* delle *fake news* (notizie false): esse hanno un modello di *business* sostenibile ma non sempre scevro da critiche associate perlopiù agli impatti della loro attività e alla loro indipendenza (o dipendenza dai soggetti controllati).

Un altro punto estremamente importante, ma generalmente trascurato nel dibattito pubblico, riguarda il sistema di appello contro le decisioni di rimozione di contenuti operate dalla piattaforma.

Una volta che a un utente venisse rimosso un contenuto che egli ha pubblicato, come assicurare il suo diritto ad appellarsi contro la decisione per tutelare la sua libertà di espressione ?

Le valutazioni circa la rimozione di contenuti sono affidate a moderatori che operano globalmente secondo princìpi definiti dalle piattaforme, non necessariamente allineati con le disposizioni dei Governi locali, in particolare per quanto concerne la tutela dei diritti civili.

Per essere efficace il diritto all'appello deve essere garantito in tempi brevi e non dovrebbe esporre il soggetto a possibili ritorsioni personali da parte di gruppi di pressione.

Deve essere altresì garantita la possibilità, nel caso in cui il fatto costituisca reato, che l'autorità giudiziaria possa risalire all'identità del soggetto.

Un altro aspetto rilevante in materia di identità *on line* riguarda il fenomeno delle criptovalute.

Le criptovalute sono unità di conto immateriali, realizzate con tecniche crittografiche, generalmente scambiate *on line* utilizzando infrastrutture distribuite, aperte, *open source*, per realizzare la necessaria infrastruttura di fiducia. Le informazioni che costituiscono le unità delle criptovalute sono custodite dagli utenti che le posseggono in « portafogli immateriali » chiamati per l'appunto *wallet*.

Le tipologie di criptovalute più diffuse utilizzano pubblicamente una tecnologia denominata *blockchain* che alimenta un registro distribuito delle transazioni e un meccanismo di pseudonimizzazione dei soggetti che effettuano transazioni, le quali sono tutte tracciate e riconducibili allo pseudonimo che le effettua. In questo senso non viene garantito il completo anonimato delle transazioni di pagamento: per ogni transazione sono registrati gli importi e gli pseudonimi di chi paga e di chi è pagato.

Le criptovalute vengono scambiate liberamente tra persone e possono essere convertite in monete fiat, cioè legali, per il tramite di uffici di cambio *on line*. A livello mondiale diversi organismi di regolamentazione hanno introdotto o stanno operando per introdurre norme di vigilanza e di controllo su questi uffici di cambio e sui gestori dei *wallet*.

In questo modo, una volta conosciuto l'attore di uno scambio verso una valuta fiat, è possibile avere visibilità di tutte le transazioni da lui effettuate.

L'attrattività di queste monete è connessa alla possibilità della loro convertibilità in monete fiat per effettuare acquisti nella dimensione materiale.

La previsione di conoscibilità degli utenti di servizi bancari (*Know Your Customer* – KYC) viene generalmente richiesta ai gestori dei *wallet* e presso gli uffici di cambio nel momento della conversione in uscita. Sebbene tale conoscenza appaia idonea a garantire un adeguato livello di contenimento del rischio di sfruttamento di queste monete per alimentare economie illegali, permane il problema della riconoscibilità di tutto lo storico delle transazioni effettuate da una persona, ben oltre le previ-

sioni regolamentari dei tradizionali servizi bancari.

Questo rappresenta un *vulnus* per la *privacy* dell'utente, in particolare se vista in chiave prospettica in un futuro in cui non sappiamo se comportamenti di molti decenni prima potranno esporre gli utenti a pressioni indebite.

I due casi citati sono emblematici della tensione tra libertà fondamentali dell'individuo e necessità di *enforcement* della legge.

In questi casi paradigmatici e in molti altri simili, queste esigenze sono contrastanti e difficilmente conciliabili in quanto gli attuali servizi *on line* e l'infrastruttura giuridica non sono stati disegnati in modo coerente per gestirli.

Nel caso delle *fake news* potrebbe essere realizzata una procedura per cui l'utente che riceve la notifica di una rimozione di un proprio contenuto possa automaticamente opporsi a tale rimozione e forzare la ripubblicazione, assumendosene la responsabilità.

Ciò potrebbe avvenire mediante un sistema di verifica da parte di un fiduciario della sua identità digitale rilasciata in conformità a quanto stabilito dal regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, e la consegna di un *token*, non contenente alcuna informazione personale, che ne attesti esclusivamente l'avvenuta identificazione da parte del fiduciario. Il *token* verrebbe inserito sulla piattaforma che lo archivierebbe e provvederebbe a ripubblicare il contenuto rimosso. In caso di intervento dell'autorità giudiziaria, la piattaforma consegnerebbe il *token* e il fiduciario sarebbe in grado di ricongiungere il *token* all'identità digitale della persona.

In questo modo l'anonimato verrebbe garantito e protetto dal fiduciario, che lo risolverebbe solo nei casi di intervento da parte dell'autorità giudiziaria previsti dalla legge.

Lo stesso meccanismo di protezione dell'anonimato può essere utilizzato per il riconoscimento dei clienti per le normative KYC in materia di criptomonete, per mitigare il rischio relativo alla tracciabilità perenne dello storico delle transazioni.

Simili esigenze di tutela dell'anonimato sono necessarie anche per la tutela dei segnalatori nei casi di *whistleblowing* e possono inoltre avvantaggiare le persone che presentano le richieste relative al *Freedom of Information Acts* (FOIA).

Per proteggere gli utenti anche da eventuali rischi di attacchi informatici può essere utile prevedere ulteriori garanzie, come ad esempio la distruzione del dato di associazione tra *token* e identità digitale trascorso un determinato periodo di tempo e la conservazione di queste informazioni su un archivio *off line* per prevenire furti di dati.

La presente proposta di legge è composta da sei articoli:

l'articolo 1 contiene le definizioni relative all'anonimato protetto;

l'articolo 2 dispone in merito alla verifica dell'identità e all'assegnazione dell'identità digitale;

l'articolo 3 tratta della conservazione delle identità digitali protette;

l'articolo 4 stabilisce che il richiedente può usare l'identità digitale protetta per soddisfare i requisiti di identificazione di fornitori di servizi;

l'articolo 5 prevede una delega al Governo per la disciplina della fornitura e dell'impiego di identità digitali protette al fine di semplificare l'attività delle amministrazioni pubbliche, di ridurre i tempi di produzione e di evitare l'acquisizione e il controllo eccessivo dei dati personali dei cittadini. Gli schemi dei decreti legislativi sono adottati su proposta del Ministro per la semplificazione e la pubblica amministrazione, di concerto con i Ministri competenti, sentita l'Agenzia per l'Italia digitale e acquisito il parere del Garante per la protezione dei dati personali, previa intesa in sede di Conferenza unificata;

l'articolo 6 prevede la clausola di invarianza finanziaria.

PROPOSTA DI LEGGE

—

ART. 1.

(Definizioni).

1. Ai fini di cui alla presente legge si applicano le seguenti definizioni:

a) identità digitale protetta: credenziali informatiche anonime che possono essere ricondotte univocamente a un'identità personale unicamente mediante i servizi di un fornitore di servizi di anonimizzazione autorizzato;

b) fornitore di servizi di anonimizzazione: il fornitore autorizzato di identità digitali protette che effettua la verifica dell'identità della persona richiedente un'identità digitale protetta e mantiene un registro inalterabile dell'associazione tra identità digitale protetta e identità della persona;

c) blockchain: libro mastro decentralizzato e crittograficamente sicuro di transazioni effettuate da utenti *on line*;

d) criptovalute: unità di conto immateriali, realizzate con tecniche crittografiche, generalmente scambiate *on line* utilizzando infrastrutture distribuite, aperte od *open source*, per realizzare la necessaria infrastruttura di fiducia;

e) whistleblowing: l'azione di chi, in un'azienda pubblica o privata, rileva un pericolo, una frode, reale o potenziale, o un qualunque altro rischio in grado di danneggiare l'azienda stessa, gli azionisti, i dipendenti, i clienti o la reputazione dell'ente;

f) FOIA: norme che assicurano il diritto di richiedere e di ottenere la conoscenza delle informazioni formate, detenute o comunque in possesso dei soggetti pubblici;

g) reti sociali: servizi *on line*, tipicamente fruibili mediante *browser* o applicazioni mobili, appoggiandosi sulla relativa piattaforma, per la gestione dei rapporti

sociali e che consentono la comunicazione e la condivisione di informazioni per mezzi testuali e multimediali.

ART. 2.

(Verifica e assegnazione dell'identità digitale protetta).

1. Il fornitore di servizi di anonimizzazione rilascia un'identità digitale protetta al richiedente previo accertamento della sua identità mediante verifica della carta d'identità elettronica, della firma digitale, dell'identità digitale o di un'altra identità digitale protetta del richiedente.

ART. 3.

(Conservazione delle identità digitali protette).

1. Il fornitore di servizi di anonimizzazione mantiene un registro inalterabile protetto delle identità digitali protette rilasciate abbinate a un codice identificativo univoco, non parlante, dell'identità del richiedente; la corrispondenza tra il codice e l'identità del richiedente è mantenuta su archivi inalterabili protetti mantenuti *off line*. La messa *off line* dell'abbinamento tra codice identificativo e identità del richiedente avviene entro ventiquattro ore dall'assegnazione dell'identità digitale protetta.

ART. 4.

(Uso e verifica dell'identità digitale protetta).

1. Il richiedente può usare l'identità digitale protetta per soddisfare i requisiti di identificazione di fornitori di servizi. Il fornitore di servizi può riscontrare presso il fornitore di servizi di anonimizzazione la validità dell'identità digitale protetta. Di tale riscontro il fornitore di servizi mantiene registrazione inalterabile firmata digitalmente per un periodo di cinque anni.

ART. 5.

(Delega al Governo per la disciplina della fornitura e dell'impiego di identità digitali protette).

1. Il Governo è delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi per la disciplina della fornitura e dell'impiego di identità digitali protette, al fine di semplificare l'attività delle amministrazioni pubbliche, di ridurre i tempi di produzione e di evitare l'acquisizione e il controllo eccessivo dei dati personali dei cittadini in caso di attribuzione di funzioni pubbliche in materia di identità digitale a professionisti fornitori di servizi di anonimizzazione, i quali possono operare anche attraverso tecnologie *blockchain* autorizzate. I decreti legislativi sono adottati nel rispetto dei seguenti princìpi e criteri direttivi:

a) individuazione delle attività che possono essere esercitate utilizzando un'identità digitale protetta, inclusi l'autenticazione su reti sociali, l'acquisto di criptovalute, l'attività di *whistleblowing*, le richieste di FOIA e le modalità con cui può essere utilizzata dall'interessato l'identità digitale protetta;

b) individuazione dei requisiti tecnici ed economici minimi del fornitore di servizi di anonimizzazione, compresa un'idonea assicurazione per responsabilità civile, per garantire la continuità del servizio anche nei casi di cessazione e di subentro nel servizio fornito;

c) individuazione delle regole tecniche, informatiche e giuridiche per l'esercizio delle attività di cui alle lettere *a)* e *b)*, nonché dei relativi poteri di vigilanza demandati all'Agenzia per l'Italia digitale e delle sanzioni da comminare ai fornitori di servizi di anonimizzazione;

d) individuazione dei casi e delle circostanze in cui è possibile rivelare l'identità di una persona da parte del fornitore di servizi di anonimizzazione nonché previsione delle sanzioni specifiche e delle ag-

gravanti per i reati commessi utilizzando un'identità digitale protetta.

2. Gli schemi dei decreti legislativi di cui al comma 1 del presente articolo sono adottati su proposta del Ministro per la semplificazione e la pubblica amministrazione, di concerto con i Ministri competenti, sentita l'Agenzia per l'Italia digitale e acquisito il parere del Garante per la protezione dei dati personali, previa intesa in sede di Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, ai sensi dell'articolo 9, comma 2, lettera *b)*, del medesimo decreto legislativo n. 281 del 1997.

3. Entro dodici mesi dalla data di entrata in vigore di ciascuno dei decreti legislativi di cui al presente articolo, nel rispetto dei princìpi e criteri direttivi di cui al comma 1, il Governo può adottare, con le procedure di cui al comma 2, disposizioni integrative e attuative dei medesimi decreti legislativi, tenuto conto delle evidenze attuative nel frattempo emerse.

ART. 6.

(Clausola di invarianza finanziaria).

1. Dall'attuazione della presente legge non devono derivare nuovi o maggiori oneri per il bilancio dello Stato.

17PDL0060910