dossier

XVIII legislatura

Dossier del Servizio Studi sull'A.S. n. 1900

Istituzione di una Commissione parlamentare di inchiesta sulla diffusione massiva di informazioni false

settembre 2020
n. 292

servizio studi del Senato

ufficio ricerche sulle questioni istituzionali, giustizia e cultura

SERVIZIO STUDI
TEL. 066706-2451
studi1@senato.it

Il presente dossier è stato redatto sulla base dei dossier nn. 182 e 182/1 predisposti dai Dipartimenti Cultura e Trasporti del Servizio Studi Camera.

Classificazione Teseo: Commissioni e giunte parlamentari. Inchieste parlamentari. Internet. Informazione.

I dossier del Servizio studi sono destinati alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. I testi e i contenuti normativi ufficiali sono solo quelli risultanti dagli atti parlamentari. Il Senato della Repubblica declina ogni responsabilità per la loro eventuale utilizzazione o riproduzione per fini non consentiti dalla legge. I contenuti originali possono essere riprodotti, nel rispetto della legge, a condizione che sia citata la fonte.

I N D I C E

Introduzione

Giunge all'esame del Senato il disegno di legge A.S. n. 1900, recante *Istituzione di una Commissione parlamentare di inchiesta sulla diffusione massiva di informazioni false*.

Esso è stato approvato in prima lettura dalla Camera dei deputati, il 29 luglio 2020.

Prevede l'istituzione di una Commissione parlamentare di inchiesta, ai sensi dell'articolo 82 della Costituzione (**articolo 1**).

Alla Commissione è attribuito un novero di compiti, enumerati dall'**articolo 2**. Sono volti ad acquisire elementi conoscitivi sulle attività di disinformazione nonché a valutare l'adeguatezza degli strumenti esistenti per fronteggiare il fenomeno, con eventuale proposta di iniziative affinché risultino più incisive la prevenzione e l'opera di contrasto.

Gli **articoli da 3 a 8** disciplinano la composizione, la durata, i poteri e le modalità di funzionamento della Commissione.

L'**articolo 9** ha per oggetto l'entrata in vigore.

Diffusione massiva di informazioni false ed attività di disinformazione

(articolo 2, comma 1, lettere *a), b), c), d), e), f) e g)*)

Alla Commissione di inchiesta - è previsto nel disegno di legge - è affidato, anzitutto, il compito di indagare sulle attività di **diffusione massiva di informazioni e contenuti illegali, falsi, non verificati, oppure dolosamente ingannevoli** sia attraverso i *media* tradizionali (fermi restando gli strumenti di controllo disciplinati dalla normativa vigente) sia attraverso le reti sociali telematiche e le altre piattaforme tecnologiche analogiche o digitali.

Siffatte "attività di disinformazione" includono altresì la creazione di false identità digitali o la produzione e la comunicazione di tali informazioni e contenuti in forma personalizzata da parte di soggetti che a questo fine utilizzino i dati degli utenti (**lettera *a)***).

Secondo la definizione adottata dalla Commissione europea nella Comunicazione congiunta "Relazione sull'attuazione del piano di azione contro la disinformazione (JOIN/2019/12 final)", l'attività di disinformazione è "un'informazione rivelatasi falsa o fuorviante concepita, presentata e diffusa a scopo di lucro o per ingannare intenzionalmente il pubblico, e che può arrecare un

pregiudizio pubblico. La disinformazione non include gli errori di segnalazione, la satira e la parodia, o notizie e commenti chiaramente identificabili come di parte".

Secondo la Commissione europea, "obiettivo della disinformazione è distrarre e dividere, insinuare il seme del dubbio distorcendo e falsando i fatti, al fine di disorientare i cittadini minando la loro fiducia nelle istituzioni e nei processi politici consolidati".

Si è sostenuto in dottrina che l'attività di disinformazione si colleghi al concetto proprio del tempo post-moderno di "post-verità" ossia di una verità costruita non su basi oggettive ma in conseguenza di "una relazione di complicità, di emozione e di reciprocità, tra chi, di volta in volta, parla o ascolta. Anche invertendo i ruoli". "Non si tratta dunque di una mera bugia ma piuttosto della verità desiderata da chi la professa e da chi la accoglie" (A. Nicita).

Uno degli strumenti più tipici della diffusione della disinformazione è rappresentato dall'utilizzo di identità digitali false, che ha formato già da tempo oggetto di attenzione da parte del Garante per la protezione dei dati personali.

In particolare, il Garante per la protezione dei dati personali si pronunciò per la prima volta nei confronti di Facebook nel 2016 [doc. web n. 4833448], imponendo di bloccare i falsi profili (i cosiddetti *fake*) e di assicurare più trasparenza e controllo agli utenti, affermando innanzitutto la propria competenza a intervenire a tutela degli utenti italiani. La multinazionale, infatti, è presente sul territorio italiano con un'organizzazione stabile, Facebook Italy srl, la cui attività è da considerare inestricabilmente connessa con quella svolta da Facebook Ireland ltd che ha effettuato il trattamento di dati contestato, per cui al caso di specie risulta applicabile il diritto nazionale (in base alla sentenza della Corte di Giustizia Europea Weltimmo del 1° ottobre 2015 C, nonché il WP 179). Il Garante ha accolto le tesi del ricorrente ritenendolo legittimato, in base alla normativa italiana, ad accedere a tutti i dati che lo riguardano compresi quelli presenti e condivisi nel falso *account*. Ha quindi ordinato a Facebook di comunicare all'interessato tutte le informazioni richieste entro un termine preciso, in modo chiaro e comprensibile, comprese le informazioni sulle finalità, le modalità e la logica del trattamento dei dati, i soggetti cui sono stati comunicati o che possano venirne a conoscenza.

Una forma più sottile di disinformazione è rappresentata dalla segnalazione automatica agli utenti di contenuti in forma personalizzata, avvalendosi dei dati personali degli stessi utenti, sia con finalità commerciali sia con finalità informative. In tal caso, le informazioni possono non essere totalmente false ma potrebbero essere tendenziose essendo, in qualche modo, tarate, ad esempio, sulla precedente attività della persona (espressa ad esempio attraverso "like" a pagine con particolari tipologie di contenuti) o semplicemente sulla navigazione di ciascun utente.

Spesso i due fenomeni (la creazione di profili falsi e la produzione di contenuti falsi o tendenziosi) sono connessi.

Con riferimento alla pubblicazione di informazioni sui media tradizionali, si ricorda che l'articolo 2 della legge n. 69 del 1963, recante ordinamento della

professione di giornalista, stabilisce che è diritto insopprimibile dei giornalisti la libertà di informazione e di critica, limitata, però, oltre che dall'osservanza delle norme di legge dettate a tutela della personalità altrui, dall'obbligo inderogabile del rispetto della verità sostanziale dei fatti, osservati sempre i doveri imposti dalla lealtà e dalla buona fede. Le notizie che risultino inesatte devono essere rettificate e gli eventuali errori devono essere riparati.

Altre disposizioni riguardano l'etica della professione e attengono al rapporto tra il giornalista e la categoria di appartenenza (ad esempio, il dovere di promuovere la fiducia tra la stampa e i lettori, il mantenimento del decoro e della dignità professionali, il rispetto della propria reputazione). La loro violazione comporta una responsabilità di tipo disciplinare, che viene accertata da appositi organi (Consigli regionali e Consiglio nazionale dell'Ordine dei giornalisti) e prevede la comminazione di sanzioni disciplinari (di cui agli articoli 51-55 della medesima legge n. 69 del 1963).

Esse sono l'avvertimento, la censura, la sospensione dall'esercizio della professione da un minimo di due mesi a un massimo di un anno, e la radiazione dall'albo.

A sua volta, l'articolo 2 del Testo unico dei doveri del giornalista (approvato dal Consiglio nazionale dell'Ordine il 27 gennaio 2016, e nato dall'esigenza di armonizzare i precedenti documenti deontologici al fine di facilitare l'applicazione delle norme la cui inosservanza possa determinare la responsabilità disciplinare dell'iscritto all'Ordine) pone, tra i fondamenti deontologici, il principio secondo cui il giornalista è tenuto a difendere il diritto all'informazione e la libertà di opinione di ogni persona, e per questo ricerca, raccoglie, elabora e diffonde con la maggiore accuratezza possibile ogni dato o notizia di pubblico interesse secondo la verità sostanziale dei fatti.

Con specifico riguardo ai doveri in tema di rispetto delle fonti e di rettifica, l'art. 9 stabilisce, tra l'altro, che il giornalista: controlla le informazioni ottenute per accertarne l'attendibilità; rettifica, anche in assenza di specifica richiesta, con tempestività e appropriato rilievo, le informazioni che dopo la loro diffusione si siano rivelate inesatte o errate; rispetta il segreto professionale e dà notizia di tale circostanza nel caso in cui le fonti chiedano di rimanere riservate; in tutti gli altri casi le cita sempre (tale obbligo persiste anche quando si usino materiali – testi, immagini, sonoro – delle agenzie, di altri mezzi d'informazione o dei *social network*); non accetta condizionamenti per la pubblicazione o la soppressione di una informazione; non omette fatti, dichiarazioni o dettagli essenziali alla completa ricostruzione di un avvenimento.

Un ulteriore compito affidato alla Commissione è quello di verificare se l'attività di disinformazione sia riconducibile a **soggetti gruppi organizzazioni, anche aventi struttura internazionale**, che si avvalgano anche del sostegno finanziario di soggetti interni o esteri con lo scopo premeditato di manipolare l'informazione e di condizionare l'opinione

pubblica "per specifici interessi", in modo particolare in occasione di **consultazioni elettorali o referendarie** (**lettera *b***).

I rischi derivanti dall'attività di disinformazione proveniente da forze esterne – in particolare, enti e organismi situati in Stati terzi - sono stati oggetto delle prime iniziative assunte in materia di disinformazione a livello europeo.

Le misure in tale settore sono spesso ricondotte dall'Unione europea nel più ampio ambito dell'azione di difesa dalle "minacce ibride". Secondo la Commissione europea (Comunicazione congiunta al Parlamento e al Consiglio JOIN(2016) 18 final, del 6 aprile 2016), le campagne massicce di disinformazione, che usano i *media* sociali per controllare il discorso politico o per radicalizzare, reclutare e dirigere mandatari, possono essere vettori di "minacce ibride".

In particolare, nella stessa Comunicazione, per minacce ibride – nozione per la quale non esiste una definizione sul piano giuridico universalmente accettata – la Commissione europea intende una serie di attività che spesso combinano metodi convenzionali e non convenzionali e che possono essere realizzate in modo coordinato da soggetti statali e non statali (pur senza oltrepassare la soglia di guerra formalmente dichiarata). Il loro obiettivo non consiste soltanto nel provocare danni diretti e nello sfruttare le vulnerabilità, ma anche nel destabilizzare le società e creare ambiguità per ostacolare il processo decisionale.

Può valere ricordare come, a partire dalle elezioni politiche del 4 marzo 2018, l'Autorità garante per le comunicazioni (AGCOM) abbia definito indirizzi per promuovere la correttezza delle informazioni e la garanzia del pluralismo nelle piattaforme digitali, alla luce del loro crescente utilizzo rispetto ai tradizionali strumenti di campagna elettorale.

Con le Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche 2018 (1° febbraio 2018) ha, in particolare, affermato la necessità di garantire per tutti i soggetti politici, con imparzialità ed equità e alle medesime condizioni, l'accesso agli strumenti di informazione e comunicazione politica forniti dalle piattaforme digitali.

Le Linee guida sono state adottate nell'ambito di un Tavolo tecnico di autoregolamentazione promosso dall'AGCOM per garantire pluralismo e correttezza dell'informazione sulle piattaforme digitali. Il Tavolo ha visto la partecipazione della quasi totalità degli *stakeholders* aderenti all'iniziativa, tra cui Google, Facebook, rappresentanti dei principali gruppi editoriali della stampa e radiotelevisione, le rispettive associazioni di categoria, nonché rappresentanti del mondo del giornalismo e della componente pubblicitaria. Le piattaforme aderenti hanno messo a disposizione dei propri utenti alcuni strumenti di contrasto alla disinformazione *online*, tra cui la campagna informativa lanciata da Facebook sulle pagine dei propri utenti italiani per l'individuazione delle notizie false e le iniziative di Google nella promozione e valorizzazione del *fact-checking* e per l'uso della propria piattaforma da parte dei soggetti politici impegnati nella campagna elettorale.

Nelle Linee guida si auspicava l'applicazione dei principi di parità di trattamento della legge sulla *par condicio* anche alle piattaforme *social*. Ad esempio, con riferimento ai messaggi pubblicitari i cui inserzionisti siano soggetti politici, è stata evidenziata la necessità, per le fattispecie in cui sia possibile, che l'inserzionista indichi la natura di "messaggio elettorale", specificando, altresì, il soggetto politico committente, alla stregua di quanto già avviene per i messaggi politico-elettorali sulla stampa quotidiana e periodica ai sensi dell'articolo 7 della legge n. 28 del 2000.

L'Autorità ha raccomandato, inoltre, di assicurare interventi rapidi in caso di diffusione di messaggi con contenuti illeciti o lesivi di altri candidati e un rafforzamento delle iniziative di *fact-checking*.

Ad un anno di distanza dall'approvazione delle Linee guida, e all'approssimarsi delle elezioni europee, l'Autorità garante ha posto in evidenza "un rilevante vuoto normativo in tema di par condicio sul fronte dei *social network*" e ha segnalato al Governo la necessità di "mettere in sicurezza" l'analisi delle campagne elettorali (AGCOM, Comunicato stampa, 30 gennaio 2019).

Anche il Garante della *privacy* ha adottato il 18 aprile 2019 un provvedimento in materia di propaganda elettorale e comunicazione politica, pubblicato nella *Gazzetta Ufficiale* del 7 maggio 2019, che ha integrato un precedente provvedimento del 6 marzo 2014.

Riguardo all'uso dei dati pubblicati dagli interessati sui *social network*, il Garante ha "messo in guardia" sui "seri rischi" di utilizzo improprio dei dati personali dei cittadini per sofisticate attività di profilazione su larga scala e di invio massivo di comunicazioni o ancora per indirizzare campagne personalizzate (il c.d. *micro-targeting*) volte a influenzare l'orientamento politico e la scelta di voto degli interessati, sulla base degli interessi personali, dei valori, delle abitudini e dello stile di vita dei singoli.

Al contempo, la Commissione per l'indirizzo e la vigilanza dei servizi radiotelevisivi ha adottato il 2 aprile 2019 il consueto provvedimento volto a disciplinare la propaganda elettorale nelle emittenti del servizio pubblico in vista delle elezioni europee 2019. In modo analogo e con riferimento alle televisioni e alle radio private, l'Autorità per le garanzie nelle comunicazioni ha proceduto approvando la delibera del 28 marzo 2019.

In quest'ultimo provvedimento, l'AGCOM ha inserito disposizioni finalizzate a garantire forme di tutela del pluralismo espressamente rivolte alle piattaforme di condivisione di video e ai *social network* (Titolo VI).

L'AGCOM ha rinviato poi al Tavolo tecnico per la garanzia del pluralismo e della correttezza dell'informazione sulle piattaforme digitali l'assunzione "di ogni utile iniziativa al fine di promuovere l'adozione condivisa di misure di contrasto ai fenomeni di disinformazione e lesione del pluralismo informativo *online*".

Inoltre, l'Autorità si è impegnata "a promuovere, mediante procedure di autoregolamentazione, l'adozione da parte dei fornitori di piattaforme di condivisione di video di misure volte a contrastare la diffusione in rete, e in particolare sui social media, di contenuti in violazione dei principi sanciti a tutela

del pluralismo dell'informazione e della correttezza e trasparenza delle notizie e dei messaggi veicolati".

Da parte loro, le piattaforme si sono impegnate ad assicurare il rispetto dei divieti sanciti dalla disciplina legislativa e regolamentare in materia di comunicazione e diffusione dei sondaggi.

Parallelamente, a livello UE, in vista delle elezioni dei componenti del Parlamento europeo del maggio 2019, la Commissione europea ha invitato le autorità nazionali competenti a individuare le migliori pratiche in materia di identificazione, mitigazione e gestione dei rischi che gli attacchi informatici e la disinformazione comportano per il processo elettorale (Raccomandazione della Commissione, del 14 febbraio 2018, sul rafforzare la natura europea e l'efficienza nello svolgimento delle elezioni del Parlamento europeo del 2019).

Nella comunicazione al Parlamento europeo Contrastare la disinformazione online: un approccio europeo (aprile 2018) la Commissione europea ha quindi invitato le piattaforme di *network* a intensificare gli sforzi per contrastare la disinformazione e ha lanciato l'elaborazione di un Codice di buone pratiche.

Nell'ottobre del 2018 alcune tra le principali società online (*Google*, *Facebook*, *Twitter* e *Mozilla*) e associazioni che rappresentano il settore pubblicitario hanno firmato il codice di buone pratiche, impegnandosi ad attuare una serie di misure in previsione delle elezioni europee per affrontare efficacemente il problema dell'utilizzo delle nuove tecnologie e dei *social media* finalizzato a diffondere, mirare e amplificare la disinformazione. In seguito anche Microsoft e Tik Tok hanno sottoscritto il codice di buone pratiche (rispettivamente, a maggio 2019 e a giugno 2020). Le piattaforme *social* hanno quindi adottato codici di autoregolamentazione finalizzati a impedire i tentativi di inquinamento del voto per le europee 2019 attraverso la diffusione di notizie false (si vedano in particolare: Facebook February update on implementation of the Code of Practice on Disinformation; EC Action Plan on Disinformation Google January Report; Twitter January update: *Code of practice on disinformation*).

Le piattaforme online e le associazioni che avevano firmato il codice di buone pratiche nel 2018 hanno anche presentato, a gennaio 2019, un rapporto riguardante le misure adottate per rispettare gli impegni presi. Dal canto suo, l'Unione Europea tra gennaio e maggio 2019 ha eseguito un monitoraggio nei confronti di Facebook, Google e Twitter. con particolare riguardo alla correttezza in occasione della campagna elettorale per il rinnovo del Parlamento Europeo del 2019. I risultati dei suddetti controlli sono stati pubblicati a settembre dello stesso anno. La Commissione Europea, inoltre, sta portando avanti l'attività di valutazione dell'efficacia del *Code of Practice on Disinformation* oltre il periodo iniziale di dodici mesi dalla sua entrata in vigore.

Altro compito affidato alla Commissione d'inchiesta consiste nella verifica se siano compiute, e con quali effetti, attività di disinformazione **in materia sanitaria** (**lettera *c)***).

O se siano state compiute durante l'**emergenza da Covid-19**, in tal caso investigando altresì sulle ripercussioni avute riguardo alla gestione dell'emergenza e sulle misure adottate per prevenirle o reprimerle (**lettera *d)***).

L'Osservatorio sulla disinformazione *online* istituito presso l'Autorità per le garanzie nelle telecomunicazioni pubblica periodicamente uno "speciale Coronavirus", in cui sono riportati prospetti relativi alla informazione e disinformazione sui *media* e sui *social* riguardo alla natura e diffusione del morbo.

Questa sorta di bollettino è andato strutturandosi per sezioni relative a: "cosa offrono informazione e disinformazione sul coronavirus" (riportando altresì un dato del tasso di disinformazione media giornaliera sul totale delle notizie *on-line* relativa al coronavirus, nel periodo considerato); "cosa guardano in rete gli italiani sul coronavirus"; come cambia il consumo di internet in Europa durante l'epidemia"; "minacce alla sicurezza informatica e coronavirus".

A metà aprile 2020 l'Autorità per le garanzie nelle comunicazioni (con le delibere 152 e 153/20/Cons.) ha ordinato la sospensione per un periodo di sei mesi dell'attività di diffusione dei contenuti da parte dei servizi di media audiovisivi sul canale 880 SAT e sul canale 61 DTT esercitati rispettivamente dalla società dalla società Italian Broadcasting S.r.l e Mediacom S.r.l. a seguito della programmazione del *format* "Il cerca salute" e dello speciale "Quello che non vi hanno detto sul Coronavirus".

Tale provvedimento, peraltro, è stato oggetto di ricorso presentato davanti al Tar del Lazio. Il tribunale amministrativo ha sospeso l'efficacia della delibera AGCOM n. 153 fino alla discussione del ricorso, che è avvenuta in data 8 maggio. All'esito dell'esame del ricorso, il TAR del Lazio ha sentenziato che gli effetti del provvedimento sanzionatorio preso dall'AGCOM apparivano, allo stato, sproporzionati rispetto al fine perseguito e che pertanto nella comparazione degli interessi in gioco l'attività di diffusione, oggetto di sospensione, potesse essere ripresa. Secondo fonti di stampa, l'AGCOM a sua volta intenderebbe ricorrere al Consiglio di Stato.

Ulteriore compito assegnato alla Commissione è quello di verificare se l'attività di disinformazione abbia **finalità di odio**, ossia di istigazione alla discriminazione o alla violenza (**lettera *e)***).

Ancora, la Commissione è chiamata a verificare se le attività di disinformazione siano correlate ad **attività di natura commerciale**, in particolare di portali, siti *internet* e piattaforme digitali.

Rimane ferma beninteso ferma restando la disciplina applicabile per i casi di pubblicità ingannevole e pratiche commerciali scorrette. La correlativa tutela è disposta, rispettivamente, dal decreto legislativo n. 145 del 2007 (il quale ha dato attuazione all'articolo 14 della direttiva 2005/29/CE a sua volta modificativa della direttiva 84/450/CEE sulla pubblicità ingannevole) e dal Codice del consumo (decreto legislativo n. 206 del 2005).

Così la **lettera *f)***.

Altro compito assegnato alla Commissione d'inchiesta è quello di verificare gli effetti derivanti dallo sviluppo dell'**intelligenza artificiale** e delle nuove tecnologie sull'attività di disinformazione, anche con riguardo alla tutela dei dati sensibili e personali e al loro utilizzo **(lettera *g)***).

La possibilità di veicolare informazioni personalizzate secondo modalità tali da produrre effetti significativi e duraturi nella pubblica opinione si avvale, sia nel caso di comunicazioni commerciali sia nel caso di vere e proprie attività di disinformazione, di strumenti tecnologici.

Sono infatti le macchine (i cosiddetti BOT, abbreviazione di Robot) i principali strumenti di creazione e diffusione di disinformazione.

Questi programmi automatizzati, in grado di interagire con gli esseri umani, possono produrre e diffondere notizie false o tendenziose senza i limiti propri degli esseri umani (ad esempio, possono essere create centinaia di migliaia di notizie in tempi molto brevi), senza poter essere immediatamente riconoscibili come programmi informatici dagli esseri umani.

Diversi sono stati i casi di studio di tali fenomeni, a fondamento dei quali può esservi anche l'utilizzo abusivo e malevolo di dati personali. Tra gli esempi più noti di utilizzazione abusiva di dati personali e di profilazione individuale vi sono quelli verificatisi in occasione della campagna referendaria sulla Brexit e in altre recenti occasioni di confronto politico-elettorale (casi Facebook, Cambridge Analytica, AggregateIQ).

In materia di intelligenza artificiale (AI), la Commissione europea ha adottato il 25 aprile 2018 una apposita Comunicazione (COM(2018)237 final), che ne analizza le caratteristiche e gli aspetti. La Commissione sta aumentando gli investimenti annuali nell'IA del 70 per cento nell'ambito del programma di ricerca e innovazione Orizzonte 2020, con 1,5 miliardi di euro previsti per il periodo 2018-2020. Il 10 aprile 2018, venticinque Paesi europei, tra cui l'Italia, hanno firmato una dichiarazione di cooperazione sull'intelligenza artificiale. Il 7 dicembre 2018 la Commissione UE ha quindi presentato il "Piano coordinato sull'intelligenza artificiale" (COM(2018)795), accolto dal Consiglio dell'UE che si è pronunciato il 18 febbraio 2019.

I sistemi di intelligenza artificiale (AI) sono basati su *software* che mostrano comportamenti 'intelligenti', avendo la capacità di analizzare caratteristiche di contesto esterno e di fornire risposte in qualche misura autonome, basate sull'analisi complessa dei dati a disposizione (ad esempio, assistenti vocali, software di analisi delle immagini, motori di ricerca, sistemi di riconoscimento facciali e vocali). L'apprendimento automatico denota la capacità di un *software/computer* di apprendere dal proprio ambiente o da una serie molto ampia di dati rappresentativi, consentendo ai sistemi di adattare il loro comportamento a circostanze mutevoli o di eseguire compiti per i quali non sono stati programmati esplicitamente. L'AI può essere utilizzata anche nell'ambito di hardware come i robot avanzati, le automobili a guida autonoma, i droni e altre applicazioni

dell'*Internet of Things*. Gli elementi essenziali che connotano l'intelligenza artificiale sono essenzialmente tre: i dati, gli algoritmi e la potenza di calcolo.

Con la comunicazione COM/2020/65 del 19 febbraio 2020 è stato emanato il libro bianco europeo sull'intelligenza artificiale che individua le prime linee di intervento dell'azione europea.

È stata infine pubblicata, nel mese di luglio 2020, la versione finale delle Proposte per una strategia italiana per l'intelligenza artificiale, elaborata dal Gruppo di esperti sull'intelligenza artificiale, istituito presso il Ministero dello sviluppo economico. Il Gruppo di esperti aveva elaborato, tra gennaio e giugno 2019, un primo documento contenente le proposte per una strategia italiana per l'intelligenza artificiale. Il Ministero le ha quindi sintetizzate il 31 luglio 2019 nella Strategia nazionale per l'intelligenza artificiale. I due documenti sono stati posti in consultazione pubblica dal 19 agosto 2019 al 13 settembre 2019, al fine di raccogliere osservazioni e suggerimenti per un raffinamento della strategia.

L'esame dell'adeguatezza degli strumenti esistenti per contrastare il fenomeno della disinformazione

(articolo 2, comma 1, lettere *h), i), l), m), n), o), p), q) ed r)*)

Un insieme di compiti della Commissione d'inchiesta concerne una riflessione circa la strumentazione giuridica esistente in materia di contrasto delle attività di disinformazione, a fini di sua eventuale rivisitazione.

Figura tra questi la verifica dello stato di attuazione della normativa vigente e delle attività e delle procedure e delle risorse (da valutare se congrue o meno). Così la **lettera *h)***, che ha riguardo al settore pubblico.

Con riferimento al settore privato, la Commissione ha il compito di verificare l'esistenza e l'idoneità delle **procedure interne predisposte dai *media* e dai fornitori di servizi** delle reti sociali telematiche e delle altre piattaforme analogiche e digitali (fermi restando gli strumenti di controllo disciplinati dalla normativa vigente) per la rimozione delle informazioni false e dei contenuti illeciti dalle proprie piattaforme.

La verifica si estende alle procedure per la gestione delle segnalazioni e dei reclami presentati dagli utenti e per la prevenzione e il contrasto dei reati commessi attraverso l'utilizzo delle medesime piattaforme, garantendo che tali procedure non siano lesive della libertà di espressione e di stampa (**lettera *i)***).

Inoltre, la Commissione è chiamata a verificare - anche sulla base della comparazione con le esperienze di altri Stati europei - la possibilità dell'adozione di un **codice di autoregolamentazione** da parte dei medesimi soggetti (*media* e fornitori di servizi delle reti e piattaforme), nel quale siano previste le procedure per rimuovere tempestivamente i contenuti derivanti dall'attività di disinformazione dalle proprie piattaforme, prevedendo altresì di vietare il conseguimento di eventuali vantaggi pubblicitari connessi

Rimangono ferme le prerogative e le competenze dell'Ordine dei giornalisti.

Così la **lettera *l)***.

Per le competenze e le prerogative dell'Ordine dei giornalisti, la disposizione richiama la specifica legge n. 69 del 1963, la quale reca l'ordinamento della professione di giornalista, nonché il d.P.R. n. 137 del 2012, ossia il regolamento di delegificazione in materia di professioni regolamentate, volto a dare attuazione ai principi dettati dall'art. 3, co. 5, del decreto-legge n. 138 del 2011, il quale ha inteso abrogare le indebite restrizioni all'accesso e all'esercizio delle professioni e delle attività economiche. In particolare, esso detta la disciplina generale per tutte le professioni ordinistiche, fatte salve alcune specificità.

Tra le misure chiave indicate dalla Commissione europea nella comunicazione COM(2018) 236 "Contrastare la disinformazione online: un approccio europeo", l'elaborazione da parte dei rappresentanti delle piattaforme online, dell'industria della pubblicità e dei principali inserzionisti, di un codice di buone pratiche dell'UE sulla disinformazione in regime di autoregolamentazione. Lo si è ricordato *supra*, a proposito della lettera *b)* dell'articolo 2 del disegno di legge.

Inoltre, alla Commissione è affidato il compito di verificare l'esistenza di azioni, interventi, politiche e buone pratiche di tipo **educativo, culturale, sociale e formativo**, volti a innalzare il livello di consapevolezza e resilienza delle comunità rispetto all'attività di disinformazione, nonché di iniziative volte alla sensibilizzazione sull'importanza della **verifica delle informazioni**, anche attraverso la ricerca e il controllo delle fonti, con particolare riguardo all'accertamento dei fatti.

Vi rientra la verifica, in particolare, del livello di attuazione dell'**insegnamento scolastico dell'educazione alla cittadinanza digitale**, nell'ambito di quello dell'educazione civica, e della sua reale efficacia formativa nei riguardi degli studenti, anche al fine di monitorare il rapporto tra il sistema educativo e l'innovazione tecnologica (**lettera *m)***).

In sede europea, la Raccomandazione del Consiglio del 22 maggio 2018 (2018/C 189/01) – che ha sostituito la Raccomandazione n. 962 del 2006 – ha sottolineato che la competenza digitale comprende, fra l'altro, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso il possesso

di competenze relative alla cibersicurezza), il pensiero critico. Ha evidenziato, infatti, che le persone dovrebbero assumere un approccio critico nei confronti della validità, dell'affidabilità e dell'impatto delle informazioni e dei dati resi disponibili con strumenti digitali, e che dovrebbero essere in grado di gestire e proteggere informazioni, contenuti, dati e identità digitali, oltre a riconoscere software, dispositivi, intelligenza artificiale o robot e interagire efficacemente con essi.

Nell'ambito delle Indicazioni nazionali per il curricolo della scuola dell'infanzia e del primo ciclo di istruzione (emanate con D.M. 16 novembre 2012, n. 254), il profilo delle competenze al termine del primo ciclo di istruzione prevede che lo studente "ha buone competenze digitali, usa con consapevolezza le tecnologie della comunicazione per ricercare ed analizzare dati e informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo".

Con specifico riferimento alle tecnologie dell'informazione e della comunicazione e alle tecnologie digitali, le Indicazioni nazionali evidenziano che "è necessario che oltre alla padronanza degli strumenti, spesso acquisita al di fuori dell'ambiente scolastico, si sviluppi un atteggiamento critico e una maggior consapevolezza rispetto agli effetti sociali e culturali della loro diffusione".

Nel successivo documento "Indicazioni nazionali e nuovi scenari" (documento – frutto del lavoro del Comitato scientifico per le Indicazioni nazionali della scuola dell'Infanzia e del primo ciclo di istruzione, che è stato presentato al MIUR il 22 febbraio 2018) – che propone alle scuole una rilettura delle Indicazioni nazionali emanate nel 2012 attraverso la lente delle competenze di cittadinanza – si sottolinea che "La responsabilità è l'atteggiamento che connota la competenza digitale. Solo in minima parte essa è alimentata dalle conoscenze e dalle abilità tecniche, che pure bisogna insegnare". "Tuttavia, come suggeriscono anche i documenti europei sulla educazione digitale, le abilità tecniche non bastano. La maggior parte della competenza è costituita dal sapere cercare, scegliere, valutare le informazioni in rete e nella responsabilità nell'uso dei mezzi, per non nuocere a se stessi e agli altri".

A livello legislativo, la legge n. 107 del 2015 recante riforma del sistema nazionale di istruzione e formazione ha inserito, fra gli obiettivi dell'espansione dell'offerta formativa nelle scuole di ogni ordine e grado, lo sviluppo delle competenze digitali degli studenti, con particolare riguardo, fra l'altro, all'utilizzo critico e consapevole dei *social network* e dei *media*, nonché il sostegno dell'assunzione di responsabilità e della consapevolezza dei diritti e dei doveri. Ha, altresì, previsto, al fine di sviluppare e di migliorare le competenze digitali degli studenti e di rendere la tecnologia digitale uno strumento didattico di costruzione delle competenze in generale, l'adozione del Piano nazionale per la scuola digitale (art. 1, co. 7, lettere *d)* ed *h)*, e 56).

Il Piano nazionale scuola digitale (PNSD) è stato adottato con d.m. 27 ottobre 2015, n. 851, e ha previsto vari ambiti di intervento, fra cui quello relativo alle competenze degli studenti, proponendo le relative Azioni.

Le misure relative alla scuola adottate nel 2020 a causa dell'epidemia di Covid-19 e della conseguente necessità di svolgere l'attività didattica a distanza sono state molteplici e, con specifico riguardo al settore digitale, si segnala il decreto del Ministro dell'istruzione 9 giugno 2020, n. 27, volto a favorire l'inclusione digitale presso le scuole più esposte al rischio di povertà educativa. Tali provvedimenti non attengono alla questione della disinformazione veicolabile *online*.

Si ricorda, inoltre, che l'articolo 5 della legge n. 92 del 2019, recante "Introduzione dell'insegnamento scolastico dell'educazione civica", ha previsto l'inserimento dell'educazione alla cittadinanza digitale nell'ambito dell'insegnamento trasversale dell'educazione civica, che si avvierà dall'anno scolastico 2020/2021.

Tra le conoscenze digitali essenziali che la relativa offerta formativa deve prevedere, vi sono le seguenti:

- ✓ analizzare, confrontare e valutare criticamente la credibilità e l'affidabilità delle fonti di dati, informazioni e contenuti digitali;
- ✓ conoscere le norme comportamentali da osservare nell'ambito dell'utilizzo delle tecnologie digitali e dell'interazione in ambienti digitali;
- ✓ conoscere le politiche sulla tutela della riservatezza applicate dai servizi digitali relativamente all'uso dei dati personali;
- ✓ creare e gestire l'identità digitale, essere in grado di proteggere la propria reputazione, gestire e tutelare i dati che si producono attraverso diversi strumenti digitali, rispettare i dati e le identità altrui.

Per verificare l'attuazione di tali previsioni e valutare eventuali esigenze di aggiornamento, il Ministro dell'istruzione convoca almeno ogni due anni la Consulta dei diritti e dei doveri del bambino e dell'adolescente digitale, di cui è stata prevista l'istituzione presso il Ministero dell'istruzione.

A livello amministrativo, già prima dell'adozione del Piano Nazionale Scuola Digitale erano stati attivati interventi finalizzati all'uso consapevole, da parte degli studenti, di internet, fra cui il progetto Generazioni connesse e la celebrazione annuale del Safer internet day (SID).

Inoltre, il 6 febbraio 2018 è stato sottoscritto un protocollo di intesa fra l'allora MIUR e l'Autorità per le garanzie nelle comunicazioni, di durata triennale, finalizzato all'acquisizione, da parte degli studenti, delle competenze necessarie all'esercizio di una cittadinanza digitale consapevole e critica.

In occasione del SID 2019 sono state presentate le nuove "Linee guida per l'uso positivo delle tecnologie digitali e la prevenzione dei rischi nelle scuole" dedicate, in particolare, agli operatori che collaborano con le scuole. Nell'anno 2020 invece il Safer Internet Day, cui hanno partecipato numerose scuole italiane e un totale di oltre sessantamila ragazzi, ha riguardato soprattutto le questioni del cyberbullismo, della privacy, del copyright e della correttezza dei comportamenti in rete, nonché l'App YouPol, la quale consente di interagire con la polizia inviando immagini o segnalazioni.

Ancora, la Commissione ha il compito di valutare l'opportunità di proporre iniziative di carattere normativo o amministrativo, volte a realizzare una più adeguata **prevenzione** e un più efficace contrasto delle attività di disinformazione e della commissione di reati attraverso i *media*, le reti sociali telematiche e le altre piattaforme analogiche e digitali (**lettera *n)***).

Del pari attiene all'opportunità di iniziative di carattere normativo o amministrativo, la valutazione che spetta alla Commissione onde contrastare la disinformazione che produca effetti negativi sulla crescita e lo sviluppo delle conoscenze dei **minori**, ove questi ricorrano all'utilizzo dei media tradizionali, delle reti sociali telematiche e delle altre piattaforme tecnologiche analogiche o digitali.

Rimane fermo quanto previsto dagli articoli 34 (disposizioni a tutela dei minori) e 35 (correlative vigilanza e sanzioni) del Testo unico dei servizi di *media* audiovisivi e radiofonici (decreto legislativo n. 177 del 2005).

Così la **lettera *o)***.

Infine spetta alla Commissione "di valutare l'opportunità" di proporre:

- ✓ iniziative normative volte al rafforzamento degli strumenti di regolazione e controllo applicabili alle **piattaforme digitali** (**lettera *p)***);
- ✓ la promozione di **campagne di informazione** e sensibilizzazione sul tema dell'**accesso responsabile alle notizie** - attraverso il sistema radiotelevisivo pubblico (anche in collaborazione con l'Ordine nazionale dei giornalisti) (**lettera *q)***);
- ✓ proporre iniziative di carattere normativo e regolamentare per contrastare il fenomeno del '***deepfake***' ossia la modellazione elettronica del linguaggio al fine di diffondere contenuti audio o video ingannevoli (**lettera *r)***).

Il *deepfake* è un contenuto audio o video manipolato attraverso strumenti informatici avanzati, in particolare strumenti legati allo sviluppo dell'intelligenza artificiale. Tali tecnologie consentono, tra l'altro, di alterare filmati di personaggi celebri o di politici, al fine di attribuire loro affermazioni false o di fantasia. Ad esempio, si veda la notizia relativa ad un video *deepfake* avente come protagonista il Presidente degli Stati Uniti Trump, fatto circolare nel 2018 da una formazione politica belga: https://www.politico.eu/article/spa-donald-trump-belgium-paris-climate-agreement-belgian-socialist-party-circulates-deep-fake-trump-video/

La composizione, i poteri e le modalità di funzionamento della Commissione (articoli 3-8)

Gli **articoli da 3 a 8** disciplinano la composizione, la durata, i poteri e le modalità di funzionamento della Commissione.

L'**articolo 3** prevede che la Commissione conclude i propri lavori **entro diciotto mesi** dalla sua costituzione (**comma 1**).

Al termine dei propri lavori, essa presenta alle Camere una relazione sull'attività svolta e sui risultati dell'inchiesta. La Commissione può riferire altresì alle Camere sullo stato dei propri lavori ogni volta che lo ritenga opportuno.

Si prevede, inoltre, la possibilità di relazioni di minoranza (**comma 2**).

L'**articolo 4** disciplina la **composizione** della Commissione.

Si prevede, in particolare, che la Commissione è composta da **venti senatori** e da **venti deputati**, nominati dai Presidenti delle rispettive Camere nel rispetto del principio di proporzione tra i gruppi parlamentari, assicurando comunque la presenza di un rappresentante per ciascun gruppo esistente in almeno un ramo del Parlamento e favorendo l'equilibrio nella rappresentanza dei sessi (**comma 1**).

La Commissione è convocata per la costituzione dell'ufficio di presidenza dai Presidenti delle due Camere entro dieci giorni dalla nomina dei suoi componenti (**comma 2**).

L'ufficio di presidenza, composto dal presidente, da due vicepresidenti e da due segretari, viene eletto dai componenti della Commissione a scrutinio segreto.

Il presidente è eletto a maggioranza assoluta dei componenti della Commissione e, qualora ciò non si verifichi, si procede al ballottaggio tra i due candidati che hanno ottenuto il maggior numero di voti, risultando eletto il candidato che ottenga il maggior numero di voti. In caso di parità di voti, è proclamato eletto (o entra in ballottaggio) il più anziano di età (**comma 3**).

Per l'elezione dei due vicepresidenti e dei due segretari, si prevede il voto limitato. Ciascun componente della Commissione può indicare sulla propria scheda un solo nome per ciascuna delle due cariche. Sono eletti coloro che abbiano ottenuto il maggior numero di voti. In caso di parità di voti, si applicano i medesimi criteri previsti per l'elezione del presidente (**comma 4**).

Le disposizioni dei **commi 3 e 4** si applicano anche per le elezioni suppletive (**comma 5**).

L'**articolo 5** definisce i **poteri** della Commissione.

Come previsto dall'articolo 82 della Costituzione, che disciplina le inchieste parlamentari, la Commissione procede alle indagini e agli esami con gli stessi poteri e le stesse limitazioni dell'autorità giudiziaria (**comma 1**).

La Commissione non può adottare provvedimenti attinenti alla libertà e alla segretezza della corrispondenza e di ogni altra forma di comunicazione nonché alla libertà personale, fatto salvo l'accompagnamento coattivo di cui all'articolo 133 del codice di procedura penale (**comma 2**).

Nello svolgimento della propria attività la Commissione non interferisce con lo svolgimento delle campagne elettorali o referendarie, in particolar modo durante il periodo di garanzia della par condicio prevista dalla legge (**comma 3**).

Inoltre, qualora la Commissione nella sua attività di indagine rilevi la diffusione di informazioni false che vedano coinvolto un giornalista, ne informa tempestivamente il presidente nazionale dell'Ordine dei giornalisti per la trasmissione degli atti al competente Consiglio di disciplina territoriale (**comma 4**).

L'articolo 133 del codice di procedura penale innanzi menzionato prevede che se il testimone, il perito, la persona sottoposta all'esame del perito diversa dall'imputato, il consulente tecnico, l'interprete o il custode di cose sequestrate, regolarmente citati o convocati, omettono senza un legittimo impedimento di comparire nel luogo, giorno e ora stabiliti, il giudice può ordinarne l'accompagnamento coattivo e può altresì condannarli, con ordinanza, al pagamento di una somma da euro 51 a euro 516 a favore della cassa delle ammende nonché alle spese alle quali la mancata comparizione ha dato causa. L'accompagnamento coattivo è disposto, nei casi previsti dalla legge, con decreto motivato, con il quale il giudice ordina di condurre l'imputato alla sua presenza, se occorre anche con la forza. La persona sottoposta ad accompagnamento coattivo non può essere tenuta a disposizione oltre il compimento dell'atto previsto e di quelli conseguenziali per i quali perduri la necessità della sua presenza. In ogni caso, la persona non può essere trattenuta oltre le ventiquattro ore.

Inoltre, la Commissione ha facoltà di acquisire, anche in deroga al divieto stabilito dall'articolo 329 del codice di procedura penale, copie di atti e di documenti relativi a procedimenti e inchieste in corso presso l'autorità giudiziaria o altri organi inquirenti. L'autorità giudiziaria può trasmettere le copie di atti e documenti anche di propria iniziativa (**comma 5**).

L'articolo 329 del codice di procedura penale concerne l'obbligo del segreto. Si prevede innanzi tutto che gli atti d'indagine compiuti dal pubblico ministero e dalla polizia giudiziaria, le richieste del pubblico ministero di autorizzazione al

compimento di atti di indagine e gli atti del giudice che provvedono su tali richieste sono coperti dal segreto fino a quando l'imputato non ne possa avere conoscenza e, comunque, non oltre la chiusura delle indagini preliminari. Inoltre, quando è necessario per la prosecuzione delle indagini, il pubblico ministero può, in deroga a quanto previsto dall'articolo 114, consentire, con decreto motivato, la pubblicazione di singoli atti o di parti di essi. In tal caso, gli atti pubblicati sono depositati presso la segreteria del pubblico ministero. Anche quando gli atti non sono più coperti dal segreto, il pubblico ministero, in caso di necessità per la prosecuzione delle indagini, può disporre con decreto motivato l'obbligo del segreto per singoli atti, quando l'imputato lo consente o quando la conoscenza dell'atto può ostacolare le indagini riguardanti altre persone e il divieto di pubblicare il contenuto di singoli atti o notizie specifiche relative a determinate operazioni.

L'autorità giudiziaria provvede tempestivamente e può ritardare la trasmissione di copia di atti e di documenti richiesti, con decreto motivato, solo per ragioni di natura istruttoria. Il decreto ha efficacia per sei mesi e può essere rinnovato. Quando tali ragioni vengono meno, l'autorità giudiziaria provvede senza ritardo a trasmettere quanto richiesto. Il decreto non può essere rinnovato o aver efficacia oltre la chiusura delle indagini preliminari (**comma 6**).

La Commissione ha altresì facoltà di acquisire copie di atti e di documenti relativi a indagini e inchieste parlamentari. Quando gli atti o i documenti siano stati assoggettati al vincolo di segreto funzionale da parte delle competenti Commissioni parlamentari di inchiesta, tale segreto non può essere opposto alla Commissione (**comma 7**).

La Commissione garantisce il mantenimento del regime di segretezza fino a quando gli atti e i documenti trasmessi in copia siano coperti da segreto (**comma 8**).

La Commissione ha inoltre facoltà di acquisire da organi e uffici della pubblica amministrazione copie di atti e di documenti da essi custoditi, prodotti o comunque acquisiti in materia attinente alle finalità della proposta di legge all'esame (**comma 9**).

Infine, la Commissione stabilisce quali atti e documenti non devono essere divulgati, anche in relazione ad esigenze attinenti ad altre istruttorie o inchieste in corso (**comma 10**).

L'**articolo 6** disciplina le **audizioni a testimonianza** innanzi alla Commissione.

Si prevede, in particolare che, ferme restando le competenze dell'autorità giudiziaria, per tali audizioni si applicano le disposizioni degli articoli 366 e 372 del Codice penale (**comma 1**).

L'articolo 366 del Codice penale sanziona chiunque, nominato dall'autorità giudiziaria perito, interprete, ovvero custode di cose sottoposte a sequestro dal giudice penale, ottiene con mezzi fraudolenti l'esenzione dall'obbligo di comparire o di prestare il suo ufficio. La sanzione prevista è la reclusione fino a sei mesi o con la multa da euro 30 a euro 516. Le stesse pene si applicano a chi, chiamato dinanzi all'autorità giudiziaria per adempiere ad alcuna delle predette funzioni, rifiuti di dare le proprie generalità ovvero di prestare il giuramento richiesto, ovvero di assumere o di adempiere le funzioni medesime. Le disposizioni precedenti si applicano alla persona chiamata a deporre come testimone dinanzi all'autorità giudiziaria e ad ogni altra persona chiamata ad esercitare una funzione giudiziaria. Se il colpevole è un perito o un interprete, la condanna importa l'interdizione dalla professione o dall'arte.

L'articolo 372 del Codice penale sanziona la falsa testimonianza punendo con la reclusione da due a sei anni chiunque, deponendo come testimone innanzi all'autorità giudiziaria o alla Corte penale internazionale, afferma il falso o nega il vero, ovvero tace, in tutto o in parte, ciò che sa intorno ai fatti sui quali è interrogato.

Per il segreto di Stato, l'articolo 6 richiama la normativa prevista dalla legge 3 agosto 2007, n. 124 (**comma 2, primo periodo**).

Il segreto di Stato è attualmente disciplinato principalmente dalla legge di riforma dei servizi di informazione (legge n. 124 del 2007) e, in sede processuale, dagli artt. 202 e segg. del codice di procedura penale. Quest'ultimo, in particolare, prevede tra l'altro che i pubblici ufficiali, i pubblici impiegati e gli incaricati di un pubblico servizio abbiano l'obbligo di astenersi dal deporre su fatti coperti dal segreto di Stato.

In nessun caso, per i fatti rientranti nei compiti della Commissione, possono essere opposti il segreto d'ufficio, il segreto professionale e il segreto bancario (**comma 2, secondo periodo**), mentre è sempre opponibile il segreto tra difensore e parte processuale nell'ambito del mandato (**comma 3**).

Si ricorda che il segreto d'ufficio obbliga l'impiegato pubblico a non divulgare a chi non ne abbia diritto informazioni riguardanti provvedimenti od operazioni amministrative, ovvero notizie di cui sia venuto a conoscenza a causa delle sue funzioni, al di fuori delle ipotesi e delle modalità previste dalle norme sul diritto di accesso (art. 15, DPR 3/1957). In sede processuale, salvi i casi in cui hanno l'obbligo di riferirne all'autorità giudiziaria, i pubblici ufficiali, i pubblici impiegati e gli incaricati di un pubblico servizio hanno l'obbligo di astenersi dal deporre su fatti conosciuti per ragioni del loro ufficio che devono rimanere segreti (art. 201 c.p.p.).

La non opponibilità del segreto professionale e di quello bancario è stata prevista da altri provvedimenti di istituzione di commissioni di inchiesta. Si veda, ad esempio, la L. 107/2017 di istituzione della Commissione di inchiesta sul sistema bancario e finanziario (art. 4) nonché, da ultimo, la L. 99/2018 che ha istituito la Commissione d'inchiesta sul fenomeno delle mafie e altre associazioni criminali, anche straniere. Determinate categorie di persone (sacerdoti, medici, avvocati ecc.) non possono essere obbligati a deporre su quanto hanno conosciuto per ragione del proprio ministero, ufficio o professione, salvi i casi in cui hanno l'obbligo di riferirne all'autorità giudiziaria, ad esempio in qualità di periti (segreto professionale ex art. 200 c.p.p.).

Per quanto riguarda il segreto bancario si applicano le disposizioni in materia di riservatezza dei dati personali che prevedono che la comunicazione a terzi di dati personali relativi a un cliente è ammessa se lo stesso vi acconsente (art. 23 del Codice della *privacy*, D.lgs. 196/2003) o se ricorre uno dei casi in cui il trattamento può essere effettuato senza il consenso (art. 24 del Codice). Fuori dei casi di operazioni di comunicazione dei dati strumentali alle prestazioni richieste e ai servizi erogati (per le quali non è necessario ottenere il consenso degli interessati: art. 24, comma 1, lettera *b)*, del Codice), gli istituti di credito e il personale incaricato dell'esecuzione delle operazioni bancarie di volta in volta richieste devono mantenere il riserbo sulle informazioni utilizzate. Parziali deroghe sono previste per le indagini tributarie.

Infine, si prevede l'applicazione dell'articolo 203 del codice di procedura penale (**comma 4**).

L'art. 203 c.p.p. stabilisce che non si possano obbligare gli ufficiali e gli agenti di polizia giudiziaria nonché il personale dipendente dai servizi per le informazioni e la sicurezza militare o democratica, a rivelare i nomi dei loro informatori. Se questi non sono esaminati come testimoni, le informazioni da essi fornite non possono essere acquisite né utilizzate.

L'**articolo 7** disciplina l'**obbligo di segreto** per i componenti della Commissione, i funzionari e il personale di qualsiasi ordine e grado addetto alla Commissione stessa, nonché ogni altra persona che collabori con la Commissione o compia o concorra a compiere atti di inchiesta oppure ne venga a conoscenza per ragioni di ufficio o di servizio.

Tali persone sono obbligate al segreto per tutto quanto riguardi gli atti e i documenti trasmessi in copia relativi a procedimenti e ad inchieste in corso presso l'autorità giudiziaria o altri organi inquirenti che siano coperti da segreto nonché per quanto riguardi gli atti e i documenti per i quali la Commissione abbia deliberato il divieto di divulgazione, anche in relazione ad esigenze attinenti ad altre istruttorie o inchieste in corso (**comma 1**).

La violazione del segreto è punita ai sensi dell'articolo 326 del codice penale, salvo che il fatto costituisca più grave reato (**comma 2**).

L'articolo 326 del Codice penale, che punisce la rivelazione e l'utilizzazione del segreto d'ufficio, prevede che il pubblico ufficiale o la persona incaricata di un pubblico servizio che, violando i doveri inerenti alle funzioni o al servizio, o comunque abusando della sua qualità, rivela notizie di ufficio, le quali debbano rimanere segrete, o ne agevola in qualsiasi modo la conoscenza, è punito con la reclusione da sei mesi a tre anni. Viene punita inoltre l'agevolazione colposa per la quale si applica la reclusione fino a un anno. Il pubblico ufficiale o la persona incaricata di un pubblico servizio che, per procurare a sé o ad altri un indebito profitto patrimoniale, si avvale illegittimamente di notizie di ufficio, le quali debbano rimanere segrete, è punito con la reclusione da due a cinque anni. Se il fatto è commesso al fine di procurare a sé o ad altri un ingiusto profitto non patrimoniale o di cagionare ad altri un danno ingiusto, si applica la pena della reclusione fino a due anni.

Le pene previste per la fattispecie sopra descritta si applicano inoltre a chiunque diffonda in tutto o in parte, anche per riassunto o informazione, atti o documenti del procedimento di inchiesta dei quali sia stata vietata la divulgazione, salvo che il fatto costituisca più grave reato (**comma 3**).

L'**articolo 8** disciplina l'**organizzazione dei lavori** della Commissione.

Si prevede che l'attività e il funzionamento della Commissione sono disciplinati da un **regolamento interno** approvato dalla Commissione stessa prima dell'inizio dell'attività di inchiesta. Ciascun componente può proporre la modifica delle norme regolamentari (**comma 1**).

La Commissione può organizzare i propri lavori tramite uno o più gruppi di lavoro, disciplinati dal sopra citato regolamento (**comma 2**).

Le sedute della Commissione sono pubbliche. Ma tutte le volte che lo ritenga opportuno, la Commissione può deliberare di riunirsi in seduta segreta (**comma 3**).

La Commissione, per l'adempimento delle sue funzioni, può avvalersi di agenti e ufficiali di polizia giudiziaria, nonché di soggetti interni o esterni all'amministrazione dello Stato, autorizzati, ove occorra e con il loro consenso, dagli organi a ciò deputati e dai Ministeri competenti. La Commissione può altresì avvalersi di consulenti ed esperti del settore dell'informazione on line e di tutte le collaborazioni che ritenga necessarie. Con il regolamento interno è stabilito il numero massimo di collaboratori (**comma 4**).

Per l'adempimento delle sue funzioni, la Commissione fruisce di personale, locali e strumenti operativi messi a disposizione dai Presidenti delle Camere, d'intesa tra loro (**comma 5**).

Per quanto riguarda le **spese per il funzionamento** della Commissione, stabilite nella misura massima di 100.000 euro annui, esse sono poste per metà a carico del bilancio interno del Senato della Repubblica e per metà a carico del bilancio interno della Camera dei deputati (**comma 6**).

La Commissione stabilisce le modalità di pubblicazione delle spese dalla stessa sostenute, fatte salve quelle connesse ad atti e a documenti soggetti a regime di segretezza (**comma 7**).

Alla Commissione spetta infine la cura dell'informatizzazione dei documenti acquisiti e prodotti nel corso della sua attività (**comma 8**).

Entrata in vigore (articolo 9)

L'**articolo 9** dispone l'entrata in vigore della legge il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

La responsabilità dei prestatori di servizi (*providers*) in Internet e il controllo delle notizie false nella rete: regolazione e autoregolazione

La diffusione intenzionale di notizie false (*fake news*) rappresenta una problematica intrinsecamente connessa alla rete Internet, connotata da una inedita possibilità per tutti gli utenti che ne fanno uso, a costi irrisori o addirittura gratuitamente, di creare e diffondere contenuti informativi.

Le informazioni possono essere generate senza filtro e senza che chi veicoli l'informazione stessa sia un professionista, e quindi vincolato ai principi deontologici della professione e ai controlli sul loro rispetto.

La diffusione di tali notizie e il credito che queste raggiungono si fondano peraltro su meccanismi molto diversi rispetto alle modalità informative tradizionali e tali da prescindere da un effettivo riscontro obiettivo dei contenuti della notizia, fondandosi di contro su una condivisione basata su forme di adesione immediata, istintiva e talora nemmeno pienamente consapevole.

L'apparente anarchia e 'orizzontalità' della rete non nasconde peraltro la possibilità che soggetti specifici, dotati di risorse talora anche ingenti, avvalendosi anche dei grandi sviluppi tecnologici dell'intelligenza artificiale, possano deliberatamente generare veri e propri flussi di informazione falsa, scientificamente diretti a perseguire gli obiettivi più variegati (commerciali, politici, di propaganda, ecc.) che finiscono, proprio avvalendosi delle piattaforme *social* e non solo, a creare tensioni nelle pubbliche opinioni inquinando talora pesantemente il dibattito pubblico.

La diffusione sempre maggiore di queste pratiche ha portato le istituzioni a interrogarsi sulle modalità più efficaci per contrastare le notizie false anche provando a individuare meccanismi di limitazione alla fonte della loro diffusione.

Occorre preliminarmente segnalare che l'esigenza di bloccare 'a monte' le *fake news* potrebbe porsi in tensione, se non in palese contrasto, con quanto prevede la direttiva 31/2000/CE in tema di responsabilità degli *Internet Service Providers* recepita in Italia dal decreto legislativo n. 70 del 2003.

Pur con vari temperamenti è infatti fermo il principio secondo il quale i prestatori di servizi della società dell'informazione **non rispondono dei contenuti immessi in rete dagli utenti** in quanto non è previsto un obbligo generale di verifica dei contenuti a loro carico (articolo 15 della direttiva 31/2000/CE).

I prestatori di servizi della società dell'informazione, ai sensi della citata direttiva, sono differenziati a seconda dell'attività che forniscono in rete: i prestatori di semplice trasporto (*mere conduit*), i prestatori di servizi di

memorizzazione temporanea (*caching*), e i prestatori di servizi di memorizzazione di informazione (*hosting*).

Rientrano in tali categorie ad esempio i fornitori di rete, i motori di ricerca, i *browser*, le piattaforme di *blogging online*, i forum *online*, le piattaforme per la condivisione di video, i *social media*, eccetera.

Con riferimento al servizio di *mere conduit* il prestatore non è responsabile a meno che non abbia dato origine alla trasmissione, non ne abbia selezionato il destinatario o abbia selezionato e modificato il contenuto trasmesso.

Con riferimento al *caching* la responsabilità del *service provider* si verifica nel caso in cui esso abbia modificato le informazioni, non si conformi alle informazioni di accesso o alle norme di aggiornamento, interferisca con l'uso lecito di tecnologia per ottenere dati sull'impiego delle informazioni; se non agisca prontamente per rimuovere le informazioni o per disabilitare l'accesso, quando le informazioni sono state rimosse dal luogo in cui si trovavano in rete o sia stato disabilitato l'accesso alle stesse ovvero un'autorità giudiziaria o amministrativa abbia disposto in tal senso.

Con riferimento infine all'*hosting* la responsabilità del prestatore del servizio è esclusa a condizione che il prestatore del servizio non sia a conoscenza che l'informazione veicolata sia illecita e non sia a conoscenza di fatti e circostanze che rendono palese l'illegalità dell'informazione o dell'attività e che, qualora ne venga a conoscenza, agisca immediatamente per rimuovere le informazioni e disabilitarne l'accesso.

L'esenzione dalla responsabilità dell'ISP (acronimo di *Internet Service Provider* ossia prestatore di servizi della società dell'informazione) si basa sulla natura esclusivamente tecnica del servizio da questo prestato, e tale esenzione viene meno quando l'ISP, venuto a conoscenza dell'illiceità dell'informazione o dell'attività, non si attivi prontamente per la sua rimozione.

La Corte di giustizia dell'Unione europea è a più riprese intervenuta in particolare in merito alla problematica della diffusione illecita in rete di contenuti coperti da *copyright.*

In questi casi la Corte ha escluso la sussistenza di un obbligo di predisporre un 'filtro preventivo' da parte degli ISP a tutela del diritto d'autore che sarebbe un onere insostenibile sia sotto il profilo tecnico che economico per gli intermediari, in quanto implicherebbe necessariamente lo scrutinio preventivo e generalizzato dei contenuti veicolati, oltre a porre seri problemi in merito al rispetto della privacy dei singoli utenti. È invece richiesta una collaborazione degli ISP a valle nel caso in cui sia segnalato nelle forme previste un contenuto o un'informazione illecita. In tale circostanza l'ISP deve intervenire prontamente.

Con riferimento alla tutela della privacy, nel **2014 la Corte di Giustizia UE** era intervenuta (Sentenza nella Causa C-131/12 contro Google Spain) nella questione dell'indicizzazione delle pagine web da parte dei motori di ricerca, affermando che **il gestore di un motore di ricerca su Internet** (come Google) **è responsabile del trattamento da esso effettuato dei dati personali che appaiono su pagine web pubblicate da terzi**, nel senso che, se a seguito di una ricerca effettuata con il motore di ricerca, a partire dal nome di una persona, l'elenco di risultati mostra un link verso una pagina web che contiene dati personali sul soggetto in questione, la persona interessata può rivolgere domanda di cancellazione dei link che la riguardino direttamente al gestore del motore di ricerca, che deve procedere al debito esame della loro fondatezza, e qualora questi non dia seguito alla sua domanda l'interessato può adire le autorità competenti per ottenere, in presenza di determinate condizioni, la soppressione di tale link dall'elenco di risultati.

Inoltre come evidenziato nella Sentenza della Corte di Giustizia del 21 dicembre 2016 (Cause riunite C-203/2015), il diritto dell'Unione **osta ad una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione degli utenti dei servizi di comunicazione elettronica**, perché tali dati presi nel loro insieme, consentono di ricostruire il profilo delle persone interessate (le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali e gli ambienti sociali frequentati). Gli Stati membri possono però limitare tali diritti e obblighi previsti della direttiva, qualora tale restrizione costituisca una misura necessaria, opportuna e proporzionata per la salvaguardia della sicurezza dello Stato, della difesa, della sicurezza pubblica, e per la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono adottare una normativa la quale consenta, a titolo preventivo, la conservazione mirata dei dati relativi al traffico e i dati relativi all'ubicazione, per finalità di lotta contro la criminalità grave, a condizione che la conservazione dei dati sia, per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista, limitata allo stretto necessario.

Sulla base di tali presupposti le iniziative di contrasto alla diffusione di notizie false sembrano privilegiare, sia a livello nazionale che europeo, la diffusione di iniziative di regolazione **consensuale**.

Cenni sull'attività delle Autorità indipendenti

Con riferimento al controllo delle notizie false l'**Autorità per le Garanzie nelle Comunicazioni** (AGCOM) ha istituito (il 6 novembre 2017) ha istituito il "Tavolo per la garanzia del pluralismo e della correttezza dell'informazione sulle piattaforme digitali" che ha l'obiettivo di favorire e promuovere

l'autoregolamentazione delle piattaforme e lo scambio di buone prassi per l'individuazione ed il contrasto dei fenomeni di disinformazione *online* frutto di strategie mirate.

Nell'ambito del Tavolo sono stati costituiti diversi gruppi di lavoro[1].

L'iniziativa, decisa con la **delibera 423/17/CONS**, si inscrive nel percorso istituzionale intrapreso da AGCOM, a partire dal 2015, con la Pubblicazione di rapporti e indagini conoscitive sul sistema dell'informazione *online*.

L'Autorità per le Garanzie nelle Comunicazioni, con delibera n. 309/16/CONS del 21 giugno 2016, ha avviato un'indagine conoscitiva su "Piattaforme digitali e sistema dell'informazione", conclusasi nel 2020. Un importante esito tale indagine è stato il rapporto **News vs. fake nel sistema dell'informazione** , pubblicato a novembre 2018. Con una nuova delibera, n. 79/20/CONS del 27 febbraio 2020, l'Autorità ha dichiarato chiusa l'indagine conoscitiva. In allegato alla delibera 79/2020CONS, l'Autorità ha pubblicato il Rapporto Percezioni e disinformazione. Molto "razionali" o troppo "pigri"?. Quest'ultimo testo analizza la domanda di informazione e di disinformazione, come gli utenti reagiscono rispetto a notizie di qualità differenti e ne valutano l'affidabilità, i meccanismi cognitivi che influenzano i processi decisionali sottostanti al consumo di informazione e la maniera nella quale in questi processi si inseriscono le percezioni dei fenomeni e altri elementi. Contestualmente, l'Autorità ha anche definito le prossime linee di intervento. In particolare, è prevista l'implementazione di un sistema di monitoraggio continuativo della qualità dell'informazione online, accanto a misure di vigilanza per salvaguardare il pluralismo e la concorrenza.

Ulteriori iniziative sono state assunte anche da parte del **Garante per la protezione dei dati personali**.

Assai significativa in questo senso l'iniziativa del Garante per la protezione dei dati personali che, per la prima volta, si è pronunciato nei confronti di ***Facebook*** nel 2016 [doc. web n. 4833448], imponendo di **bloccare i falsi profili** (i cosiddetti *fake*) e di assicurare più trasparenza e controllo agli utenti, affermando innanzitutto la propria competenza a intervenire a tutela degli utenti italiani. La multinazionale, infatti, è presente sul territorio italiano con un'organizzazione stabile, *Facebook Italy srl*, la cui attività è da considerare inestricabilmente connessa con quella svolta da

[1] Sono: Gruppo a) Metodologie di classificazione e di revisione: che si propone l'obiettivo della definizione delle metodologie di classificazione e rilevazione dei fenomeni di disinformazione online; Gruppo b) Definizione dei sistemi di monitoraggio dei flussi economici pubblicitari, da fonti nazionali ed estere, volti al finanziamento di contenuti *fake* volto a ricostruire i flussi di finanziamento delle strategie mirate di disinformazione *online* al fine di elaborare soluzioni per il monitoraggio dei flussi economici pubblicitari, da fonti nazionali ed estere, volti al finanziamento dei contenuti di disinformazione online. Obiettivo del gruppo è quello di favorire l'utilizzo di codici di elaborazione di codici di auto-regolamentazione Gruppo c): *Fact-checking*: organizzazione, tecniche, strumenti ed effetti con l'obiettivo di redazione di un report e di implementazione di soluzioni di mercato; Gruppo d): Media e *digital literacy*, con l'obiettivo di promuovere la cultura mediatica e digitale fornendo ai cittadini strumenti per un uso consapevole e critico dei (social e non) media.

Facebook Ireland ltd che ha effettuato il trattamento di dati contestato, per cui al caso di specie risulta applicabile il diritto nazionale (in base alla sentenza della Corte di Giustizia Europea Weltimmo del 1° ottobre 2015 C, nonché il WP 179). Il Garante ha accolto le tesi del ricorrente ritenendolo, in base alla normativa italiana, legittimato ad accedere a tutti i dati che lo riguardano compresi quelli presenti e condivisi nel falso account. Ha quindi ordinato a *Facebook* di comunicare all'interessato tutte le informazioni richieste entro un termine preciso, in modo chiaro e comprensibile, comprese le informazioni sulle finalità, le modalità e la logica del trattamento dei dati, i soggetti cui sono stati comunicati o che possano venirne a conoscenza.

Il ricorso a **profili falsi** rappresenta infatti uno dei principali strumenti per favorire la diffusione e la condivisione di notizie false.

Gli strumenti penali di repressione delle *fake news*

Le notizie false possono implicare anche **conseguenze penali**, derivanti dalla loro pubblicazione e diffusione ad un numero indeterminato di persone.

In particolare, la pubblicazione in rete di una notizia falsa può essere certamente idonea a determinare la lesione dell'onore di una persona, così come la diffusione di notizie false potrebbe procurare allarme sociale.

Nel primo caso può essere integrata la fattispecie delittuosa della **diffamazione** a mezzo stampa[2]; nella seconda – che, per caratteristiche della fattispecie si avvicina più alle fake news - potrebbero ricorrere gli estremi del reato di **pubblicazione o diffusione di notizie false, esagerate o tendenziose, idonee a turbare l'ordine pubblico**.

Altro possibile illecito nell'ambito in questione, pur non avendo la notizia falsa come elemento oggettivo del reato, è quello che si ricollega al fenomeno dei falsi profili in rete (cd. **profili *fake***).

L'ordinamento nazionale non prevede una specifica fattispecie penale che punisca i cd. falsi profili (profili fake) presenti sul web

Attualmente, creare, ad esempio, un **profilo falso su Facebook non costituisce reato**. Il regolamento del social network vieta questo tipo di attività ma non vi è alcuna legge nazionale che pone divieti o sanzioni in tal senso.

In certe ipotesi, tuttavia**, possono sussistere conseguenze penali** ove il falso profilo è utilizzato per commettere illeciti (come diffamazione, truffa, molestie, ecc.). In particolare, se mediante la creazione del falso profilo si finge di essere un'altra persona si incorre nel **delitto di sostituzione di persona**.

Infatti, l'**art. 494 c.p.** punisce con la **reclusione fino a un anno** chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a

[2] Al contrario, l'ingiuria è ora estranea all'ambito penale in quanto oggetto di depenalizzazione ex D.Lgs. 7/2016. L ingiurie (in rete e non) sono punite con sanzioni pecuniarie civili.

sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici. Oggetto della tutela penale è qui l'interesse alla pubblica fede, da tutelare da inganni relativi all'identità della persona o ai suoi attributi sociali. Trattandosi di inganni particolarmente pervasivi che possono, tramite la diffusione in rete, raggiungere un numero indeterminato di persone, il legislatore ha ravvisato in essi una costante insidia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome.

La diffamazione online

L'**art. 595 c.p**. punisce chiunque comunicando con più persone offende l'altrui reputazione. La **diffamazione col mezzo della stampa** o con qualsiasi altro mezzo di pubblicità è considerata aggravante del reato base (sanzionato con la reclusione fino a un anno o con la multa fino a 1.032 euro) ed è punita *con la* ***reclusione da sei mesi a tre anni o la multa non inferiore a 516 euro.***

La giurisprudenza ha costantemente compreso tra le modalità di perfezionamento del reato gli strumenti telematici (cd. ***diffamazione online***), anche se non esplicitamente indicati dalla legge. In particolare, il riferimento a "qualsiasi altro mezzo di pubblicità" di cui all'articolo 595 c.p., comma 3, ha consentito di ritenere aggravata la diffamazione consumata tramite internet (Cassazione penale, Sez. 5, sent. n. 40980 del 2012). Si pensi, inoltre, allo stesso dettato costituzionale, che, all'articolo 21, accanto alla parola e allo scritto (e in particolare alla stampa), prevede "ogni altro mezzo di diffusione".

Con riguardo alla diffamazione a mezzo Internet la sussistenza della comunicazione a più persone si presume nel momento stesso in cui il messaggio offensivo viene inserito su un sito Internet che, per sua natura, è destinato ad essere visitato da un numero indeterminato di persone in breve tempo. Da ciò ne deriva che il principio secondo cui la diffusione di una notizia immessa nei c.d. mezzi di comunicazione di massa si presume fino a prova contraria, non viene meno in relazione alle comunicazioni su Internet (Cass, sez. 5, sent. 4 aprile 2008). Oggi è indubbio che offendere una persona scrivendo un "post" sulla sua bacheca di Facebook integra il reato di diffamazione aggravata, esattamente come se l'offesa venisse portata dalle colonne di un giornale (Cass., sent., Sezione I, sentenza 28 Aprile 2015, n. 24431; nello stesso senso, Cassazione penale, Sezione V, sentenza 1 Marzo 2016, n. 8328).

La diffusione di notizie false, esagerate o tendenziose

Certamente **più aderente alle ipotesi di fake news** è la fattispecie che nel codice penale sanziona in via contravvenzionale la diffusione di notizie false idonee a turbare l'ordine pubblico. Ciò, anche se il serio limite alla perseguibilità penale appare qui l'accertamento della effettiva idoneità della falsa notizia a creare tale turbativa.

L'art. **656 c.p.** punisce, infatti, – se il fatto non costituisce un più grave reato - con **l'arresto fino a tre mesi o con l'ammenda fino a euro 309 chiunque pubblica o diffonde notizie false, esagerate o tendenziose**, per le quali possa essere turbato l'ordine pubblico. Si tratta di un reato di pericolo, sicché nulla rileva, ai fini della sua esclusione, il fatto che non si sia verificato alcun turbamento dell'ordine pubblico, essendo sufficiente che vi fosse un'astratta possibilità che un tale turbamento in effetti si verificasse.

L'esplicita formulazione della norma e la sua collocazione sistematica chiarisce che il bene tutelato è l'ordine pubblico, da intendersi come il buon assetto e il regolare andamento del vivere civile, cui corrisponde nella collettività l'opinione ed il senso della tranquillità e della sicurezza. Risulta minoritaria in dottrina l'idea che l'art. 656 tuteli anche il **bene della *verità cronistica*** (così Chiarotti, Diffusione o pubblicazione di notizie false o tendenziose, in ED, XII, Varese, 1964, 515; Nuvolone, I reati di stampa, Milano, 1951, 97): non è sanzionata, infatti, la divulgazione di notizie false inidonee a esporre a pericolo l'ordine pubblico.

L'art. 656 tutela l'ordine pubblico in senso lato e generico: in virtù della clausola di sussidiarietà espressamente prevista, la diffusione di notizie false, esagerate o tendenziose le quali espongano a pericolo o turbino l'ordine pubblico in qualche suo speciale aspetto, particolarmente tutelato dalla legge penale, integra il solo reato specifico, sempre che esso sia più grave della contravvenzione in esame. Quest'ultima, ad esempio, risulta assorbita dai reati previsti dagli artt. 265 (disfattismo politico), 267 (disfattismo economico), 269 (attività antinazionale del cittadino all'estero), 501 (rialzo e ribasso fraudolento di prezzi sul pubblico mercato o nelle borse di commercio), 661 (abuso della credulità popolare).

La **Corte costituzionale** - premesso che l'espressione ***«notizie false, esagerate e tendenziose»*** va letta come «una forma di endiadi, con la quale il legislatore si è proposto di abbracciare ogni specie di notizie che, in qualche modo, rappresentino la realtà in modo alterato» e precisato che le "notizie tendenziose" sono quelle che, pur riferendo cose vere, le presentino tuttavia in modo che chi l'apprende possa avere una rappresentazione alterata della realtà (perché sono riferiti solo una parte degli accadimenti, o perché l'esposizione è tale da determinare confusione fra la notizia e il commento) - **ha escluso la illegittimità costituzionale dell'art. 656**, prospettata in

relazione agli artt. 18, 21 e 49 Cost.: devono ritenersi legittime, infatti, tutte le disposizioni legislative che - come l'art. 656 - siano volte a prevenire turbamenti all'ordine pubblico, poiché tale bene, da intendersi come «ordine legale su cui poggia la convivenza sociale» è «connaturale ad un sistema giuridico in cui gli obiettivi consentiti ai consociati non possono essere realizzati se non con gli strumenti e attraverso i procedimenti previsti dalle leggi, e non è dato per contro pretendere di introdurvi modificazioni o deroghe attraverso forme di coazione o addirittura di violenza»; né all'emanazione di disposizioni di tale genere può costituire ostacolo l'esistenza di diritti costituzionalmente garantiti, i quali trovano un limite insuperabile nell'esigenza che attraverso l'esercizio di essi non vengano sacrificati beni ugualmente garantiti dalla Costituzione (C., Cost. 16.3.1962, n. 19; nello stesso senso la successiva ordinanza C., Cost. 22.6.1962, n. 80 e le sentenze C., Cost. 29.12.1972, n. 199 e C. Cost. 3.8.1976, n. 210).

Il significato del termine **pubblicare** nell'art. 656 è stato variamente ricostruito; appare certo, tuttavia, che, che la pubblicazione sia una specie della più ampia condotta di diffusione e che, dunque, la norma punisca in definitiva la trasmissione di notizie ad un numero indeterminato di persone in qualunque forma.

Gli strumenti penali di repressione del c.d. *hate speech*

Uno degli illeciti più comuni commessi sulla rete internet riguarda l'incitamento all'odio (razziale, etnico, religioso), il cd. ***hate speech***.

Il principale riferimento della normativa italiana nella lotta all'odio è stato la legge n. 654 del 1957, come modificata dalla legge n. 122 del 1993, con cui il nostro Paese ha ratificato la Convenzione di New York sull'eliminazione di tutte le forme di discriminazione razziale.

Il contenuto del suo articolo 3 - che il D.lgs. 21 del 2018 ha fatto confluire nel nuovo **art. 604-*bis* del codice penale** – punisce con pene detentive chi propaganda idee fondate sulla superiorità o sull'odio razziale, ovvero istiga a commettere o commette atti di violenza o di provocazione alla violenza, nei confronti di persone perché appartenenti a un gruppo nazionale, etnico o razziale.

L'art. 604-bis c.p. punisce:

a) con la reclusione fino ad un anno e sei mesi o con la multa fino a 6.000 euro chi propaganda idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi;

b) con la reclusione da sei mesi a quattro anni chi, in qualsiasi modo, istiga a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi.

La norma vieta ogni organizzazione, associazione, movimento o gruppo avente tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi. Chi partecipa a tali organizzazioni, associazioni, movimenti o gruppi, o presta assistenza alla loro attività, è punito, per il solo fatto della partecipazione o dell'assistenza, con la reclusione da sei mesi a quattro anni. Coloro che promuovono o dirigono tali organizzazioni, associazioni, movimenti o gruppi sono puniti, per ciò solo, con la reclusione da uno a sei anni.

Si applica la pena della reclusione da due a sei anni se la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale.

La disposizione vigente è il risultato di una modifica avvenuta con **legge n. 85 del 2006** sui reati di opinione che, oltre a ridurre i limiti edittali delle pene detentive (peraltro già ridotti in precedenza con la citata legge Mancino) e a prevedere pene pecuniarie alternative alla reclusione, ha sostituito con «propaganda» la precedente espressione «diffonde in qualsiasi modo» e con «istiga» il precedente «incita». Ne deriva che **la qualificazione del reato deve oggi corrispondere a condotte di maggiore gravità** (propaganda e istigazione in luogo di diffusione e incitamento). Va inoltre ricordata la *legge n. 962 del 1967*, che all'art. 8 sanziona l'apologia di genocidio e la pubblica istigazione a commettere qualcuno dei delitti di genocidio previsti dalla legge stessa.

Nella scorsa legislatura, la **legge n. 115 del 2016** ha attribuito rilevanza penale (reclusione da 2 a 6 anni) alle ***affermazioni negazioniste*** della Shoah, dei fatti di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti rispettivamente dagli artt. 6, 7 e 8 dello Statuto di Roma, istitutivo della Corte penale internazionale. Tali affermazioni non integrano un autonomo reato, bensì una ***circostanza aggravante speciale*** dei delitti di propaganda razzista, di istigazione e di incitamento di atti di discriminazione commessi per motivi razziali, etnici, nazionali o religiosi, ora puniti dall'art. 604-bis, terzo comma, del codice penale

Più di recente, la legge europea 2017 (**legge 167 del 2017**) ha ampliato il campo di applicazione della citata aggravante di "negazionismo" prevedendo la sanzionabilità – oltre che della negazione – anche della ***minimizzazione in modo grave***, dell'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra.

É stato poi modificato il decreto legislativo n. 231 del 2001 aggiungendo al catalogo dei delitti che comportano la responsabilità delle persone giuridiche anche i reati di razzismo e xenofobia aggravati dal negazionismo. Oltre a pene pecuniarie sono, in tal caso, applicate all'ente specifiche sanzioni interdittive di entità proporzionata alla gravità dell'illecito.

Sui temi del discorso d'odio va, infine, ricordata nella scorsa legislatura l'attività della **Commissione** "Jo Cox"[3] sull'intolleranza, la xenofobia, e i fenomeni d'odio, istituita presso la Camera dei deputati per iniziativa della Presidenza.

La Commissione, al termine di un'ampia attività conoscitiva, nella quale sono stati auditi 31 soggetti, ed acquisiti 187 documenti tra studi, ricerche, pubblicazioni monografiche, raccolte di dati, position papers - ha presentato una Relazione finale approvata il 6 luglio 2017, che formula una serie di **raccomandazioni** per la prevenzione e il contrasto del linguaggio d'odio a livello sociale, culturale, informativo e istituzionale.

Tra le raccomandazioni, si segnalano quelle volte a ***sanzionare penalmente le campagne d'odio*** (insulti pubblici, diffamazione o minacce) contro persone o gruppi; di valutare, sulla base delle esperienze di altri Paesi e tutelando la libertà d'informazione in Internet, la possibilità di esigere l'*autoregolazione delle piattaforme al fine di rimuovere l'hate speech online* e di stabilire la responsabilità giuridica solidale dei provider e delle piattaforme di social network e obbligarli a rimuovere con la massima tempestività i contenuti segnalati come lesivi da parte degli utenti; di esigere da parte delle piattaforme dei social network l'istituzione di *uffici dotati di risorse umane adeguate, al fine della ricezione delle segnalazioni e della rimozione tempestiva dei discorsi d'odio*, anche attivando *alert* sulle pagine online e numeri verdi a disposizione degli utenti.

Nel corso dei lavori della Commissione sono inoltre emerse, tra le altre, le seguenti proposte:

- fornire una **definizione legale di *hate speech*** universalmente riconosciuta;
- **includere il genere** tra gli elementi aggravanti della commissione di fatti di *hate speech (dunque una modifica dell'art. 3 della legge 654/1975)*;
- aggiornare la legislazione per includere, dopo averli individuati, i discorsi d'odio sessisti nella casistica dei divieti inseriti riguardo alle espressioni di odio, dove la normativa già lo prevede piuttosto che, come succede in molti Stati membri, applicare a tali casi, con interpretazione estensiva, norme che regolano situazioni quali cyberstalking, leggi sulla pornografia, sul cyber bullismo; dalla carenza definitoria derivano infatti, a cascata: - difficoltà per le autorità di controllo, la polizia, pubblici ministeri e giudici, di circoscrivere il fenomeno, - difficoltà nelle indagini; - facilità nel creare un clima di impunità per i responsabili;

[3] La Commissione prendeva il nome dalla deputata presso la Camera dei Comuni del Regno Unito, uccisa il 16 giugno 2016 mentre si apprestava a partecipare ad un incontro con gli elettori. La Commissione, istituita presso la Camera dei deputati, era composta da un deputato per ogni gruppo politico, rappresentanti di organizzazioni sovranazionali, di istituti di ricerca e di associazioni ed esperti.

- prevedere un **referente nazionale** che possa fare da canale diretto e, su segnalazione della vittima del contenuto, d'odio, di molestia, ecc. possa intervenire rapidamente e raggiungere l'organo di comunicazione online che ha pubblicato il contenuto per farlo bloccare prontamente;
- rendere il controllo, oltre che finalizzato alla rimozione dei contenuti, anche preventivo, attraverso **meccanismi di filtraggio automatici** (imposti dalla legge) dei contenuti d'odio e l'introduzione di un c.d. early warning, una sorta di avvertimento, che appaia prima della pubblicazione di un post, segnalandone il contenuto potenzialmente lesivo e discriminatorio e richiedendo all'utente un'ulteriore ed espressa conferma per procedere alla pubblicazione online; Attivare quindi i cd. *trigger warning*, filtri che permettano il blocco dei contenuti che possono essere ritenuti offensivi o sensibili o inadatti anche a fasce di età particolari; se, dunque, navigando su Facebook e sfogliando il proprio flusso di notizie, un utente incontra un contenuto che gli altri utenti hanno segnalato come inadatto o potenzialmente offensivo, quest'ultimo non verrà mostrato fino al momento in cui l'utente stesso decida di visualizzarlo.
- prevedere **un'azione governativa** che possa imporre ai social network che vogliano operare in un Paese, la condizione di osservarne integralmente le regole e, quindi, anche l'eventuale richiesta dell'autorità di eliminare un contenuto.
- prevedere in via legislativa una **responsabilità solidale** in capo ai soggetti che operano sulla rete e a coloro che gestiscono tali siti, in modo da obbligare questi ultimi a predisporre un controllo quanto meno successivo di quanto pubblicato online dagli utenti.
- predisporre un **sistema di monitoraggio** dei principali media e social network, basato su regole condivise, che permetta, da un lato, di minare la credibilità di quei siti web che maggiormente si caratterizzano per fenomeni di hate speech e, dall'altro, di individuare tematiche particolarmente colpite da detto fenomeno, al fine di porre in essere un'opera di "controinformazione" per scongiurare la diffusione di sentimenti d'odio a contenuto discriminatorio.