Camera dei deputati
Servizio Studi
XVIII Legislatura

Documentazione per l'esame di
Progetti di legge

Istituzione di una Commissione parlamentare di inchiesta sulla diffusione massiva di informazioni false
A.C. T.U. 1056-2103-2187-2213-A

Dossier n° 182/1 - Elementi per l'esame in Assemblea
17 luglio 2020

Informazioni sugli atti di riferimento

A.C.	T.U. 1056-2103-2187-2213-A
Titolo:	Istituzione di una Commissione parlamentare di inchiesta sulla diffusione massiva di informazioni false
Iniziativa:	Parlamentare
Primo firmatario:	Fiano, Boschi, Frassinetti, Lattanzio

Contenuto

Il testo unificato delle proposte di legge – elaborato dal Comitato ristretto e modificato, dopo l'adozione quale testo base, durante l'esame in sede referente - prevede l'istituzione, ai sensi dell'art. 82 della Costituzione, di una Commissione parlamentare di inchiesta sulla diffusione massiva di informazioni false (**articolo 1**).

In particolare, alla Commissione sono attribuiti **undici** compiti, indicati all'**articolo 2**. Gli stessi possono essere raggruppati in due ambiti.

Il **primo gruppo** di compiti (co. 1, lett. da *a*) ad *e*)) è volto ad acquisire **elementi conoscitivi in merito all'attività di disinformazione** ed ai suoi fini ed effetti.

Il **secondo gruppo** di compiti (co. 1, lett. da *f*) ad *m*)) è, invece, diretto a **valutare** l'**adeguatezza** degli **strumenti esistenti per contrastare** il fenomeno della disinformazione ed **eventualmente a valutare l'opportunità di proporre l'adozione di iniziative per una più adeguata prevenzione e un più efficace contrasto.**

La diffusione massiva di informazioni false e l'attività di disinformazione (articolo 2, co. 1, lett. da a) ad e))

Nell'ambito del primo gruppo, alla Commissione **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, - ossia, sulle "attività di disinformazione" - anche mediante 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 utilizzano i dati degli utenti, nonché sulle condizioni nelle quali sono realizzate le suddette attività ***(lett. a)).***

Al riguardo, si ricorda che, 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**".
Come autorevolmente sostenuto in dottrina, l'attività di disinformazione si collega al concetto, tipico del 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, 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.
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'art. 2 della **L. 69/1963**, 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 artt. 51-55 della medesima L. 69/1963). 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'art. 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 può 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**, **o organizzazioni**, anche aventi struttura internazionale, che si avvalgano anche del sostegno finanziario di soggetti interni o esteri con lo scopo di manipolare l'informazione e di condizionare l'opinione pubblica, in modo particolare in occasione di **consultazioni elettorali** o referendarie ***(lett. b)***.

Al riguardo, si ricorda che 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'UE nel più ampio ambito dell'azione di difesa dalle minacce ibride. Infatti, 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.

Un terzo compito affidato alla Commissione 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 ***(lett. e)***.

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, producono e diffondono notizie false o tendenziose senza i limiti propri degli esseri umani (ad esempio, possono essere create centinaia di migliaia di notizie in tempi molto contenuti), senza poter essere immediatamente riconoscibili come programmi informatici dagli esseri umani e sfruttando proprio la nostra natura (le nostre opinioni, i nostri pregiudizi) per veicolare direttamente contenuti mirati alle persone "giuste" nel momento "più opportuno" per il committente.
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 (si tratta dei 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% nell'ambito del programma di ricerca e innovazione Orizzonte 2020. Raggiungerà 1,5 miliardi di euro per il periodo 2018-2020. Il 10 aprile 2018, 25 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 MISE nel 2019. 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.

Oltre alle descritte tematiche di carattere generale, alla Commissione sono attribuiti anche i seguenti compiti:

- verificare eventuali attività di **disinformazione** compiute nel corso dell'emergenza derivante dalla diffusione del **COVID-19**, gli effetti che ne sono conseguiti sulla gestione dell'emergenza e le misure adottate per prevenirle e contrastarle **(lett. *c*)**);
- verificare se **l'attività di disinformazione abbia finalità di odio**, ossia di istigazione alla discriminazione o alla violenza per motivi razziali, etnici, nazionali, religiosi o di **istigazione a delinquere** alla commissione di atti discriminatori e violenti per motivi sessuali o di orientamento sessuale **(lett. *d*))**.

L'esame dell'adeguatezza degli strumenti esistenti per contrastare il fenomeno della disinformazione (articolo 2, co. 1, lett. da f) a m))

Con riferimento al **settore pubblico**, alla Commissione è affidato il compito di verificare **lo stato di attuazione** della **normativa vigente** e le attività previste dalla medesima normativa in materia di **prevenzione** delle attività di disinformazione e, in particolare, di verificare se l'ordinamento vigente preveda **procedure adeguate** e destini **proporzionate risorse, anche finanziarie,** alle autorità e alle pubbliche amministrazioni competenti ***(lett. f))*.**

Con riferimento al **settore privato,** la Commissione deve verificare, anzitutto, 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, nonché delle 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 (**lett. *g*)).**
Inoltre, deve verificare, anche sulla base della **comparazione** con le esperienze di altri **Stati europei**, ferme restando le prerogative e le competenze dell'Ordine dei giornalisti, la possibilità dell'adozione di un

codice di autoregolamentazione da parte degli stessi soggetti, 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 (**lett. *h***)).

Per le competenze e le prerogative dell'Ordine dei giornalisti si richiamano la specifica L. 69/1963 – per la quale si veda *ante* – nonché il DPR 137/2012, ovvero il regolamento di delegificazione in materia di **professioni regolamentate**, volto a dare attuazione ai principi dettati dall'art. 3, co. 5, del D.L. 138/2011 (L. 148/2011), che 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.
Con riferimento a quanto previsto dalla lett. *h*), occorre ricordare, 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**.
Il codice è stato adottato nell'ottobre del 2018 dalle principali piattaforme *online* (tra le quali Facebook, Google, e Twitter), dalle società di *software* (in particolare, nel maggio del 2019, ha aderito al codice la Microsoft), e dalle organizzazioni che rappresentano il settore della **pubblicità**.

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

Al riguardo, si ricorda, preliminarmente, che, secondo la definizione delle **otto competenze-chiave** per l'**apprendimento permanente individuate** dalla Raccomandazione del Parlamento europeo e del Consiglio del 18 dicembre 2006 (2006/962/CE) – ossia, delle competenze di cui tutti hanno bisogno per la realizzazione e lo sviluppo personali, la cittadinanza attiva, l'inclusione sociale e l'occupazione –, la **competenza digitale** consisteva nel "saper utilizzare con dimestichezza e **spirito critico** le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC *(tecnologie dell'informazione e della comunicazione)*: l'uso del computer per reperire, **valutare**, conservare, produrre, presentare e scambiare **informazioni** nonché per comunicare e partecipare a reti collaborative tramite Internet". In base alla definizione, la competenza digitale presupponeva una consapevolezza delle **opportunità** e dei **potenziali rischi** di Internet e della comunicazione tramite i supporti elettronici. Si evidenziava, infatti, che "Le persone dovrebbero anche […] rendersi conto delle problematiche legate alla validità e all'**affidabilità delle informazioni** disponibili e dei principi giuridici ed etici che si pongono nell'uso interattivo delle TSI".
Successivamente, la Raccomandazione del Consiglio del 22 maggio 2018 (2018/C 189/01) – che ha sostituito la Raccomandazione 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, da ultimo, 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 **L. 107/2015** 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, lett. *d)* ed *h)*, e 56).

Il **Piano nazionale scuola digitale** (PNSD) è stato adottato con DM 27 ottobre 2015, n. 851, e ha previsto vari ambiti di intervento, fra cui quello relativo alle competenze degli studenti, proponendo le relative Azioni.
In generale, ha evidenziato che la sempre maggiore articolazione e complessità di contenuti digitali richiede competenze adeguate – fra le quali quelle logiche, argomentative e interpretative –, sottolineando che **gli studenti devono trasformarsi da consumatori in "consumatori critici"** e "produttori" di contenuti e architetture digitali, in grado, fra l'altro, di acquisire autonomia di giudizio, pensiero creativo, consapevolezza delle proprie capacità.
In particolare, nell'ambito dell'**Azione n. 15** – Scenari innovativi per lo sviluppo di competenze digitali applicate – il Piano ha previsto che, secondo le modalità più adatte all'ordine e al grado della scuola, tutti gli studenti italiani devono affrontare i temi relativi ai diritti della rete, a partire dalla Dichiarazione per i Diritti in Internet redatta dalla Commissione per i diritti e i doveri relativi ad Internet della Camera dei Deputati nella XVII legislatura, all'educazione ai media e alle dinamiche sociali online, alla qualità, integrità e circolazione dell'informazione (attendibilità delle fonti, diritti e doveri nella circolazione delle opere creative, privacy e protezione dei dati, information literacy).
Da ultimo, l'art. 5 della **L. 92/2019**, 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'a.s. 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 PNSD 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**.
Infine, 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.

Infine, la Commissione deve valutare l'**opportunità di proporre:**

- l'adozione di **iniziative di carattere normativo o amministrativo** volte a realizzare una più adeguata **prevenzione** e un più efficace **contrasto** dell'attività di disinformazione e della commissione di reati attraverso i media, le reti sociali telematiche e le altre piattaforme analogiche e digitali (**lett. *l***)).

- l'adozione di **iniziative di carattere normativo o amministrativo** volte a contrastare l'attività di disinformazione che produce **effetti negativi sulla crescita e lo sviluppo delle conoscenze dei minori** che ricorrono all'utilizzo dei media tradizionali, delle reti sociali telematiche e delle altre piattaforme tecnologiche analogiche o digitali (**lett. *m***)).

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.

In particolare, 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 ottiene 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, posto che ciascun componente della Commissione può indicare sulla propria scheda un solo nome per ciascuna delle due cariche. Sono eletti coloro che hanno 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 vedono 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 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 (L. 124/2007) e, in sede processuale, dagli artt. 202 e segg. c.p.p. Quest'ultimo, in particolare, prevede tra l'altro che i pubblici ufficiali, i pubblici impiegati e gli incaricati di un pubblico servizio hanno 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 possono 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 collabora con la Commissione o compie o concorre a compiere atti di inchiesta oppure ne viene a conoscenza per ragioni di ufficio o di servizio. Tali persone sono obbligate al segreto per tutto quanto

riguarda gli atti e i documenti trasmessi in copia relativi a procedimenti e inchieste in corso presso l'autorità giudiziaria o altri organi inquirenti che siano coperti da segreto e per quanto riguarda gli atti e i documenti per i quali la Commissione ha 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.

Discussione e attività istruttoria in Commissione in sede referente

Le Commissioni VII e IX hanno avviato l'esame dell'A.C. 1056 il 17 luglio 2019. Successivamente, sono state abbinate le altre 3 proposte di legge ed è stato costituito un Comitato ristretto, che ha proceduto, prima, ad audire numerosi soggetti e, successivamente, ad elaborare un testo unificato.

Nella seduta del 9 luglio 2020 le Commissioni VII e IX hanno adottato il testo unificato elaborato dal Comitato ristretto quale testo base.

Nelle sedute del 14 e del 15 luglio 2020 le Commissioni hanno approvato alcune modifiche al testo che è stato, dunque, inviato alle Commissioni competenti in sede consultiva.

A seguito del parere della II Commissione, nella seduta del 16 luglio 2020 il testo è stato ulteriormente modificato. Nella stessa seduta, le Commissioni hanno conferito mandato alle relatrici a riferire favorevolmente in Assemblea sul testo come modificato.

Di seguito, il quadro dei soggetti auditi, corredato di link ai documenti in molti casi depositati:

Data	Ente	Link web-tv	Memorie
2020.03.03	Autorità garante della concorrenza e del mercato	https://webtv.camera.it/evento/16039	memoria
2020.03.03	Garante per la protezione dei dati personali		NO
2020.03.03	Consiglio nazionale Ordine dei giornalisti		memoria
2020.03.03	Associazione italiana editori (AIE)		memoria
2020.03.03	Federazione italiana editori di giornali (FIEG)		NO
2020.03.03	Coordinamento nazionale dei presidenti del Comitato regionale per le comunicazioni (CORECOM)		memoria
2020.03.05	Associazione italiana per l'educazione ai media e alla comunicazione (MED)	https://webtv.camera.it/evento/16071	memoria
	Confindustria radio televisioni *		memoria
2020.03.05	Google Italy Srl		memoria
2020.03.05	RAI – Radiotelevisione italiana Spa		memoria
2020.06.09	Presidente dell'Autorità per le garanzie nelle comunicazioni (AGCOM)	https://webtv.camera.it/evento/16309	memoria
2020.06.09	Rappresentanti del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri	Il Dis non ha dato autorizzazione alla trasmissione dell'audizione sulla *web-tv*	NO
2020.06.16	Federazione Nazionale Stampa Italiana (FNSI)	https://webtv.camera.it/evento/16352	NO
2020.06.16	Facebook Italy Srl		memoria

***Confindustria, impossibilitata a partecipare, ha inviato una memoria il 5.03.2020**

I pareri espressi dalle Commissioni in sede consultiva

Il 16 luglio 2020 la I Commissione ha espresso parere favorevole
Nella stessa data, la II Commissione ha espresso parere favorevole con osservazione.
La V Commissione esprimerà il parere di competenza direttamente all'Assemblea.

CU0083a	Servizio Studi Dipartimento Cultura	st_cultura@camera.it - 066760-3255	CD_cultura
	Servizio Studi Dipartimento Trasporti	st_trasporti@camera.it - 066760-2614	CD_trasporti