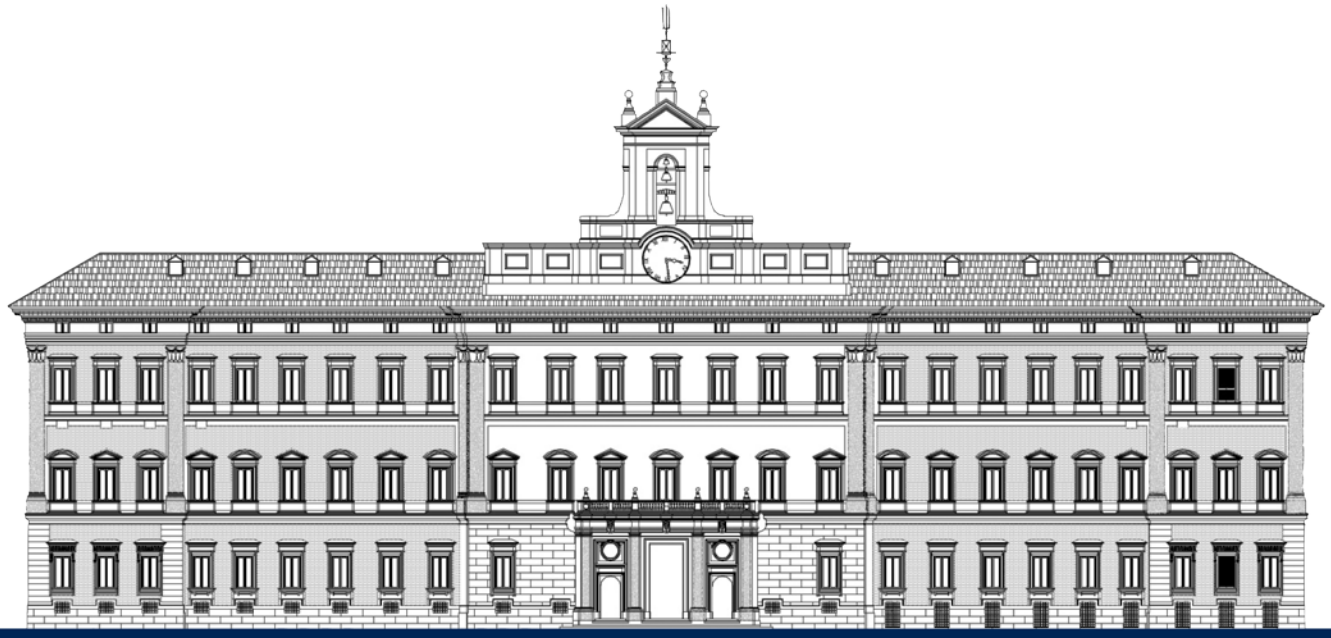
Camera dei deputati

XVIII LEGISLATURA

Documentazione per l'esame di

Progetti di legge



Istituzione di una Commissione parlamentare di inchiesta sulla diffusione intenzionale e massiva di informazioni false attraverso la rete internet e sul diritto all'informazione e alla libera formazione dell'opinione pubblica

A.C. 1056

Schede di lettura

n. 182

Camera dei deputati

XVIII LEGISLATURA

Documentazione per l'esame di

Progetti di legge

Istituzione di una Commissione parlamentare di inchiesta sulla diffusione intenzionale e massiva di informazioni false attraverso la rete internet e sul diritto all'informazione e alla libera formazione dell'opinione pubblica

A.C. 1056

Schede di lettura

n. 182

16 luglio 2019

Servizio responsabile:

SERVIZIO STUDI – Dipartimenti Cultura e Trasporti

☎ 066760-3255 – ✉ st_cultura@camera.it –

☎ 066760-2614 – ✉ st_trasporti@camera.it -

Hanno partecipato alla redazione del *dossier*:

SERVIZIO STUDI – DIPARTIMENTI:

Istituzioni - Giustizia

☎ 066760-9475 – ✉ st_istituzioni@camera.it

☎ 066760-9148 – ✉ st_giustizia@camera.it

SERVIZIO BIBLIOTECA – Osservatorio della legislazione straniera

☎ 066760-2278 – ✉ *bib_segreteria@camera.it*

SERVIZIO RAPPORTI INTERNAZIONALI

☎ 066760-3948 – ✉ cdrin1@camera.it

SEGRETERIA GENERALE – Ufficio Rapporti con l'Unione europea

☎ 066760-2145 – ✉ *cdrue@camera.it*

La documentazione dei servizi e degli uffici della Camera è destinata alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. La Camera dei deputati 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.

***File**: CU0083.docx*

I N D I C E

SCHEDE DI LETTURA

- Articolo 1 *(Istituzione e funzioni della Commissione parlamentare di inchiesta)* 3
- Articoli 2-8 *(Poteri, organizzazione e funzionamento della Commissione parlamentare di inchiesta)* 5

MATERIALI DI APPROFONDIMENTO

- *Le competenze digitali per un uso consapevole di internet* 13
- *L'obbligo del rispetto della verità da parte dei giornalisti* 17
- *La fase della campagna elettorale: indirizzi espressi per la correttezza delle informazioni e la garanzia del pluralismo nelle piattaforme digitali* 19
- *La responsabilità dei provider in Internet e il controllo delle notizie false nella rete: regolazione e autoregolazione* 22
- *Gli strumenti penali di repressione delle fake news* 26
- *Gli strumenti penali di repressione del c.d. hate speech* 29
- Iniziative dell'Unione europea per il contrasto alla disinformazione *(a cura dell'Ufficio Rapporti con l'Unione europea)* 33
- Le iniziative assunte nei principali paesi europei per fronteggiare il fenomeno delle notizie false sul web *(a cura del Servizio Biblioteca)* 37
- Gli atti del Consiglio d'Europa per contrastare la diffusione dei discorsi d'odio e delle fake news *(a cura del Servizio Rapporti Internazionali)* 55
- Contrasto alle fake news e "guerra ibrida" nelle attività dell'Assemblea parlamentare della NATO *(a cura del Servizio Rapporti Internazionali)* 63

Schede di lettura

Articolo 1
(Istituzione e funzioni della Commissione parlamentare di inchiesta)

L'**articolo 1** istituisce la Commissione parlamentare di inchiesta sulla **diffusione intenzionale e massiva di informazioni false** attraverso la rete **internet** e sul **diritto all'informazione** e alla libera formazione dell'opinione pubblica, e ne stabilisce i **compiti**.

Alla Commissione è affidato, innanzitutto, il compito di **indagare sulla «disinformazione *on line*»**, ovvero sulla diffusione intenzionale e massiva di informazioni false o fuorvianti attraverso la rete internet, anche mediante la creazione di **false identità digitali**. Più nello specifico, la Commissione deve **verificare**:

- se la disinformazione on line può essere imputata a, o sostenuta, anche finanziariamente, da **gruppi organizzati o Stati esteri** che se ne servono allo scopo di manipolare l'informazione e condizionare l'opinione pubblica, anche in occasione delle **consultazioni elettorali e referendarie**;
- se esistono correlazioni tra la disinformazione on line e i cosiddetti «discorsi dell'odio o ***hate speech***», ossia di incitamento alla discriminazione o alla violenza per **motivi razziali, etnici, nazionali o religiosi**, e se e in quali casi la disinformazione on line può aver destato **allarme presso la popolazione**.

Inoltre, la Commissione ha il compito di **accertare la congruità** della **normativa** vigente in materia. In particolare, alla Commissione è affidato l'incarico di **indicare** le **iniziative di carattere normativo o amministrativo** ritenute necessarie a:

- assicurare un'**esatta definizione** delle informazioni false, anche in conformità con quanto stabilito dall'Unione europea, al fine di identificarle con chiarezza e di limitarne la circolazione, di favorire la **trasparenza** e la **differenziazione** delle **fonti** di informazione e delle **procedure per la gestione dei reclami** formulati dagli utenti su contenuti illegali, garantendo risposte celeri;
- promuovere sistemi di **monitoraggio e** di **contrasto** della diffusione delle informazioni false, in particolare nei periodi di **campagna elettorale e referendaria**.

Alla Commissione sono affidati, altresì, ulteriori compiti nell'ambito specifico delle **piattaforme *on line***. In particolare, essa deve:

- valutare l'**adeguatezza** delle misure introdotte dalle medesime piattaforme per **prevenire la disinformazione *on line***, indicando le eventuali iniziative di carattere normativo o amministrativo ritenute necessarie;
- valutare, anche sulla base delle esperienze di altri Paesi, la possibilità di prevedere che le medesime piattaforme adottino un **codice di autoregolazione** al fine di rimuovere la disinformazione on line e di **vietare** eventuali **vantaggi pubblicitari** legati alla diffusione massiva di informazioni false.

Infine, la Commissione può prevedere iniziative per **favorire** l'adozione condivisa e il consolidamento di **buone pratiche** per contrastare la disinformazione online e i discorsi dell'odio.

Per la previsione di tali iniziative – alle quali possono prendere parte tutti gli enti istituzionali e i soggetti pubblici o privati interessati – possono essere invitati a collaborare i soggetti operanti nei mercati dell'informazione *on line* e, in particolare, le piattaforme che offrono servizi di *social network* e motori di ricerca.

Articoli 2-8
(Poteri, organizzazione e funzionamento della Commissione parlamentare di inchiesta)

Gli **articoli da 2 a 7** disciplinano **i poteri, l'organizzazione e il funzionamento** della Commissione parlamentare di inchiesta, indicandone **vincoli e poteri**. L'**articolo 8** disciplina **l'entrata in vigore**.

Con riferimento alla **durata della Commissione**, l'**articolo 2** stabilisce che la Commissione conclude i propri lavori **entro ventiquattro mesi dalla sua costituzione** e presenta alle Camere **una relazione finale sui risultati delle sue indagini**. Sono ammesse relazioni di minoranza.

La Commissione può anche presentare relazioni intermedie ogni volta che lo ritenga opportuno.

La Commissione riferisce alle Camere **al termine dei suoi lavori**, nonché ogni volta che lo ritenga opportuno **e comunque al termine del primo anno di attività.**

L'**articolo 3** disciplina la **composizione della Commissione**. Si tratta di una **Commissione bicamerale composta da 40 membri,** venti senatori e venti deputati (comma 1), scelti rispettivamente dal Presidente del Senato della Repubblica e dal Presidente della Camera dei deputati in proporzione al numero dei componenti i gruppi parlamentari, assicurando comunque la presenza di un rappresentante per ciascun gruppo esistente in almeno un ramo del Parlamento.

Entro dieci giorni dalla nomina dei suoi componenti, il Presidente del Senato della Repubblica e il Presidente della Camera dei deputati, d'intesa tra loro, **convocano la Commissione per la costituzione dell'ufficio di presidenza**, composto dal presidente, da due vicepresidenti e da due segretari, ed eletto a scrutinio segreto (comma 2).

Il presidente è **eletto tra i componenti appartenenti ai gruppi di opposizione** con **la maggioranza assoluta dei componenti la Commissione**. Se nessuno riporta tale maggioranza, si procede al ballottaggio tra i due candidati che hanno ottenuto il maggior numero di voti e risulta 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, ciascun componente della Commissione scrive sulla propria scheda un solo nome. Sono eletti coloro che hanno ottenuto il maggior numero di voti. In caso di parità di voti si procede al ballottaggio tra i due candidati che hanno ottenuto il maggior numero di voti e, in caso di parità di voti, risulta eletto il più anziano di età (comma 4).

Tali norme si applicano anche per le elezioni suppletive (comma 5).

Come previsto dall'articolo 82 della Costituzione, che disciplina le inchieste parlamentari, l'**articolo 4** stabilisce che 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).

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 lire centomila a lire un milione 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 3).

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 a norma del comma 1, 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.

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

4). 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 5). 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 6).

L'**articolo 5** disciplina le **audizioni a testimonianza** innanzi alla Commissione.

Si prevede in particolare che, ferme restando le competenze dell'autorità giudiziaria, per le audizioni a testimonianza davanti alla Commissione 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 testimonio 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 si richiama la normativa prevista dalla legge 3 agosto 2007, n. 124.

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. 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.).

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), mentre è sempre opponibile il segreto tra difensore e parte processuale nell'ambito del mandato (comma 3).

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 legge 107/2017 di istituzione della Commissione di inchiesta sul sistema bancario e finanziario (art. 4) nonché, da ultimo, la legge n.99 del 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 che 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 6** 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**. È 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 tali fattispecie 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 7** 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).

Tutte le volte che lo ritenga opportuno, la **Commissione può deliberare di riunirsi in seduta segreta** (comma 2).

Inoltre, la Commissione, per l'adempimento delle sue funzioni, può **avvalersi 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, nonché 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 collaborazioni** di cui può avvalersi la Commissione (comma 3).

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 4).

Per quanto riguarda le **spese per il funzionamento** della Commissione, 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 e sono stabilite nella **misura massima di 300.000 euro** (comma 5).

Alla Commissione spetta infine la cura dell'informatizzazione dei documenti acquisiti e prodotti nel corso della sua attività (comma 6).

Ai sensi dell'**articolo 8** la legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

Materiali di approfondimento

Le competenze digitali per un uso consapevole di internet

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[1]: 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**

[1] Tecnologie dell'informazione e della comunicazione.

necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo".

Con particolare riguardo alla materia "**Tecnologia**", le Indicazioni nazionali sottolineano come "è specifico compito della tecnologia quello di promuovere nei bambini e nei ragazzi forme di pensiero e atteggiamenti che preparino e sostengano interventi trasformativi dell'ambiente circostante attraverso un **uso consapevole e intelligente delle risorse**". Con specifico riferimento alle tecnologie dell'informazione e della comunicazione e alle tecnologie digitali, 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"[2]– che propone alle scuole una rilettura delle Indicazioni nazionali emanate nel 2012 attraverso la lente delle competenze di cittadinanza[3] – 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).

---

[2] Il documento – frutto del lavoro del Comitato scientifico per le Indicazioni nazionali della scuola dell'Infanzia e del primo ciclo di istruzione – è stato presentato al MIUR il 22 febbraio 2018.

[3] Nel comunicato stampa del MIUR del 22 febbraio 2018 si legge «Il documento presentato oggi non è una integrazione né una riscrittura delle Indicazioni nazionali. Non si tratta, si legge nel testo illustrato al MIUR, "di 'aggiungere' nuovi insegnamenti, ma di ricalibrare quelli esistenti", rileggendo le Indicazioni del 2012, alla luce dei nuovi spunti offerti che guideranno le scuole nella predisposizione della loro offerta formativa, della loro progettazione. Il tema della cittadinanza viene affrontato come il "vero sfondo integratore e punto di riferimento di tutte le discipline che concorrono a definire il curricolo della scuola dell'infanzia e del primo ciclo di istruzione in una prospettiva verticale"».

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 dell'A.S. 1264, già approvato dalla Camera, recante "Introduzione dell'insegnamento scolastico dell'educazione civica", prevede l'inserimento dell'**educazione alla cittadinanza digitale** nell'ambito dell'insegnamento trasversale dell'educazione civica. 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, si prevede che il Ministro dell'istruzione, dell'università e della ricerca convoca almeno ogni due anni la **Consulta dei diritti e dei doveri del bambino e dell'adolescente digitale**[4], di cui il testo prevede l'istituzione presso il Ministero dell'istruzione, dell'università e della ricerca.

[4] I criteri di composizione e le modalità di funzionamento della Consulta sono definite con decreto del Ministro dell'istruzione, dell'università e della ricerca, in modo da assicurare la rappresentanza degli studenti, degli insegnanti, delle famiglie e degli esperti del settore. L'Autorità garante per l'infanzia e l'adolescenza designa un componente della Consulta.

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.

Il progetto Generazioni connesse - la cui terza edizione (SIC III), avviata il 1° luglio 2016, è cofinanziata dalla Commissione Europea nell'ambito del programma "Connecting Europe Facility" (CEF), attraverso il quale la Commissione promuove strategie finalizzate a rendere Internet un luogo più sicuro per gli utenti più giovani, promuovendone un **uso positivo e consapevole** - è coordinato dal Ministero dell'istruzione, dell'università e della ricerca, in partenariato, tra gli altri, con il Ministero dell'Interno-Polizia Postale e delle Comunicazioni, l'Autorità Garante per l'infanzia e l'adolescenza, Save the Children Italia, Telefono Azzurro, Università degli Studi di Firenze, Università degli studi di Roma "La Sapienza".

Tra le azioni previste dal progetto vi sono:

- una campagna di comunicazione e sensibilizzazione ad ampio raggio, attraverso l'utilizzo di canali media tradizionali, media online e social media, realizzata da tutti i partner del progetto e dall'Advisory Board;
- attività di formazione (online e in presenza) rivolte in maniera specifica alle comunità scolastiche (insegnanti, educatori, studenti, genitori). I soggetti coinvolti possono inoltre usufruire di strumenti e risorse didattiche disponibili nella piattaforma online del progetto;
- il coinvolgimento diretto dei giovani nella creazione di piccole redazioni giornalistiche, per raccontare il mondo del web dal loro punto di vista. Questi ragazzi costituiscono lo Youth Panel del Safer Internet Centre.

Il Safer Internet Day (SID) è un evento organizzato a livello internazionale con il supporto della Commissione Europea nel mese di febbraio. La ricorrenza annuale è stata istituita nel 2004 al fine di promuovere un uso più sicuro e responsabile del web e delle nuove tecnologie, in particolare tra i bambini e i giovani di tutto il mondo.

La XVI edizione del Safer internet day si è svolta il 5 febbraio 2019 con il motto "**Together for a better internet**" ed è stata finalizzata a far riflettere i ragazzi non solo sull'uso consapevole della rete, ma sul ruolo attivo e responsabile di ciascuno nella realizzazione di internet come luogo positivo e sicuro.

Inoltre, il 6 febbraio 2018 è stato sottoscritto un protocollo di intesa fra il 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**. Per l'attuazione e il monitoraggio degli impegni assunti dalle parti, il Protocollo ha previsto l'istituzione di un comitato paritetico coordinato da un rappresentante del MIUR e composto da tre rappresentanti del Ministero e tre dell'AGCOM.

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.

L'obbligo del rispetto della verità da parte dei giornalisti

L'**art. 21**, commi primo e secondo, della **Costituzione** dispone che "Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione. La stampa non può essere soggetta ad autorizzazioni o censure".

Tale principio è ribadito nell'**art. 2** della **L. 69/1963**, recante ordinamento della professione di giornalista, che, in particolare, 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) 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.

In particolare, 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.

I medesimi principi, inoltre, sono variamente declinati anche con riguardo a specifici ambiti. In particolare, il giornalista:

- **evita**, nella pubblicazione di notizie su argomenti scientifici, un **sensazionalismo** che potrebbe far sorgere timori o speranze infondate, e diffonde **notizie sanitarie solo se verificate** con autorevoli fonti scientifiche (art. 6);
- nei confronti delle **persone straniere evita la diffusione di informazioni imprecise**, sommarie o distorte riguardo a richiedenti asilo, rifugiati, vittime della tratta e migranti (art. 7);
- nell'ambito della **cronaca giudiziaria**, nelle trasmissioni televisive, rispetta il principio del contraddittorio delle tesi, assicurando la presenza e la pari opportunità nel confronto dialettico tra i soggetti che le sostengono, garantendo il principio di buona fede e della **corretta ricostruzione degli avvenimenti** (art. 8).

Infine, in tema di pubblicità, l'art. 10 stabilisce, in particolare, che il giornalista assicura ai cittadini il diritto di ricevere un'**informazione corretta**, **sempre distinta dal messaggio pubblicitario** attraverso chiare indicazioni.

La fase della campagna elettorale: indirizzi espressi per la correttezza delle informazioni e la garanzia del pluralismo nelle piattaforme digitali

A partire dalle elezioni politiche del 4 marzo 2018, l'Autorità garante per le comunicazioni (AGCOM) ha 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 *stakeholder* 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 è possibile, che l'inserzionista indichi la natura di "messaggio elettorale" di questi, 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. 28/2000.

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.

Al contempo, in occasione del discorso sullo stato dell'Unione 2018, pronunciato il 12 settembre 2018 al Parlamento europeo dall'allora Presidente della Commissione europea, erano state annunciato una serie di iniziative volte a garantire che le elezioni del Parlamento europeo del 2019 si svolgessero in modo libero, regolare e sicuro (si veda in proposito la comunicazione COM(2018) 637 della Commissione europea del 12 settembre 2018).

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.

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 pf practice on disinformation.

Sempre in vista delle elezioni europee 2019 il Consiglio europeo – nelle conclusioni del 21 e 22 marzo 2019 – aveva chiesto maggiori sforzi coordinati per affrontare gli aspetti interni ed esterni della disinformazione e proteggere le elezioni europee e nazionali in tutta l'UE.

Si veda in proposito anche il paragrafo *Iniziative dell'Unione europea per il contrasto alla disinformazione*.

La responsabilità dei provider 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 natura stessa della 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 alcun tipo di filtro e senza che chi veicoli l'informazione stessa sia un professionista, e quindi vincolato ai principi deontologici della professione e ai controlli sul rispetto degli stessi.

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

Peraltro l'apparente anarchia e "orizzontalità" della rete non nasconde tuttavia 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 Provider recepita in Italia dal decreto legislativo n. 70 del 2003.

Pur con vari temperamenti è infatti fermo il principio secondo il quale gli ISP **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).

Gli Internet Service Provider, 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 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 (si veda la scheda "**Iniziative dell'UE per il contrasto alla disinformazione**) la diffusione di **iniziative di regolazione consensuale**.

L'attività delle Autorità indipendenti

Con riferimento al **controllo delle notizie false l'Autorità per le Garanzie nelle Comunicazioni (AGCOM**), 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**. 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.*

Di particolare interesse tra tali indagini il rapporto **News vs. fake nel sistema dell'informazione** - Interim report di cui all'indagine conoscitiva delibera n. 309/16/CONS su "Piattaforme digitali e sistema dell'informazione".

Nell'ambito del Tavolo sono stati costituiti diversi gruppi di lavoro in particolare: 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.

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 *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[5]; 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 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

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

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 "Mancino" 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.

E' 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"**[6] 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.

[6] 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.

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;
- 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.

Iniziative dell'Unione europea per il contrasto alla disinformazione
(a cura dell'Ufficio Rapporti con l'Unione europea)

Dal 2015 l'UE è sistematicamente impegnata in una serie di iniziative volte a proteggere le istituzioni e i processi democratici dall'attività di disinformazione.

A tale attività - secondo la definizione adottata dalla Commissione europea[7] - deve essere ricondotta "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"**.

Data la sensibilità del tema, con particolare riguardo alla questione della protezione delle **elezioni europee**, il contrasto alla disinformazione è stato oggetto di conclusioni da parte dei Consigli europei del 13 -14 dicembre 2018, del 22 marzo e 20-21 giugno 2019.

In particolare, nella riunione del 20-21 giugno 2019, il Consiglio europeo ha chiesto un impegno costante per sensibilizzare sul tema della disinformazione e rafforzare la preparazione e la resilienza delle nostre democrazie di fronte a tale fenomeno; il Consiglio europeo ha, altresì, sottolineato la necessità di una **valutazione costante** e di una **risposta adeguata** nei confronti della continua evoluzione delle minacce e del crescente rischio di interferenze dolose e manipolazioni *online*, associati allo sviluppo dell'**intelligenza artificiale** e di **tecniche di raccolta dati**.

Task force East StratCom

Tra le prime iniziative dell'UE in materia di disinformazione, le misure nell'ambito della **azione esterna** volte a contrastare la diffusione di informazioni fuorvianti o palesemente false da parte di **enti** e **organismi** situati in **Stati terzi**.

Le misure in tale settore sono spesso ricondotte dall'UE nel più ampio ambito dell'azione di difesa dalle **minacce ibride**. Secondo la Commissione europea, le campagne massicce di disinformazione, che usano i media sociali per controllare il

[7] Comunicazione congiunta "Relazione sull'attuazione del piano di azione contro la disinformazione (COM (2019) 12).

discorso politico o per radicalizzare, reclutare e dirigere mandatari, possono essere vettori di minacce ibride[8].

In particolare, a seguito della decisione del Consiglio europeo del marzo 2015 di contrastare le **campagne** di **disinformazione** da parte della **Russia**, il Servizio europeo per l'azione esterna (SEAE) ha istituito la ***task force* East StratCom,** con il compito di sviluppare prodotti e campagne di comunicazione incentrate sulla spiegazione delle politiche dell'UE nella regione del partenariato orientale (Armenia, Azerbaijan, Bielorussia, Georgia, Moldavia e Ucraina).

La *task force* si concentra sui seguenti obiettivi: comunicare efficacemente le politiche dell'UE al suo **vicinato orientale**; rafforzare l'ambiente mediatico generale nel vicinato orientale, anche sostenendo la **libertà** dei **mezzi di informazione** e consolidando i **media indipendenti**; migliorare le capacità dell'Unione di prevedere e affrontare le attività di disinformazione a favore del Cremlino e di **sensibilizzare** il pubblico in proposito. Sono state istituite altre due altre *task force* incentrate su aree geografiche diverse: la *task force* StratCom per i Balcani occidentali e la *task force* South Med Stratcom per il mondo di lingua araba.

Approccio europeo per il contrasto alla disinformazione

Nell'aprile del 2018 la Commissione europea ha presentato la comunicazione COM(2018) 236 "Contrastare la disinformazione *online*: un approccio europeo" recante i principi e gli obiettivi generali che dovrebbero guidare le azioni volte a sensibilizzare l'opinione pubblica alla disinformazione e a contrastare efficacemente tale fenomeno, nonché una serie di iniziative considerate prioritarie. Tra le misure chiave indicate dalla Commissione europea, 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**.

---

[8] Comunicazione "Quadro congiunto per contrastare le minacce ibride" del 6 aprile 2016. 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.

Il codice prevede una serie di impegni, che comprendono, tra l'altro: **vaglio delle inserzioni pubblicitarie** per ridurre gli introiti pubblicitari di coloro che diffondono disinformazione; garanzia della **trasparenza** dei **messaggi pubblicitari** di natura politica; contrasto all'abuso delle piattaforme da parte di **profili falsi** e di "**bot" automatizzati**; maggiore collaborazione con i **verificatori di fatti**; miglioramento della **visibilità** dei **contenuti** sottoposti a **verifica dei fatti**; predisposizione di **strumenti** messi a disposizione degli **utenti** per individuare meglio la disinformazione.

Nel giugno del 2019, la Commissione europea ha manifestato l'intenzione di procedere ad una valutazione dell'efficacia del codice entro la fine del 2019, preannunciando peraltro ulteriori iniziative, anche di **natura regolamentare**, qualora i risultati di tale valutazione non fossero soddisfacenti.

Il pacchetto elezioni

In occasione del discorso sullo Stato dell'Unione del settembre 2018, la Commissione europea ha presentato una serie di iniziative per garantire **elezioni libere ed eque** (in vista della tornata elettorale del maggio del 2018) tra l'altro, anche in materia di contrasto alla disinformazione.

Si tratta, in particolare, di: una comunicazione della Commissione europea "Assicurare elezioni europee libere e corrette (COM(2018)637); una raccomandazione (C(2018)5949) relativa alle reti di cooperazione in materia elettorale, alla trasparenza *online*, alla protezione dagli incidenti di cibersicurezza e alla lotta contro le campagne di disinformazione; orientamenti della Commissione sull'applicazione del diritto dell'Unione in materia di **protezione dei dati** nel contesto elettorale; una serie di modifiche (entrate in vigore nel marzo del 2019) al regolamento relativo al **finanziamento dei partiti politici europei**, che introducono in particolare **sanzioni finanziarie** ai partiti politici europei e alle fondazioni politiche europee che **influenzano** deliberatamente, o tentano di influenzare, i **risultati** delle **elezioni** del PE approfittando di **violazioni** delle norme in materia di **protezione dei dati**.

Piano d'azione contro la disinformazione

Presentato dalla Commissione europea e dall'Alto rappresentante dell'unione per gli affari esteri e la politica di sicurezza nel dicembre del 2018, il Piano contiene una serie di iniziative per far fronte alle minacce provenienti dall'interno e dall'esterno dell'UE che possono riassumersi nelle seguenti linee di azione[9]:

[9] Il 14 giugno 2019, è stata pubblicata una relazione sullo stato dell'arte dell'attuazione del piano.

- capacità di **individuazione** dei casi di **disinformazione**, in particolare tramite il rafforzamento delle *task force* di comunicazione strategica e della cellula dell'UE per l'analisi delle **minacce ibride** del Servizio europeo per l'azione esterna (SEAE);
- **risposta coordinata**, dotando istituzioni UE e Stati membri di un **sistema di allarme rapido** per la condivisione e valutazione delle campagne di disinformazione;

  Istituito nel marzo del 2019, il **sistema di allarme rapido** è una piattaforma digitale volta a consentire a istituzioni dell'UE e Stati membri la migliore condivisione di approfondimenti relativi alle campagne di disinformazione e il coordinamento delle loro risposte. Il sistema si basa su informazioni *open-source*, nonché su approfondimenti dal mondo accademico, *fact-checker*, piattaforme *online* e partner internazionali.
- mobilitazione del **settore privato** nelle attività di **contrasto** (in particolare, mediante l'attuazione efficace da parte delle **piattaforme *online*** e dell'industria firmatarie degli impegni nell'ambito del **codice di buone pratiche)**;
- **campagne di sensibilizzazione** e **di responsabilizzazione** dei **cittadini,** in particolare mediante l'alfabetizzazione mediatica.

  La diffusione di notizie da parte della Commissione europea sulle iniziative dell'UE, nonché sulla disinformazione nei confronti dell'Unione, avviene regolarmente attraverso i propri **account social** (in particolare, sulle piattaforme Facebook, Twitter, Instagram e Linkedin).

  Obblighi a carico degli Stati membri circa il rafforzamento delle misure di **alfabetizzazione mediatica** sono in linea con le previsioni della recente direttiva UE n. 2018/1808 sui **servizi di media audiovisivi**.

  Nell'ambito di tale settore si ricorda, infine, l'istituzione di una sezione europea della **rete internazionale di verificatori di fatti**, con il compito di approfondire le strutture che sostengono la disinformazione e dei meccanismi che ne determinano le modalità di diffusione *online*, e di scambiare le migliori pratiche per conseguire la più ampia copertura possibile di correzioni fattuali nell'UE.

Le iniziative assunte nei principali paesi europei per fronteggiare il fenomeno delle notizie false sul web

(a cura del Servizio Biblioteca)

In **Francia** la normativa volta a contrastare il cosiddetto fenomeno delle *fake news* è contenuta in una legga approvata sul finire dello scorso anno: la *Loi n. 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information*.

Il provvedimento è teso a combattere la **manipolazione delle informazioni** nell'era digitale e ad arginare la **diffusione di notizie false** durante i periodi delle **campagne elettorali**.

La legge attiva, in primo luogo, una procedura giudiziaria accelerata, tesa a far cessare la diffusione di false informazioni durante i tre mesi precedenti le elezioni nazionali e quelle per il Parlamento europeo.

In particolare, il giudice competente, quando viene adito, deve valutare entro 48 ore, in primo grado o in appello, se una falsa informazione è stata diffusa in modo intenzionale, artificiale (o "automatizzato") e massivo attraverso un servizio di comunicazione pubblico *online* e se essa può alterare il regolare svolgimento delle elezioni.

La richiesta può essere avanzata dal pubblico ministero, da un candidato, da un partito o un raggruppamento politico ovvero da qualsiasi persona che abbia un interesse ad agire. Il giudice, in caso di accoglimento della richiesta, può adottare tutte le **misure proporzionate e necessarie** a far cessare tale diffusione (*Code électoral*, art. L. 163-2, come introdotto dall'art. 1 della Legge n. 2018-1202).

Nella sua decisione del 20 dicembre 2018 il *Conseil constitutionnel* ha peraltro precisato che il giudice può far cessare la diffusione della notizia solo qualora il carattere inesatto o fuorviante della notizia sia manifesto e sia altrettanto evidente il rischio dell'alterazione della regolarità del risultato elettorale. Secondo il Consiglio la nozione di "false informazioni" dovrebbe essere intesa come riferita ad accuse imprecise o fuorvianti o a imputazioni di cui è possibile dimostrare la falsità oggettiva, al di fuori quindi di opinioni, parodie, imprecisioni parziali o semplici esagerazioni. Il Consiglio costituzionale ha, infine, chiarito che l'inesattezza o la natura fuorviante delle accuse e delle imputazioni in questione, o il rischio di un'alterazione della genuinità del voto, devono essere inequivocabili.

Tornando all'atto normativo, l'art. 8 della legge n. 2018-1202, di modifica dell'art. 42-6 della legge n. 86-1067 sulla libertà di comunicazione, consente al *Conseil supérieur de l'audiovisuel* di assumere provvedimenti contro i media "controllati da uno Stato straniero o posti sotto l'influenza di questo Stato" se questi

diffondono “deliberatamente false informazioni che possono alterare la genuinità del voto”.

In particolare il Consiglio superiore dell’audiovisivo **può ordinare la sospensione della trasmissione per via elettronica** di tale contenuti fino alla conclusione del procedimento elettorale, ad esito di una procedura che prevede la notifica ai media della contestazione e la possibilità per gli stessi di formulare delle osservazioni nel termine di 48 ore. La decisione deve in ogni caso essere motivata e notificata ai soggetti interessati, inclusi gli operatori e i distributori dei contenuti sospesi (*Loi n. 86-1067 du 30 septembre 1986 relative à la liberté de communication*, art. 33-1-1, come introdotto dall’art. 6 della Legge n. 2018-1202).

In caso di necessità il *Conseil supérieur de l'audiovisuel* indirizza agli operatori di piattaforme online una serie di **raccomandazioni** volte a contrastare in modo più efficace la diffusione di tali informazioni. Garantisce inoltre il monitoraggio dell'obbligo per gli operatori delle piattaforme online di adottare le misure previste dall'art. 11 della legge n. 2018-1202. Pubblica, infine, un rapporto periodico sulla loro applicazione ed efficacia, raccogliendo a tal fine dai suddetti operatori, alle condizioni di cui all'art. 19 della legge, tutte le informazioni necessarie (*Loi n. 86-1067 du 30 septembre 1986 relative à la liberté de communication*, art. 17-2, come introdotto dall’art. 12 della Legge n. 2018-1202).

Le piattaforme digitali (Facebook, Twitter, ecc.) sono inoltre soggette a una **serie di obblighi** con riferimento ai **periodi preelettorali**.

In particolare, ai sensi dell’art. L. 163-1 del *Code électoral* (introdotto dall’art. 1 della legge n. 2018-1202), durante i tre mesi che precedono il primo giorno del mese delle elezioni generali e fino alla data del ballottaggio, gli operatori di piattaforme online la cui attività supera una certa soglia di numero di collegamenti sul territorio francese (ai sensi dell'art. L. 111-7 del Codice del Consumo) sono tenuti, con riguardo all’interesse generale legato alle informazioni fornite ai cittadini in campagna elettorale e alla regolarità del voto:

- a fornire all'utente informazioni corrette, chiare e trasparenti sull'identità della persona fisica o sul nome della società, la sede legale e lo scopo sociale della persona giuridica, che versa una somma di denaro alla piattaforma in cambio della diffusione di contenuti informativi relativi a un dibattito di interesse generale;
- a fornire all'utente informazioni corrette, chiare e trasparenti sull'utilizzo dei suoi dati personali nel contesto della diffusione di contenuti informativi relativi a un dibattito di interesse generale;
- a pubblicizzare l'importo della remunerazione ricevuta in cambio della diffusione di tale contenuto informativo quando l'importo supera una certa soglia.

Tali informazioni devono essere riportate su un registro messo a disposizione del pubblico per via elettronica, in un formato aperto e regolarmente aggiornato durante il summenzionato periodo.

In caso di violazione delle disposizioni previste dall'art. L. 163-1 la pena prevista è pari a **1 anno di reclusione** e ad una **sanzione pecuniaria di 75 mila euro** (*Code électoral*, art. L. 112, come introdotto dall'art. 1 della legge n. 2018-1202).

L'art. 11 della legge n. 2018-1202 dispone, invece, che gli operatori di piattaforme online sono tenuti a mettere in atto misure volte a combattere la diffusione di false informazioni che possano **turbare l'ordine pubblico** o **alterare la regolarità del voto**.

Gli operatori medesimi, sempre in base all'art. 11, hanno inoltre l'obbligo di impostare **un dispositivo facilmente accessibile e visibile** che consenta ai propri utenti di segnalare tali informazioni, soprattutto quando provengono da contenuti promossi per conto di terzi.

Essi devono parimenti adottare misure complementari riguardanti in particolare:

- la trasparenza dei loro algoritmi;
- la promozione di contenuti provenienti da aziende, agenzie di stampa e servizi di comunicazione audiovisiva;
- la lotta contro i siti che propagandano diffusamente false informazioni;
- le informazioni agli utenti circa l'identità della persona fisica o giuridica che elargisce loro somme di denaro in cambio della diffusione di contenuti informativi relativi a un dibattito d'interesse generale;
- le informazioni agli utenti circa la natura, l'origine e le modalità di diffusione dei propri contenuti;
- l'educazione all'uso dei media e all'informazione.

Tali misure sono **rese pubbliche**. Ogni operatore invia ogni anno al Consiglio superiore dell'audiovisivo una dichiarazione in cui sono specificate le modalità di attuazione di tali misure.

Le piattaforme che superano un certo volume di connessioni al giorno devono avere un rappresentante legale in Francia e rendere pubbliche le statistiche relative ai loro algoritmi (Legge n. 2018-1202, art. 13 e art. 14).

Possono inoltre essere conclusi accordi di cooperazione con altri organi di stampa per la lotta contro la diffusione di false informazioni false (Legge n. 2018-1202, art. 15).

Gli artt. 16-19 della legge n. 1202 del 2018, attraverso puntuali modifiche al codice dell'educazione, mirano a rafforzare e a ribadire il valore dell'affidabilità delle informazioni propagate attraverso i media.

Nei mesi successivi all'approvazione delle due leggi sono stati emanati due decreti.

In ordine di tempo, il primo decreto (*Décret n. 2019-53 du 30 janvier 2019 désignant le tribunal de grande instance et la cour d'appel compétents pour connaître des actions fondées sur l'article L. 163-2 du code électoral*) designa il *Tribunal de grande instance de Paris* quale giurisdizione di primo grado competente per i procedimenti basati sull'art. L. 163-2 del codice elettorale. Da tale disposizione consegue che in secondo grado è la *Cour d'appel de Paris* ad essere competente per i medesimi procedimenti.

Il secondo decreto (*Décret n. 2019-297 du 10 avril 2019 relatif aux obligations d'information des opérateurs de plateforme en ligne assurant la promotion de contenus d'information se rattachant à un débat d'intérêt général*) specifica, invece, che il numero delle connessioni al di là delle quali le piattaforme *online* devono sottostare agli obblighi di cui all'art. L. 163-1 del codice elettorale è fissato in **cinque milioni di visitatori per mese** per ciascuna piattaforma, calcolato sulla base dell'anno precedente.

Tale decreto stabilisce, inoltre, che l'obbligo di rivelare le remunerazioni ricevute come contropartita della diffusione di contenuti informativi collegati a un dibattito di interesse generale scatta qualora la remunerazione sia superiore a 100 euro netti. Le informazioni devono peraltro essere riferite a ciascun contenuto di interesse generale e il registro deve essere consultabile a partire da tutte le pagine del sito.

Lo stesso giorno in cui è stata approvata la legge n. 2018-1202 il Parlamento francese ha varato anche la relativa legge organica (*Loi organique n. 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information*), che estende le norme previste dalla legge n. 2018-1202 (la legge ordinaria) anche alle elezioni presidenziali.

In **Germania** la diffusione di notizie false e la diffamazione rappresentano fattispecie punibili ai sensi del Codice penale tedesco (*Strafgesetzbuch – StGB*)[10].

[10] Nello specifico, il § 187 StGB disciplina la **menzogna diffamatoria** (*Verleumdung*): "Chiunque, riferendosi ad un'altra persona, afferma o divulga in mala fede un fatto non vero, idoneo a denigrarla o a svalutarla di fronte all'opinione pubblica o a mettere in pericolo la sua reputazione, è punito con la pena detentiva fino a due anni o con la pena pecuniaria; se l'azione è commessa pubblicamente, in una riunione o tramite la diffusione di scritti, l'agente è punito con la pena detentiva fino a cinque anni o con la pena pecuniaria". Punibile è, altresì, il reato di **diffamazione**

Come era stato preannunciato fin dal novembre 2016 dal Ministro federale della Giustizia, il legislatore tedesco è intervenuto in maniera estremamente ferma sulla questione, approvando una legge *ad hoc* – la **Legge per il miglioramento dell'applicazione delle norme sulle reti sociali** (*Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*, *Netzwerkdurchsetzungsgesetz* - NetzDG*)* del 1° settembre 2017 - che ha introdotto in modo dettagliato **obblighi** e **sanzioni** per **siti** e ***social network*** che ospitano *fake news*.

La legge, entrata in vigore il successivo 1° ottobre[11], si applica a qualsiasi fornitore di servizi telematici (*Telemediendiensteanbieter*) che, con intento di lucro, gestisca piattaforme internet progettate per consentire agli utenti di condividere qualsiasi contenuto con altri utenti o di rendere disponibili al pubblico tali contenuti. Tale definizione (§ 1, comma 1, NetzDG) si riferisce ai c.d *social network* (*soziale Netzwerke*), ma non rientrano nel campo di applicazione della legge le piattaforme che offrono contenuti giornalistici o editoriali, la cui responsabilità è riconducibile al fornitore di servizi, nonché le piattaforme progettate per consentire la comunicazione individuale (ad esempio, le applicazioni di messaggistica) o la diffusione di contenuti specifici (come i siti di incontri).

La *Netzwerkdurchsetzungsgesetz* impone alle piattaforme sociali e mediali con più di **2 milioni di utenti registrati** sul territorio nazionale l'**obbligo** di **rimuovere o bloccare l'accesso ai contenuti illeciti** presenti al loro interno. L'obbligo riguarda anche l'incitamento all'odio, il **cd. *hate-speech***, ovvero quelle pubblicazioni discriminatorie o più genericamente diffamatorie che appaiono in rete.

I *provider* che ricevano **oltre 100 reclami** (*Beschwerden*) **all'anno** in merito a contenuti illeciti pubblicati sulle proprie piattaforme, hanno l'obbligo di produrre una **relazione semestrale** (c.d. *Berichtspflicht*, di cui al § 2 NetzDG) sulla gestione di tali reclami. La relazione deve essere pubblicata sulla Gazzetta federale e sul sito web dello stesso *provider* entro il mese successivo alla scadenza del semestre di riferimento. La legge elenca in modo dettagliato il contenuto minimo della relazione che, una volta pubblicata in rete, dovrà essere facilmente riconoscibile, direttamente accessibile e permanentemente disponibile.

Per la **gestione dei reclami**, la legge prevede che il fornitore di *social network* si doti di una procedura efficace e trasparente, che possa agevolare le

---

ai sensi del § 186 StGB (*Üble Nachrede*), in base al quale "chiunque, riferendosi ad un'altra persona, afferma o divulga un fatto idoneo a denigrarla o a svalutarla di fronte all'opinione pubblica, se il fatto non è provabile e vero, è punito con la pena detentiva fino ad un anno o con la pena pecuniaria; se l'azione è commessa pubblicamente o mediante la diffusione di scritti, l'autore è punito con la pena detentiva fino a due anni o con la pena pecuniaria".

[11] Al fine di adeguare, anche dal punto di vista tecnico, le rispettive piattaforme, ai fornitori di *social network* è stato concesso un termine di adattamento di tre mesi per poter applicare la nuova disciplina (§ 6, comma 2, NetzDG).

segnalazioni di contenuti illeciti da parte degli utenti della piattaforma. La procedura deve inoltre consentire l'immediata presa in carico della denuncia, la verifica dell'illiceità del contenuto denunciato e la rimozione o il blocco del relativo accesso entro i termini stabiliti. Il legislatore ha, infatti, fissato obblighi di intervento particolarmente stringenti nel caso di **contenuti palesemente e gravemente illeciti**[12], come ad esempio scritti che propagandano il **negazionismo**. In tale ipotesi la rimozione dei contenuti dovrà avvenire al massimo **entro 24 ore**. Per le **ipotesi meno gravi** o che richiedano un vaglio più approfondito il termine concesso ai *social network* per la rimozione è, invece, esteso fino a **7 giorni**. Il *social network* può anche delegare la decisione sull'eliminazione dei contenuti a un'**istituzione di autoregolamentazione** riconosciuta ai sensi della legge (*Einrichtung der Regulierten Selbstregulierung*)[13] e concordare di accettarne le determinazioni.

La direzione del *social network* è tenuta ad assicurare il **monitoraggio** sulla gestione dei reclami attraverso **controlli mensili** e sopperire alle eventuali carenze organizzative per quanto concerne i reclami pervenuti. Al personale preposto alla procedura di presa in carico e gestione dei reclami devono essere offerti regolarmente, almeno ogni sei mesi, corsi di formazione e aggiornamento professionale.

Il comportamento inadempiente del *provider* può essere sanzionato, ai sensi del § 4 NetzDG, con una **multa da 500.000 a 5 milioni di euro**. Il *provider* è inoltre tenuto a notificare al denunciante e all'utente ogni decisione adottata in materia con le relative motivazioni. In caso di rimozione di contenuti illeciti, il fornitore del servizio è altresì obbligato alla **conservazione del contenuto rimosso** quale materiale probatorio per un periodo di 10 settimane. Le segnalazioni per crimini, minacce, accuse e diffamazioni pubblicate sulla piattaforma del *social network* devono poter contare su un **referente territoriale** (*inländischer Zustellungsbevollmächtigter*), raggiungibile con facilità in caso di urgenza. È invece prevista una sanzione pecuniaria fino a 500.000 euro per i responsabili delle piattaforme nel caso di mancata nomina del referente territoriale o di una persona incaricata per i reclami (*inländischer Empfangsberechtigter*); la medesima

---

[12] Il § 1,comma 3, NetzDG fa esplicito riferimento a 20 articoli del Codice penale tedesco. Tali disposizioni includono i divieti sulla propaganda nazista e la pornografia infantile, nonché reati di carattere più generale, come insulti, diffamazione, istigazione all'odio, la diffusione di immagini violente, la falsificazione sediziosa e la violazione della quiete pubblica con la minaccia di commettere un crimine.

[13] Ai sensi del § 3, comma 6, NetzDG, un'istituzione è riconosciuta quale istituzione di autoregolamentazione se: ne è garantita l'indipendenza e l'esperienza degli analisti; dispone di adeguate strutture e garantisce analisi tempestive e comunque entro 7 giorni; dispone di norme procedurali che disciplinano l'ambito e la struttura dell'analisi, stabiliscono i requisiti delle reti sociali affiliate e la possibilità di riesaminare le decisioni; ha istituito un servizio reclami (*Beschwerdestelle*); è finanziata da *provider* di *social network* che garantiscano l'adeguatezza dei servizi, ferma restando la disponibilità all'ammissione di ulteriori fornitori, specie di reti sociali.

sanzione (fino a 500.000 euro) è altresì prevista per l'incaricato dei reclami qualora questi non si attivi entro le 48 ore successive alla ricezione del reclamo stesso.

La legge prevede, infine, che il Ministero federale della Giustizia e della Tutela dei consumatori, d'intesa con il Ministero federale dell'Interno, il Ministero federale per l'Economia e l'Energia e il Ministero federale dei Trasporti e dell'infrastruttura digitale, emani i principi amministrativi generali per l'esercizio del potere discrezionale dell'autorità amministrativa preposta nell'avvio di un procedimento sanzionatorio e nella valutazione dell'ammenda. Tali principi sono oggetto delle **Linee guida** per la determinazione delle sanzioni pecuniarie in caso di violazioni della *Netzwerkdurchsetzungsgesetz* (*Leitlinien zur Festsetzung von Geldbußen im Bereich des Netzwerkdurchsetzungsgesetzes*), adottate il 22 marzo 2018. Nei casi in cui sorgano dubbi sull'obbligo di rimozione dei contenuti è previsto anche l'intervento del giudice competente sul ricorso contro la sanzione pecuniaria. La decisione del giudice è inoppugnabile e vincolante per l'autorità amministrativa (*Bundesamt für Justiz*).

Nel **Regno Unito**, il tema controverso della "post-verità"[14] è stato oggetto dell'**inchiesta parlamentare** (*Fake news inquiry*[15]) svolta, tra il settembre 2017 e il febbraio 2019, dal ***Digital, Culture, Media and Sports Committee*** della *House of Commons*.

Il tema dell'indagine, come individuato nei *terms of references*, ha riguardato in particolare: (a) l'individuazione della nozione di *fake news* e della linea di confine tra l'espressione di opinioni di parte, ma legittime, e la diffusione di dati falsi a fini propagandistici; (b) l'impatto delle cosiddette *fake news* sulla comprensione dell'attualità da parte del pubblico, nonché sui tradizionali valori di obiettività e di equilibrio dell'informazione giornalistica; (c) le reazioni del pubblico a tale fenomeno, differenziate per età, sesso ed estrazione sociale; (d) il ruolo della pubblicità commerciale nella sua diffusione, anche in relazione al collocamento delle inserzioni pubblicitarie sui siti internet il cui maggior richiamo si basi sul "sensazionalismo" di notizie false; (e) la responsabilità dei *social networks* e dei motori di ricerca; (f) l'educazione del pubblico all'uso delle diverse fonti di informazione; la possibile utilità di meccanismi automatici in grado di individuare e rimuovere, attraverso algoritmi, le informazioni di questo genere; (g) il confronto tra le esperienze degli Stati membri relativamente al grado di accettazione di tale categorie di informazioni da parte del pubblico.

---

[14] Come riportato da organi di stampa, il sintagma "*post-truth*" è stato designato quale espressione dell'anno (per il 2016) dagli *Oxford Dictionaries*.

[15] House of Commons, DCMS Committee, *Fake news inquiry*.

Peraltro, gli aspetti ora enumerati sono stati considerati dalla commissione parlamentare nel più generale contesto dell'impatto che la diffusione di informazioni così manipolate può avere sui processi democratici. Essa ha perciò preso in esame particolare la questione del ruolo e della responsabilità delle **piattaforme di servizi on-line**, venuta in risalto in relazione ad episodi di utilizzazione abusiva di dati personali e di profilazione individuale come quelli verificatisi in occasione della campagna referendaria sulla **Brexit** e in altre recenti occasioni di confronto politico-elettorale (si tratta dei casi *Facebook*, *Cambridge Analytic*a, *AggregateIQ*).

Nel corso dei suoi lavori la Commissione ha svolto l'audizione di diversi soggetti istituzionali, di *stakeholders* e di esperti anche stranieri. Essa ha così acquisito, tra le altre, le valutazioni del ***Committee on Standards on Public Life*** (nota anche come "commissione Nolan" dal nome del suo primo presidente), preposto dal 1994 alla vigilanza sul rispetto dei **principi deontologici** che informano la condotta dei soggetti titolari di cariche pubbliche (ovvero i principi di *Selflessness*, *Objectivity*, *Integrity*, *Accountability*, *Openness*, *Honesty* e *Leadership*)[16]". Nel documento[17] predisposto per l'indagine parlamentare, la commissione Nolan ha messo in relazione la diffusione delle *fake news* con il progressivo discredito pubblico verso le istituzioni e gli esponenti politici.

L'analisi dei diversi aspetti implicati dal fenomeno e dei relativi effetti, d'altra parte, ha indotto la commissione ad adottare la nozione di ***disinformazione*** in luogo di quella, più vaga se non equivoca[18], di *fake news*, dovendosi intendere la prima come la "deliberata creazione e condivisione di informazioni false o manipolate dirette a ingannare e a fuorviare il pubblico, sia per finalità lesive che per interesse politico, personale o finanziario".

Di tale fenomeno la commissione ha indagato gli aspetti più rilevanti, formulando una serie di raccomandazioni in una prima relazione del 2018 e svolgendo più ampie valutazioni nella **relazione finale** del 2019[19], dedicate a profili la cui incidenza non si limita all'ambito dei diritti della persona, ma riguarda evidentemente la sfera pubblica e la formulazione delle scelte politico-elettorali.

---

16 V. anche: Committee on Standards on Public Life, *Fake news and the Nolan Principles*.

17 *Submission of The Committe on Standards in Public Life*, 1 marzo 2017.

18 La commissione ha infatti ritenuto che l'espressione "*fake news*" ha generalmente "assunto una varietà di significati, incluso quello riferito ad affermazioni che non sono gradite al lettore o da lui condivise".

19 House of Commons, DCMS Committee, *Disinformation and "fake news": Final report*, pubblicato il 18 febbraio 2019. In precedenza la commissione aveva pubblicato il 29 luglio 2018 un *Interim Report*, i cui contenuti si sono successivamente arricchiti con gli esiti di una serie di audizioni; già a questo rapporto "intermedio" aveva fatto seguito la replica del Governo: *Disinformation and "fake news": Interim report: Government Response to the Committee's Fifth Report of Session 2017-19*, 23 ottobre 2018.

È stato affrontato in primo luogo il tema delle ***online harms***, ovvero delle lesioni all'integrità psicofisica dell'individuo arrecategli attraverso comunicazioni veicolate dalle piattaforme digitali allo scopo di esporlo a distorsioni "mirate" della realtà, a forme di istigazione o ad espressioni d'odio. A tale riguardo la commissione ha ritenuto (considerata anche l'esperienza legislativa di altri Paesi) che di tali piattaforme debba essere prevista e disciplinata la responsabilità per i contenuti immessi e ha perciò raccomandato, in coerenza con moduli già sperimentati in altri ambiti dell'ordinamento britannico, l'ampliamento della sfera di competenza dell'autorità indipendente di regolazione delle telecomunicazioni (*Ofcom*) in prospettiva dell'applicazione di un **codice di condotta** vincolante per gli operatori del settore.

L'orientamento rivolto ad un complessivo rafforzamento delle **autorità indipendenti di regolazione e controllo** è espresso dalla commissione in relazione ad ulteriori profili oggetto di indagine.

Tra questi, un tema cruciale, esaminato dalla commissione in relazione ad elementi acquisiti dall'autorità di garanzia della *privacy* (*Information Commissioner Office* – ICO), è quello del **trattamento dei dati personali**, raccolti perlopiù senza consapevolezza dell'interessato mediante l'osservazione dei suoi comportamenti *on-line*, allo scopo di generare *big data* utilizzabili a fini di **profilazione** degli individui per renderli destinatari di propaganda politica "mirata"[20]. Al riguardo la commissione ha approfondito il *modus operandi* (e lo stesso *business model*) di *Facebook* in ordine alla raccolta dei dati sui propri utenti e alla loro condivisione con altri soggetti, e ha così ricostruito lo scenario complessivo in cui si sono verificati casi eclatanti di illecito trattamento di dati personali come quello, già ricordato, di *Cambridge Analytica*.

Il medesimo scenario, d'altronde, si connota per la **posizione dominante** acquisita a livello globale da imprese come *Facebook* e per la loro inadeguata interlocuzione con le autorità nazionali[21]. Secondo la commissione, "la posizione di dominio di poche potenti *tech companies* fa sì che queste si comportino come monopoliste nel loro specifico ambito, e che sorgano preoccupazioni circa i dati su cui i relativi servizi sono basati. Facebook, in particolare, non è disponibile a rispondere del proprio operato ai soggetti regolatori nei diversi paesi. Il Governo dovrebbe dunque considerare l'impatto di questi monopoli sulla vita politica e sulla democrazia"[22].

---

[20] Al tema specifico dell'utilizzazione dei *big data* per finalità di propaganda elettorale l'ICO ha presentato, nel 2018, una relazione al parlamento, *Investigation into the use of data analytics in political campaign*.

[21] Tale giudizio della commissione della Camera dei Comuni si fonda anche sulla indisponibilità da parte del CEO di *Facebook* a presentarsi in audizione dinanzi alla medesima nel novembre 2018.

[22] House of Commons, DCMS Committee, *Disinformation and "fake news": Final report*, cit., p. 42.

A tale proposito si è prospettata (tanto più in un quadro di riferimento normativo ora innovato dalla vigenza del Regolamento UE 679/2016[23]) l'esigenza di un potenziamento dell'autorità di garanzia della *privacy* e della sua capacità di vigilare in un ambito caratterizzato dall'incessante evoluzione tecnologica; ed è stata formulata la proposta di sottoporre le *tech companies* ad un **prelievo fiscale** il cui gettito sia destinato al finanziamento dell'organismo di controllo (in modo analogo a quanto avviene nel settore finanziario, in cui le risorse destinate all'autorità regolatrice, la *Financial Services Authority*, si alimentano anche degli oneri fiscali posti sulle imprese che vi operano).

D'altra parte la posizione dominante di tali imprese ha rilievo specifico per l'**assetto competitivo del mercato di riferimento**[24]. A questo riguardo la commissione ha raccomandato che l'autorità di garanzia della concorrenza, la *Competition and Markets Authority* (CMA), effettui un'analisi della struttura e del funzionamento del mercato pubblicitario riferito ai social media, al fine di accertare se effettivamente "*Facebook* abusa della sua posizione dominante sul mercato dei social media per determinare il successo o il fallimento di altre imprese", posto che "società come *Facebook* non dovrebbero comportarsi come *gangster digitali* nel mondo *on-line*, considerandosi al di là e al di sopra della legge"[25].

L'incidenza della disinformazione e della propaganda veicolata dai *social media* è stata considerata dalla commissione della Camera dei Comuni anche a proposito della campagna referendaria svoltasi sul distacco del Regno Unito dell'Unione europea, in relazione a forme di **violazione della normativa elettorale** conseguenti sia alla illegittima utilizzazione di dati personali degli elettori, sia all'indebito superamento dei limiti di spesa previsti per le campagne referendarie[26].

A questo proposito, la ricostruzione svolta dalla commissione delle influenze esercitate a sostegno della campagna referendaria per il "*leave*" da alcuni soggetti imprenditoriali impegnati nel fronte favorevole alla ***Brexit*** (attraverso l'incrocio di dati personali, l'applicazione di procedimenti algoritmici di profilazione degli

---

[23] Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

[24] Tale profilo è venuto in evidenza in relazione al caso *Six4Three*, che ha messo in luce le attività anticoncorrenziali poste in essere da *Facebook* (dopo aver acquisito *Instagram* nel 2012 e *WhatsApp* nel 2014) nei confronti dei propri concorrenti, ai quali negava l'accesso ai dati dei propri utenti.

[25] House of Commons, DCMS Committee, *Disinformation and "fake news": Final report*, cit., p. 42.

[26] A questo profilo specifico è dedicata la relazione della *Electoral Commission* del giugno 2018, *Digital Campaigning: increasing transparency for voters*, in cui si raccomanda il complessivo adeguamento dell'apparato sanzionatorio per la violazione della normativa elettorale attraverso tali modalità di propaganda politica: sono infatti necessarie "more clarity over who is spending what, and where and how, and bigger sanctions for those who break the rules. Funding of online campaigning is already covered by the laws on election spending and donations. But the laws need to ensure more clarity about who is spending what, and where and how, and bigger sanctions for those who break the rules".

elettori, l'accesso a disponibilità finanziarie di fonte privata) tende a mostrare con efficacia il livello di opacità e il potenziale manipolatorio di simili forme di organizzazione del consenso politico.

Nondimeno si riconosce, da parte della commissione, che la legislazione vigente necessita di modifiche e aggiornamenti a fronte di modalità di comunicazione politica che, per loro natura, esulano dall'ambito tipico di attività dei partiti politici, presentano elementi comuni alla pubblicità commerciale e, soprattutto, hanno la più vasta diffusione attraverso le reti di contatto e di condivisione consentite dai canali digitali e dalle applicazioni tecnologiche alla portata di chiunque.

Le regole esistenti non sono infatti sufficienti a disciplinare compiutamente l'odierna comunicazione politica digitale (***digital campaigning***), specialmente in relazione alla pubblica conoscibilità delle fonti di finanziamento, alla trasparenza delle tecniche utilizzate per l'individuazione selettiva dei soggetti destinatari della propaganda e all'efficace azione di vigilanza dell'autorità competente, la ***Electoral Commission***[27]. Di questo organismo la commissione prospetta, come negli altri casi, il rafforzamento dei poteri nelle materie di sua competenza, in relazione – ad esempio - all'accesso alle informazioni detenute dalle *social media companies*; all'irrogazione di sanzioni pecuniarie in misura non predeterminata bensì proporzionale agli introiti di tali imprese; all'abilitazione ad impugnare i risultati di consultazioni elettorali in cui siano state commesse violazioni (finora riservata in via esclusiva ai soggetti privati); all'inibitoria di comportamenti posti in essere durante lo svolgimento delle campagne elettorali da soggetti stranieri.

A quest'ultimo profilo – le **interferenze straniere nei processi elettorali nazionali** – la commissione dedica particolare attenzione, stante la risonanza che il tema ha avuto nel recente dibattito politico[28], e riserva considerazioni dirette a promuovere una revisione del diritto interno relativamente alla disciplina dei finanziamenti elettorali conferiti da soggetti stranieri (al momento non oggetto di divieto legislativo), alla portata applicativa delle norme vigenti che puniscono gli atti di corruzione perpetrati all'estero (*Bribery Act 2010*), e all'opportunità di adottare disposizioni analoghe a quelle previste già nel 1938 dal legislatore

---

[27] L'inadeguatezza della legislazione elettorale è chiaramente evidenziata dalla commissione, che indica alcune linee di riforma: "Electoral law is not fit for purpose and needs to be changed to reflect changes in campaigning techniques, and the move from physical leaflets and billboards to online, microtargeted political campaigning. There needs to be: absolute transparency of online political campaigning, including clear, persistent banners on all paid-for political adverts and videos, indicating the source and the advertiser; a category introduced for digital spending on campaigns; and explicit rules surrounding designated campaigners' role and responsibilities" (House of Commons, DCMS Committee, *Disinformation and "fake news": Final report*, cit., p. 60).

[28] Alle interferenze straniere nelle campagne elettorali svoltesi recentemente nel Regno Unito, riconducibili all'azione deliberata di disinformazione posta in essere da apparati di Stati esteri e da gruppi di interesse a questi collegati, è dedicato il sesto capitolo della relazione (*Foreign influence on political campaign*).

statunitense (*Foreign Agents and Registration Act* -FARA) al fine di sottoporre ad obblighi di trasparenza e di rendicontazione i soggetti i quali, presenti nel territorio nazionale, vi operino come rappresentanti di enti o soggetti stranieri "in veste politica o a questa analoga".

In ultimo, la relazione della commissione parlamentare si sofferma sul tema della "**alfabetizzazione digitale**" (*digital literacy*), nella consapevolezza di quanto le pratiche di disinformazione si giovino di limiti culturali diffusi nell'ampia platea degli utenti dei *social media*, spesso non in grado di discernere (al di là delle sofisticate manipolazioni informative di cui possono essere bersaglio) tra contenuti veritieri ed altri di lampante inattendibilità. Sotto questo profilo la commissione raccomanda l'intensificazione delle attività promozionali e di sensibilizzazione pubblica già attribuite all'*Ofcom* (ritenendo la *digital literacy* come il "quarto pilastro" dell'educazione, dopo la lettura, la scrittura e le abilità matematiche), e per altro verso ritiene che l'indicazione, nei *social media*, della fonte e della finalità dei singoli contenuti che vi sono immessi possa costituire uno strumento efficace per il formarsi dell'opinione di chi ne è destinatario.

Conclusa l'indagine parlamentare, in seno alla suddetta commissione dei Comuni è stato costituito il *Sub-Committee on Disinformation*, con il compito di sottoporre al costante **esame del parlamento** i fenomeni di disinformazione ritenuti suscettibili di alterare in vario modo le forme della partecipazione politica e conseguentemente l'equilibrio democratico del Paese. Ai lavori della sottocommissione, concepita come "sede istituzionale per l'esame di materie concernenti la disinformazione e la *privacy*"[29], possono peraltro partecipare tutti i membri della commissione "plenaria", nonché essere invitati i componenti di altre commissioni permanenti al fine di prendere parte ad audizioni, così come ora consente una recente innovazione regolamentare (*Standing Order* 137A, introdotto il 6 febbraio 2019)[30].

La **sottocommissione sulla disinformazione** è altresì inserita nella rete di **cooperazione interparlamentare** istituita in questo ambito (nota come "*International Grand Committee on Disinformation and 'Fake-News'*"), la cui sessione inaugurale ha avuto luogo a Londra il 27 novembre 2018[31] seguita dall'incontro svoltosi presso il parlamento canadese ad Ottawa il 28 maggio 2019[32]. In occasione della prima riunione, il *Grand Committee* ha emesso una

---

[29] House of Commons, DCMS Committee, *The launch of the Sub-Committee on Disinformation*, 2 aprile 2019.

[30] *Standing Order* 137A, *Select committees: power to work with other committees*.

[31] Il *grand committee* riunitosi a Londra nel 2018 si è formato di 24 membri, in rappresentanza di nove Paesi (incluso il Regno Unito): Argentina, Belgio, Brasile, Canada, Francia, Germania, Lettonia, Singapore (oltre agli 11 membri della commissione ospitante della Camera dei Comuni).

[32] L'incontro è stato organizzato dalla commissione permanente *on Access to Information, Privacy and Ethics* del parlamento canadese. Questa ha a sua volta pubblicato nel dicembre 2018 una

dichiarazione sulla disciplina delle piattaforme digitali (*International Principles on the Regulation of Tech Platforms*) [33].

Nel **preambolo** del documento si riconosce che "il mondo in cui operano le istituzioni tradizionali del governo democratico muta ad una velocità senza precedenti; è priorità urgente e fondamentale per le assemblee legislative e i governi assicurare che i diritti fondamentali e le guarentigie dei cittadini non siano violati o indeboliti dall'avanzare incontrollato della tecnologia; l'ordine del mondo democratico patisce una crisi di fiducia alimentata dalla crescente disinformazione, dalla proliferazione delle aggressioni online e dei discorsi d'odio, da concertati attacchi ai nostri comuni valori democratici di tolleranza e di rispetto per le opinioni altrui, e dall'ampio abuso di dati appartenenti ai cittadini al fine di consentire tali tentativi di sabotare i processi democratici, incluse le elezioni". Ciò premesso, il testo del documento prosegue affermando che "la democrazia rappresentativa è troppo importante, e conquistata a così caro prezzo, da potersi lasciare indifesa rispetto alle *online harms*, in particolare alle aggressive campagne di disinformazione a cui la collettività assiste sui social media"; e ritenendo che "si deve creare un sistema di *governance* globale di Internet che possa servire a tutelare i diritti e le libertà fondamentali delle generazioni a venire, fondato su consolidati codici di comportamento per i soggetti agenti per conto degli Stati, e a disciplinare le principali piattaforme tecnologiche internazionali le quali hanno realizzato i sistemi che diffondono contenuti online a miliardi di utenti nel mondo".

Il documento si conclude con l'enunciazione - "nell'interesse della trasparenza, della responsabilità e della tutela della democrazia rappresentativa" – dei cinque **principi fondamentali della dichiarazione**: "1. Internet è globale e la sua disciplina giuridica deve derivare da principi globalmente condivisi. 2. Diffondere in modo deliberato disinformazione e divisione costituisce una concreta minaccia al mantenimento e alla crescita della democrazia e di un civile dialogo globale. 3. Le imprese tecnologiche globali devono riconoscere il potere che esse detengono e dimostrare di essere pronte ad assumersi le grandi responsabilità che ne derivano. 4. Le *social media companies* dovrebbero essere tenute responsabili per l'inosservanza di disposizioni giudiziarie, legislative o regolamentari concernenti la rimozione di contenuti offensivi o ingannevoli dalle loro piattaforme, e dovrebbero essere regolamentate al fine di assicurare che tali prescrizioni siano adempiute. 5. Le imprese tecnologiche devono dimostrare la propria responsabilizzazione (*accountability*) nei confronti degli utenti rendendosi pienamente disponibili

relazione dedicata al tema, *Democracy under threat: risks and solutions in the era of disinformation and data monopoly*.

[33] Il testo originale della dichiarazione si legge in allegato alla già citata relazione del *DCMS Committee* del 2019.

all'interlocuzione con i parlamenti nazionali e gli altri organi della democrazia rappresentativa".

Il **Governo** britannico, dal canto suo, ha affrontato il tema degli *online harms* dedicandovi un "**Libro bianco**" la cui pubblicazione, nel 2019, ha dato avvio ad una pubblica consultazione (conclusasi il 1° luglio dell'anno corrente)[34]. Nel documento è delineato un **piano di azione** da realizzare attraverso l'adozione di misure sia legislative che di diversa natura, nel complesso preordinate a garantire la sicurezza delle persone (specialmente i minori e i soggetti vulnerabili) senza porre ostacoli all'innovazione tecnologica e allo sviluppo dell'economia digitale.

Tali linee programmatiche fanno leva, per quanto riguarda in modo specifico il fenomeno della **disinformazione**, sull'ampliamento della nozione di diligenza (*duty of care*) dei gestori di piattaforme digitali al fine di sottoporli ad **obblighi di controllo** relativi ai contenuti diffusi per loro tramite, e sull'attribuzione ad un'**autorità indipendente di regolazione** (non è chiaro se individuata tra quelle esistenti oppure di nuova istituzione) di penetranti poteri di vigilanza e di intervento, da esercitare sulla base di una valutazione dei rischi connessi al contenuto delle comunicazioni digitali in sé considerate o alla particolare vulnerabilità dei possibili destinatari. Inoltre, secondo un tratto dell'ordinamento britannico che tradizionalmente valorizza la normazione di matrice deontologica e autodisciplinare, è prevista l'introduzione di **codici di condotta** il cui carattere obbligatorio per le imprese interessate si accompagna alla formulazione "per principi" e alla flessibilità delle clausole, affinché queste possano adattarsi alla mutevolezza del contesto di riferimento.

Quanto al loro contenuto, il "Libro bianco" stabilisce che i codici suddetti contemplino previsioni da incorporare nelle condizioni di contratto per l'accesso ai servizi digitali, al fine di introdurvi la definizione dei comportamenti tipicamente costitutivi della disinformazione (definita nel documento come "l'informazione creata o disseminata con deliberato intento ingannevole", che "possa arrecare danno ad altri per vantaggio personale, politico o finanziario")[35].

I codici, inoltre, devono prevedere le sanzioni in cui l'utente incorre in caso di violazione; le misure da applicare nei riguardi di utenti che deliberatamente celano

---

[34] *Online Harms White Paper* (aprile 2019) redatto congiuntamente dallo *Home Office* e dal *Department for Digital, Culture, Media and Sport*. Quest'ultimo ha contestualmente pubblicato documenti diretti a promuovere comportamenti "virtuosi" nei *social media*, nel presupposto che in tale ambito la tutela dei diritti dell'individuo non debba differire da quella assicuratagli nella dimensione *off line*: si vedano, ad esempio, il *Digital Charter* e il *Code of Practice for providers of online social media platforms* (entrambi dell'aprile 2019).

[35] Il "Libro bianco" assegna rilievo particolare alla *disinformation* nel novero degli *online harms* (qualificandola come "una minaccia al nostro stile di vita"), e di essa individua varie forme di manifestazione: la *online disinformation* (diffusione intenzionale di notizie false o ingannevoli) e *misinformation* (involontaria condivisione delle medesime); la *online manipulation* (manipolazione delle opinioni attraverso la propaganda basata su false informazioni); *online abuse of public figures* (offese e intimidazioni rivolte ad esponenti della vita pubblica).

la propria identità al fine di diffondere contenuti "dis-informativi"; le soluzioni da adottarsi per rendere meno visibili le informazioni ritenute non attendibili dopo il vaglio effettuato da servizi accreditati di *fact-checking*; il ricorso a tali servizi, specialmente durante i periodi elettorali; la promozione delle fonti informative autorevoli e tra loro diversificate, al fine di contrastare il formarsi delle cosiddette "eco-camere" in cui l'utente è reso destinatario unicamente di contenuti informativi diretti a rafforzare le opinioni che già detiene; l'esplicitazione all'utente di *accounts* operanti in forma automatizzata; l'incremento della trasparenza della pubblicità di argomento politico, in linea con gli obblighi previsti dalla legislazione in materia elettorale; procedure che consentano all'utente di segnalare facilmente contenuti di cui conosca oppure sospetti la falsità; indicazioni circa il livello di efficacia delle iniziative adottate dalle stesse imprese tecnologiche per contrastare le attività di disinformazione in rete. In relazione ai profili fin qui richiamati appare evidente il proposito del Governo di introdurre, per la diffusione dell'informazione in rete, standard qualitativi non dissimili da quelli raccomandati ad esito dell'indagine sul giornalismo affidata dal Governo medesimo ad esperti indipendenti[36].

Ancora sul versante del Governo, se il rilievo attribuito alla minaccia rappresentata dalla disinformazione è indicato dalla costituzione in seno al *Cabinet Office*, nell'aprile 2018, di un'unità dedicata al **contrasto della disinformazione** - la *Rapid Response Unit* [37]-, pari attenzione è stata riservata al tema nel quadro dei **programmi di cooperazione internazionale** ai quali partecipa il Regno Unito: da ultimo, il Governo ha disposto (il 7 luglio 2019) lo stanziamento di 18 milioni di sterline, distribuito nell'arco di tre anni e a carico del *Conflict, Stability and Security Fund* gestito dal *Cabinet Office*, per il finanziamento di iniziative di contrasto della disinformazione nei Paesi dell'Europa orientale e a sostegno dell'indipendenza dei mezzi di informazione nei Balcani occidentali[38].

Peraltro, le iniziative adottate in ambito parlamentare e governativo si sono caratterizzate per l'apporto fornito da centri studi, fondazioni, soggetti accademici. Le complesse questioni determinate sul piano sociale, politico e deontologico dalle frequenti pratiche di manipolazione dei dati, di presentazione artificiosa dei fatti, di diffusione attraverso i canali informativi di "notizie" di apparente veridicità e oggettività (ma che invece è ormai d'uso connotare come *post-truth*, *fake news*, *echo-chambers*, *"alternative" facts*), hanno infatti costituito anche materia di **dibattiti** e **iniziative** promossi in sede scientifica.

---

[36] Si tratta della Cairncross Review, conclusasi con la relazione pubblicata nel Febbraio 2019, *A sustainable future for journalism*.

[37] La *Rapid Response Unit* è preposta al monitoraggio e all'analisi dei *trends* della comunicazione digitale, al fine di individuare i contenuti finalizzati alla disinformazione in materie rilevanti per la sfera pubblica e ad apprestare rapidamente gli idonei correttivi attraverso smentite e rettifiche.

[38] Si veda il comunicato stampa del 7 luglio 2019, *UK steps up fight against fake news*.

L'*Oxford Internet Institute*, in particolare, ha dedicato attenzione al tema delle *fake news*. Oltre ad aver promosso progetti di ricerca sulla "**politica digitale**" e sulla "*computational propaganda*", ha svolto un'opera di sensibilizzazione, provvedendo a riprodurre sul suo sito web alcuni articoli dedicati a diversi nodi problematici dell'informazione trasmessa attraverso i canali digitali. Essi riguardano, rispettivamente: i "**filtri**" che selezionano con criteri di acritica omogeneità le notizie circolanti sui *social networks*[39]; la necessità di presidiare l'"**infosfera**" dall'inquinamento della "post-verità"[40]; le implicazioni per la vita democratica delle "*fake news*" e gli obblighi da porre sulle **piattaforme digitali** in relazione al trattamento dei dati sugli utenti[41]; la trasparenza degli **algoritmi** utilizzati per la "personalizzazione" delle informazioni e dei loro meccanismi di funzionamento[42]; i procedimenti, umani o tecnologici, di **verifica dei fatti** riferiti attraverso i canali suddetti[43].

Il tema della veridicità e dell'accuratezza delle notizie è emerso anche in relazione alla diffusione di **dati statistici**, oggetto di un recente seminario promosso dalla *Royal Statistical Society* e svoltosi il 7 febbraio 2017 ("*Post-truth: what is it and can we do about it*?").

In tale ambito, peraltro, l'autorità indipendente di vigilanza sull'informazione statistica (la *UK Statistics Authority*), la **Biblioteca della Camera dei Comuni** e lo *Economic and Social Research Council* hanno instaurato, assieme alla fondazione indipendente *Full Fact*, un rapporto di collaborazione finalizzato a porre in essere attività promozionali e di verifica della veridicità, oggettività e integrità delle notizie diffuse al pubblico ("*fact checking*"). Il progetto, denominato *Need to know*, muove dal presupposto che "la qualità dei dati e delle relative analisi sia essenziale per un'effettiva democrazia parlamentare"[44]; l'informazione statistica, d'altro canto, "offre un solido fondamento per i processi decisionali e i relativi dibattiti", cosicché si rende necessario identificare gli ambiti in cui è opportuno rafforzare il "potere dei dati" per consentire che il Paese possa compiere le scelte migliori[45].

---

39 B. Hogan, *How Facebook divides us*, Times Literary Supplement, 27 ottobre 2016.

40 **L. Floridi,** *Fake news and a 400-year-old problem: we need to resolve the 'post-truth' crisis***, The Guardian, 29 novembre 2016.**

41 **P. Howard,** *Facebook and Twitter's real sin goes beyond spreading fake news***, Reuters, 3 gennaio 2017.**

42 **B. Mittelstadt,** *Auditing for Transparency in Content Personalization Systems***,** International Journal of Communication 10 (2016), 4991–5002.

43 **H. Ford:** *Verification of crowd-sourced information: is this 'crowd wisdom' or machine wisdom?***, 19 novembre 2013.**

44 Così si è espresso il *Librarian and Director General of Participation, Research and Information* della Camera dei Comuni, P. Young, rilevando anche che i servizi di documentazione parlamentare, sotto questo profilo, consentono ai "membri del Parlamento di adottare decisioni ben informate, in modo che quanto più sono affidabili le informazioni ad essi fornite, tanto più sono ben fondate le loro decisioni".

45 Affermazione del *National Statician*, J. Pullinger, nell'illustrare le finalità del progetto *Need to know*.

Tra i casi di studio finora esaminati nello svolgimento di questo progetto, può segnalarsi quello concernente la questione del contributo finanziario del Regno Unito all'Unione europea, emersa – tra le altre - nelle discussioni relative al referendum del 2016 sulla *Brexit* e alle successive iniziative del Governo; analogo studio di *fact checking* è stato svolto con riguardo alle notizie inerenti l'ordine di grandezza dell'immigrazione diretta verso il Regno Unito.

Non ancora consolidati appaiono, nel dibattito pubblico e nelle pratiche dell'informazione, l'efficacia e l'impatto di tali operazioni di verifica: mentre non ha avuto seguito la richiesta indirizzata dalla fondazione *Full Fact* ad un ministro del Governo in carica affinché correggesse, in ottemperanza agli obblighi derivanti dal *Ministerial Code* (par. 1.2, lett. c), precedenti affermazioni rese al Parlamento ma rivelatesi imprecise o non veritiere al riscontro dei fatti, per altro verso è stato annunciato, nel novembre 2016, il supporto finanziario di Google (nell'ambito della sua *Digital Information Initiative*) per le ricerche finalizzate alla realizzazione di dispositivi automatici di controllo della veridicità delle informazioni (*automated fact checking*)[46].

In **Spagna** la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, oltre ad aver adattato la legislazione interna al regolamento generale sulla protezione dei dati[47], ha inteso garantire i **diritti digitali della cittadinanza** in conformità con il mandato stabilito nell'articolo 18.4 della Costituzione[48] (art. 1.b).

In particolare il titolo finale della legge, il decimo, intitolato "Garanzia dei diritti digitali", composto da diciannove articoli (da 79 a 97), riconosce e regola l'esercizio di diritti quali la neutralità della rete e l'accesso universale o i diritti alla sicurezza e all'educazione digitale, la libertà di espressione su internet, il diritto all'oblio nei motori di ricerca e nei social network, la portabilità, il testamento digitale, l'intimità nell'uso di dispositivi digitali e sul posto di lavoro e la disconnessione digitale.

In particolare l'art. 85 prevede, al comma 2, che i responsabili dei social network e servizi equivalenti adottano protocolli appropriati per consentire l'esercizio del diritto di rettifica nei confronti degli utenti che diffondono contenuti che violano il diritto all'onore, l'intimità personale e familiare su internet e il diritto

---

46 Al tema la Fondazione *Full Fact* ha dedicato un rapporto in cui si esamina in dettaglio il ruolo della tecnologia nei procedimenti di verifica della fondatezza e veridicità delle informazioni circolanti su Internet: *The State of Automated Factchecking*, agosto 2016.

47 Si tratta del Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

48 "Articolo 18 (…)
4. La legge porrà limiti all'uso dell'informatica per salvaguardare l'onore e l'intimità personale e familiare dei cittadini e il pieno esercizio dei loro diritti".

di comunicare liberamente o **ricevere informazione veritiera (*información veraz*)**, secondo i requisiti e le procedure di cui alla Legge organica 2/1984, del 26 marzo, che disciplina il diritto di rettifica[49].

Nell'aprile 2019 è stata pubblicata la **Strategia nazionale sulla cybersicurezza 2019** (*Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional*).

In essa vi sono alcuni riferimenti alle "*fake news*" (***noticias falsas***). Ad esempio si sottolinea come le campagne di disinformazione fanno uso di elementi come notizie false per influenzare l'opinione pubblica. Internet e social network amplificano l'effetto e la portata delle informazioni trasmesse, con potenziali applicazioni contro obiettivi quali organizzazioni internazionali, Stati, iniziative politiche o figure pubbliche o perfino processi elettorali democratici (capitolo 2).

Tra le misure considerate vi è quella di promuovere uno spirito critico in favore di informazioni veritiere e di qualità e che contribuisca all'individuazione di notizie false e disinformazione (capitolo 4).

[49] Si rinvia inoltre a Carlos B Fernández, "*Los nuevos derechos digitales reconocidos por la Ley Orgánica 3/2018, de Protección de Datos y Garantía de los Derechos Digitales*, Noticias Jurídicas, dicembre 2018.

Gli atti del Consiglio d'Europa per contrastare la diffusione dei discorsi d'odio e delle fake news

(a cura del Servizio Rapporti Internazionali)

Atti approvati dall'Assemblea parlamentare del Consiglio d'Europa

L'Assemblea parlamentare del Consiglio d'Europa ha affrontato il tema del contrasto al discorso di odio, della difesa della libertà dei media e del contrasto alle *fake news* in ripetute occasioni nel corso dell'ultimo biennio. Il perseguimento di tali obiettivi è infatti strettamente legato alla difesa dei diritti umani nel suo complesso, vale a dire ad uno dei principali obiettivi dell'organizzazione.

Si segnalano, in particolare, i seguenti atti recentemente approvati:

- Nella **Risoluzione 2212** del **25 aprile 2018** *("Protezione dell'integrità editoriale")* è stato messo in risalto il ruolo della stampa e dei giornalisti in favore della diffusione di un'informazione di qualità, priva di pregiudizi, accurata, in grado di tenere conto di diverse opinioni politiche. I giornalisti e tutti gli operatori dell'informazioni sono pertanto chiamati a cooperare a tal fine, scambiandosi le proprie esperienze e cercando di rendere l'opinione pubblica sempre più conscia di tali problematiche.
- Nella **Risoluzione 2254** del **23 gennaio 2019** ("*La libertà dei media come premessa per elezioni democratiche"*) l'Assemblea ha delineato - e ne ha auspicato la realizzazione – linee guida di comportamento per tutti gli attori coinvolti nelle campagne elettorali al fine di garantirne la correttezza, la trasparenza, l'imparzialità nell'accesso ai mezzi di informazione e il pluralismo. Una campagna elettorale non dev'essere basata sulla concentrazione in poche mani dei mezzi di comunicazione, non deve diffondere con alcun mezzo false informazioni, soprattutto quelle che possano danneggiare i candidati avversari, deve basarsi su regole stringenti e consentire di distinguere nettamente la propaganda dalle attività di informazione. L'informazione prodotta a fine elettorale dovrebbe essere posta al vaglio di particolari organi in grado di garantirne la veridicità (c.d. *fact checking*). Sempre nell'ottica di sviluppare la massima correttezza, si auspica la creazione di "*media regulators*" che debbano essere organi di controllo indipendenti dal potere economico e politico. Particolare attenzione l'Assemblea dedica ai messaggi veicolati attraverso Internet, dove è più facile trovare informazioni false, basate su pregiudizi oppure odio razziale: è necessario per combattere tali forme di espressione diffondere i principi del rispetto per la dignità umana e della non-discriminazione. Nei casi più gravi, l'Assemblea naturalmente invita le autorità a bloccare i siti che abbiano diffuso e continuino a diffondere messaggi e false informazioni di tale tenore. I gestori di servizi connessi alla rete sono chiamati

anch'essi a svolgere un ruolo cooperando con la società civile e le organizzazioni politiche, sostenendo la ricerca e le applicazioni tecniche che possano scoraggiare sempre di più la diffusione di intolleranza, pregiudizi e false informazioni.

- La **Risoluzione 2255,** discussa congiuntamente alla precedente ed approvata il 23 gennaio 2019 *("I media del servizio pubblico nel contesto della disinformazione e della propaganda"),* ribadisce i temi precedentemente trattati affermando il ruolo del servizio pubblico in tale ambito. E' necessario, infatti, che sia presente un servizio pubblico forte ed efficiente per garantire un'informazione corretta e di qualità. La risoluzione introduce il termine di "*information disorder*" al posto di "*fake news*" per indicare il contenuto, la portata e la diffusione di informazioni false. Ogni Stato deve poter contare su un servizio pubblico indipendente, fornito di adeguati mezzi economici, affiancato da una rete di centri di ricerca sulla disinformazione che sappiano valutarne la portata, gli effetti e le tecniche.
- La **Risoluzione 2275** ("*Ruolo e responsabilità dei dirigenti politici nel contrasto al discorso d'odio e di intolleranza")* riprende i temi di una precedente campagna condotta a livello continentale dal Consiglio d'Europa, con lo scopo di favorire soprattutto la conoscenza dei giovani di tali problematiche e la loro partecipazione a programmi di contrasto. Nella risoluzione gli Stati membri sono chiamati a: monitorare la situazione relativa al discorso di odio, incluso quello di carattere politico, e aggregare i dati affinché sia possibile distinguerne gli obiettivi, gli autori, i canali usati; dare seguito alla Raccomandazione ECRI n. 15 che prevede sanzioni civili e penali per scoraggiare il discorso di odio; incoraggiare i partiti politici ed i gruppi di opinione affinché evitino nelle loro espressioni pregiudizi e manifestazioni di odio. L'opinione pubblica, inoltre, deve essere sempre più informata su tali temi favorendo programmi nelle scuole e addestrando adeguatamente le forze di polizia, la magistratura ed i medici. Anche i politici possono svolgere un ruolo importante divulgando messaggi positivi nei confronti delle minoranze, inserendo negli statuti dei loro partiti particolari disposizioni che contrastino il discorso di odio. E' necessario anche dare vita a gruppi di studio che includano anche la presenza di rappresentanti della società civile per monitorare gli effetti del discorso di odio a livello nazionale.
- La **Risoluzione 2276**, discussa congiuntamente alla precedente ed approvata il 10 aprile 2019 ("*Porre fine al discorso e ad atti di odio nello sport*"), prende in esame un altro settore dove l'intolleranza ha trovato terreno fertile. Anche in questo caso, gli Stati membri sono chiamati ad elaborare una banca dati che possa dare conto del luogo, della vittima e dell'autore di tali atti. Le vittime devono essere a loro volta divise tra atleti dilettanti e professionisti, così come devono essere individuate le parti offese tra i tifosi. La definizione ed il

contrasto di tale particolare forma di discorso di odio deve rientrare nei piani di contrasto a livello nazionale, sviluppando forme di cooperazione con le associazioni sportive, e garantendo adeguate sanzioni per contrastare il fenomeno. Anche in tale caso, l'educazione è chiamata a svolgere un compito primario per contrastare alla nascita i pregiudizi, il razzismo ed ogni forma di odio in generale. I media non devono tacere su tali episodi e le federazioni sportive devono avviare programmi di contrasto ad ogni forma di razzismo ed odio, chiamando i propri atleti a rivestire il ruolo di "ambasciatori dell'uguaglianza e della non-discriminazione". Lo sport, in ultima analisi, non può basarsi solo sulla competizione, ma è chiamato a svolgere un ruolo essenziale per armonizzare le diversità.

- Nella **Risoluzione 2281** approvata il **13 aprile 2019** (*"Social media: creatori di legami sociali o minacce per i diritti umani?*) si chiede agli Stati di adempiere a tutti gli obblighi connessi in particolare all'art. 10 della Convenzione per i Diritti Umani del Consiglio d'Europa, con particolare riguardo alla libertà di espressione, obbligando i gestori di piattaforme social a rispettare la diversità di opinioni astenendosi dal bloccare idee politiche e contenuti ritenuti controversi. Rilevante è il fatto che la Risoluzione chieda agli Stati anche di inserire nella formazione informatica per gli studenti anche l'apprendimento dell'uso dei social network, apprendimento che dovrebbe essere favorito dalla più tenera età. Gli Stati sono chiamati, inoltre, a ratificare al più presto il Protocollo aggiuntivo alla Convenzione n. 108 per la protezione dei diritti delle persone con particolare riguardo alla gestione automatica dei dati (*L'Italia ha ratificato il Protocollo il 5 marzo 2019),* che ha aggiornato e modernizzato i contenuti della Convenzione. La Risoluzione chiede inoltre che gli algoritmi usati nella ricerca e gestione di dati siano sostenuti da buone pratiche, così come la gestione dei dati personali da parte dei gestori dei servizi. Le società operanti nel settore sono chiamate a definire con precisione quali contenuti siano ammissibili e quali no (confrontandosi anche con l'art. 10 della Convenzione) accompagnando le loro decisioni, se necessario, con esempi pratici. Allo stesso modo gli utenti devono essere informati con chiarezza sui contenuti che loro prendono in esame, limitando all'occorrenza le funzioni "like"o "share".

La Commissione europea contro Il razzismo e l'intolleranza (ECRI)

Creata nel 1993 la **Commissione europea contro il razzismo e l'intolleranza del Consiglio d'Europa** (ECRI) ha il compito di monitorare la situazione nei Paesi membri alla luce delle norme della Convenzione Europea sui Diritti Umani e dei protocolli aggiuntivi, nonché della giurisprudenza della Corte europea e pubblica dei **rapporti dopo aver effettuato visite in ciascun Paese**. Questi rapporti sono pubblicati mediamente ogni cinque anni.

Una delegazione dell'ECRI ha effettuato una visita in Italia dal 13 al 18 settembre 2015 per preparare il successivo rapporto sul nostro Paese, che è stato pubblicato (come quinto ciclo del monitoraggio) il 7 giugno 2016 (*vedi infra)*. Nel precedente rapporto sull'Italia, del 2012, l'ECRI aveva evidenziato la mancanza d'indipendenza dell'Ufficio Nazionale Antidiscriminazioni Razziali (**UNAR**) e l'aumento di espressioni razziste e xenofobe nei discorsi in politica.

L'ECRI adotta inoltre delle Raccomandazioni tematiche o *General Policy Recommendations*. Si segnala, in particolare, la Raccomandazione n. 15, approvata l'8 dicembre 2015, sulla lotta contro il discorso d'odio. Nella Raccomandazione viene chiesto, tra l'altro, agli Stati membri di utilizzare i poteri regolamentari nei confronti dei media (compresi i fornitori di servizi Internet, gli intermediari online e i social media) per promuovere azioni volte a combattere l'utilizzo del discorso di odio e a contestarne il carattere inaccettabile, accertandosi al contempo che tali misure non costituiscano una violazione del diritto alla libertà di espressione e di opinione. Tale obiettivo va perseguito attraverso la vigilanza, l'incoraggiamento all'adozione di codici di buona condotta e di azioni di monitoraggio, l'uso di eventuali filtri ai contenuti in rete e di meccanismi di ricorso, incoraggiando al tempo stesso i professionisti dei media a promuovere un giornalismo etico (par. 7).

Le conclusioni dell'ECRI sull'attuazione delle raccomandazioni rivolte all'Italia nel rapporto 2016

Il **3 aprile 2019** l'ECRI ha adottato **le Conclusioni sull'attuazione delle Raccomandazioni**[50] rivolte alle Autorità italiane nel rapporto del 2016**.**

Si ricorda che **nel rapporto del 2016, l'ECRI raccomandava all'Italia**:

1) di completare quanto prima l'iter legislativo per la ratifica del Protocollo n. 12 alla Convenzione europea dei diritti dell'uomo;
2) che le autorità vigilino affinché il colore e la lingua siano espressamente inclusi tra i motivi di comportamento razzista e di discriminazione razziale punibili ai sensi del Codice penale e che la divulgazione pubblica o la distribuzione o la produzione o la conservazione a fini di diffusione o di distribuzione al pubblico, a scopo razzista, di scritti, immagini, o altro materiale che costituisca un incitamento alla discriminazione razziale e alla violenza razziale sia riconosciuta come reato penale;
3) di valutare l'efficacia delle disposizioni per combattere la diffusione di idee razziste e l'incitamento a commettere o il fatto di commettere atti discriminatori motivati dall'odio;
4) di introdurre disposizioni nel Codice penale per criminalizzare l'ingiuria e la diffamazione o le minacce proferite in pubblico contro una persona o un gruppo di

[50] Pubblicate **il 6 giugno 2019.**

persone per motivi basati sulla razza, il colore, la lingua, la religione, la nazionalità o l'origine nazionale o etnica;

5) di completare quanto prima la legge per il contrasto e la prevenzione del genocidio, dei crimini contro l'umanità e dei crimini di guerra (in tema di contrasto e repressione del genocidio, si ricorda che è stata approvata la Legge n. 115/16 del 16 giugno 2016);

6) di introdurre disposizioni di legge che vietino la discriminazione basata non soltanto su motivi quali la "razza", la religione e l'origine etnica, ma anche la lingua, il colore e la nazionalità e b) accertarsi che tutte le organizzazioni attive nel campo della lotta contro il razzismo e la discriminazione razziale possano agire in giudizio a nome delle presunte vittime di tali fenomeni o nei casi di discriminazione collettiva;

7) di garantire la completa indipendenza de jure e de facto dell'UNAR, dotandola di tutte le risorse umane e finanziarie necessarie alla sua missione;

8) di predisporre senza indugio un metodo di raccolta dei dati sugli episodi collegati al discorso dell'odio, suddivisi nelle varie categorie della motivazione razziale e delle vittime, e di pubblicare regolarmente i risultati, con le informazioni riguardanti il numero di procedimenti penali, le ragioni per cui non sono stati avviati e l'esito dei relativi procedimenti giudiziari;

9) di completare quanto prima l'iter di ratifica del Protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la criminalizzazione degli atti di razzismo o xenofobia commessi a mezzo di sistemi informatici (in corso di esame in Parlamento il DDL di ratifica, all'esame della Camera, AC 1094).

10) di impegnarsi maggiormente per sensibilizzare i giovani alla tolleranza e al reciproco rispetto e metterli in guardia sui pericoli di utilizzare internet per diffondere il discorso di incitamento all'odio e contenuti offensivi. In particolare, dovrebbero accertarsi, sia nell'ambito del Piano d'azione contro il razzismo, la xenofobia e l'intolleranza che nelle disposizioni della Legge n. 107/15 sulla "buona scuola", che tutti i giovani ricevano le informazioni e il supporto di cui hanno bisogno per un utilizzo responsabile dei social.

11) di adottare le misure legislative necessarie per fornire un supporto specializzato alle vittime dei crimini dettati dall'odio, se del caso adattando i servizi già esistenti per le vittime di altri reati.

12) di istituire un organismo indipendente dalla polizia e dalla procura incaricato di indagare sulle presunte violazioni dei diritti umani da parte delle forze di polizia, ivi compresi tutti i presunti episodi di discriminazione razziale o di comportamenti motivati dall'odio razziale.

13) di completare l'iter legislativo per la modifica della legislazione sull'acquisto della cittadinanza al più presto possibile, al fine di facilitare la naturalizzazione di minori stranieri nati o che hanno frequentato la scuola in Italia, ed evitare che ci siano bambini apolidi.

14) di garantire che l'estensione del Piano "Identità e Incontro" preveda una valutazione di tutti i progetti di integrazione avviati negli ultimi anni, sulla base di dati precisi sui tassi di integrazione raggiunti nei vari settori della vita sociale.

15) di garantire che, nel contesto dei rapporti tra Stato e regioni, venga reso disponibile un supporto adeguato per il processo di integrazione in ogni regione, tra gli altri rendendo più effettivo l'uso dei Fondi Strutturali dell'Unione Europea.

16) di completare la raccolta di dati statistici in tutte le aree relative all'integrazione dei Rom per poter stabilire un ordine di priorità per l'attuazione della Strategia nazionale per l'integrazione dei Rom; di completare l'istituzione di gruppi di lavoro regionali; di stanziare un finanziamento speciale per la Strategia; e di fornire all'UNAR le risorse necessarie per poter coordinare, monitorare e valutare la Strategia.

17) di garantire a tutti i Rom atti ad essere sgomberati dalle loro case di godere della piena protezione delle garanzie del diritto internazionale in materia.

18) di estendere i poteri dell'UNAR affinché le disposizioni giuridiche pertinenti coprano chiaramente la discriminazione basata, tra l'altro, sull'orientamento sessuale e l'identità di genere.

19) di attuare nelle scuole misure atte a promuovere la tolleranza ed il rispetto reciproci a scuola, a prescindere dall'orientamento sessuale o dall'identità di genere.

In particolare, i profili su cui si soffermano le **conclusioni del 2019** riguardano:

a) la **garanzia della completa indipendenza** *de jure* e *de facto* dell'**UNAR** (punto 7). L'ECRI rimarca come, in ragione della collocazione presso il Dipartimento Pari Opportunità della Presidenza del Consiglio, l'UNAR non osservi pienamente il requisito dell'indipendenza degli organismi specializzati nel contrasto al razzismo e all'intolleranza, né appare sufficiente ipotizzare, cosa che peraltro in Italia si tenta di fare dal 1994, la creazione di una Commissione nazionale per la promozione e la protezione dei diritti umani, come prevede la pdl Quartapelle (855) abbinata alla pdl Scagliusi (1323), al momento all'esame della I Commissione affari costituzionali della Camera dei Deputati.

b) l'introduzione di **disposizioni** di legge **che vietino la discriminazione basata** non soltanto su motivi quali la "razza", la religione e l'origine etnica, ma anche su: la lingua, il colore e la nazionalità, estendendo a tal fine i poteri dell'UNAR (punto 6). L'ECRI pur prendendo atto che, in particolare con l'adozione nel 2015 del Piano Nazionale d'Azione contro razzismo, xenofobia e intolleranza, sia stato considerevolmente ampliato il raggio di protezione contro quasi tutte le forme di discriminazione, sottolinea **l'assenza di un chiaro quadro legislativo di riferimento** che finisce per incidere sulla stessa effettività dell'azione dell'UNAR.

c) l'introduzione e l'applicazione **nelle scuole** di ogni grado di **misure volte a favorire tolleranza e rispetto reciproci**, tra differenti orientamenti sessuali e identità di genere (punto 19).

Al riguardo, le Autorità italiane hanno osservato che nell'ambito dell'attuazione della legge n.107 del 2015 (c.d. Legge sulla Buona Scuola) sono state adottate misure volte a favorire una sempre maggiore tolleranza reciproca. L'ECRI ha tuttavia osservato come l'attuazione di tali misure sia spesso affidata ad iniziative

volontarie di associazioni, sebbene queste ultime ricevano risorse dalle autorità ministeriali. Inoltre, tali attività extracurriculari incontrano talvolta forti resistenze da parte dei parenti, delle scuole e delle autorità regionali. Per tali ragioni, ECRI ritiene che anche tale raccomandazione sia stata ad oggi soltanto parzialmente attuata.

La campagna No Hate Speech Movement

Il Consiglio d'Europa ha condotto, dal 2012 al 2014, una Campagna contro l'istigazione all'odio *online* (*No Hate Speech Movement*), mirante a combattere il razzismo e tutte le altre forme di discriminazione e di istigazione all'odio *online*, rivolta in particolare ai giovani.

La Camera dei deputati ha contribuito al tale Campagna organizzando, il 10 giugno 2013 a Montecitorio, il Seminario parlamentare "*Parole libere o parole d'odio. Prevenzione della violenza online*".

Alla fine di tale Campagna, l'Assemblea parlamentare del Consiglio d'Europa ha adottato il 28 gennaio 2014 la Risoluzione 1967 e la Raccomandazione 2032 "*Una strategia per la prevenzione del razzismo e dell'intolleranza in Europa*"[51], chiedendo un approccio strategico e non frammentario e sottolineando il ruolo specifico svolto da legislatori e responsabili politici.

Relatore generale sul razzismo e l'intolleranza

A seguito all'adozione della richiamata **Risoluzione 1967** del **28 gennaio 2014**, l'Assemblea parlamentare ha chiesto di sostenere la campagna *"No Hate Speech"* , organizzando campagne su larga scala con l'utilizzo di media e di internet, di promuovere la pubblicazione di materiale educativo rivolto in particolare alle scuole, di provvedere ad una specifica formazione delle forze dell'ordine.

L'Assemblea ha quindi istituito il mandato di **Relatore generale sul razzismo e l'intolleranza**, con il compito di coordinare il lavoro della **"Alleanza contro l'odio"**, costituendo *network* di parlamentari che si impegnano a *"prendere una posizione pubblica, ferma e proattiva contro il razzismo, l'odio e intolleranza, quali che siano le ragioni, e come si manifestano"*. Il Relatore generale è aiutato nei suoi compiti dal Bureau della Commissione uguaglianza e non discriminazione dell'Assemblea Parlamentare del CdE.

All'Alleanza possono aderire anche i membri delle delegazioni dell'Assemblea parlamentare. **Al momento i parlamentari che hanno aderito alla rete sono circa 40**. L'Alleanza è aperta, inoltre, ai membri dei Paesi non membri del CdE

[51] Relatore della Commissione sull'uguaglianza e la non discriminazione, Jonas Gunnarsson (Svezia, SOC).

(*Partners* per la democrazia e Osservatori). L'impegno viene formalizzato con la sottoscrizione della ***Charter of Commitments*** dell'Alleanza. Il Messico partecipa come osservatore con un parlamentare.

L'incarico di Relatore Generale, e di conseguenza la Presidenza del *Network,* è stata attribuita, nell'ottobre del 2017 a Gabriela HEINRICH (SOC). Del *Network* fa parte, per l'Italia, il **senatore Roberto Rampi**.

Contrasto alle fake news e "guerra ibrida" nelle attività dell'Assemblea parlamentare della NATO

(a cura del Servizio Rapporti Internazionali)

Nell'ambito dell'Assemblea NATO il concetto di *fake news* viene analizzato in connessione alle nuove strategie di "**guerra ibrida**" messe in campo dalla Russia. Di questo tema l'Assemblea NATO si è occupata in occasione della Sessione annuale di Halifax (novembre 2018) dove sono stati presentati due rapporti ***Aggiornamento sulla lotta alle minacce ibride della Russia*** e ***L'ingerenza russa nelle elezioni e nei referendum dei Paesi all'Alleanza***.

Con riferimento alla prima relazione (Doc. 166 CDS 18, Rel. lord Jopling, Regno Unito), essa mira a far conoscere meglio le attività ibride della Russia, che includono interferenze politiche, un basso utilizzo della forza, spionaggio, criminalità e corruzione, disinformazione e propaganda, attacchi cibernetici e pressioni economiche, oltre a mostrare come alcune di queste tecniche si rafforzano e si integrano a vicenda.

Sotto la voce "guerra ibrida" si possono raccogliere **un ampio spettro di attività**, tra cui anche la disinformazione e la propaganda abilmente utilizzati dalla Russia per diffondere fake news dai contenuti socialmente divisivi in Occidente.

La **relazione** esamina le contromisure adottate dalla NATO, dall'Unione europea e a livello nazionale dai membri dell'Alleanza e non. Tra le iniziative nazionali, il relatore sottolinea che la minaccia ibrida può essere contrastata oltre che a livello governativo, anche in campo civile, accademico e a livello di mezzi di informazione.

Il Relatore rivolge la sua attenzione soprattutto ai social media e ai giganti della tecnologia come Facebook, Microsoft, Twitter e You Tube, al momento più concentrate nella rimozione di contenuti legati al terrorismo. Il relatore è tuttavia consapevole che nello spazio cyber l'assenza di confini nazionali rende difficile al legislatore nazionale realizzare dei cambiamenti significativi.

Nella **seconda relazione** (Doc. 181 STC 18, rel. Susan DAVIS, Stati Uniti), sono esaminati i casi recenti di presunte interferenze negli Stati Uniti, nel Regno Unito, in Francia, in Germania e in Spagna. Molte di queste azioni sono la prosecuzione del tentativo della Russia di dividere, destabilizzare e in ogni caso minacciare i membri dell'Alleanza. Esse hanno per oggetto le istituzioni politiche e i media, con attacchi informatici e fughe di notizie. I singoli utenti dei social media si trovano di fronte a informazioni errate e a campagne di propaganda ben coordinate.

Alla luce della novità di questo problema e della difficoltà di trovare una risposta, il progetto di relazione sintetizza alcuni casi recenti che hanno avuto per oggetto infrastrutture elettorali, sistemi informatici e social media. **La Relatrice solleva questioni importanti sulle responsabilità delle società di social media** e sul ruolo dei governi nel promuovere un'attività responsabile sulle piattaforme degli stessi social media. Il testo si chiude sottolineando che la Russia probabilmente continuerà la propria azione di minaccia nei confronti delle istituzioni democratiche e si appella ai legislatori affinché promuovano il dialogo su come rispondere a presunte interferenze all'interno dei loro stessi Paesi.

In tre diversi paragrafi del rapporto vi sono citazioni riguardanti l'Italia.

Il par. 66, relativo ai tentativi recenti, in particolare svolti da Facebook, di produrre un controllo dei fatti e una informazione agli utenti sui contenuti falsi, segnala che prima delle elezioni parlamentari del 2018 in Italia, Facebook si è associato a organizzazioni attive nel fact-checking per avvisare gli utenti che avessero condiviso false informazioni sulle scoperte fatte dai fact-checker's.

Il par. 70, incentrato sugli sforzi fatti da task forces governative, istituite appositamente per contrastare la disinformazione, riporta che in vista delle elezioni parlamentari del 2018, il governo italiano aveva un portale Internet che permetteva ai cittadini di segnalare i falsi contenuti online.

Il par. 71, relativo alla necessità che gli sforzi si concentrino anche sulla società civile e sulla promozione dell'educazione civica e dell'alfabetizzazione mediatica, riporta fra gli altri l'esempio dell'Italia, dove il Ministero dell'Istruzione ha presentato dei corsi destinati a insegnare agli studenti italiani come identificare le notizie false e capire come i social network possono essere manipolati.

Dal dibattito in Commissione sono scaturite rispettivamente **la risoluzione 445** "**Aggiornare le risposte alle tattiche ibride della Russia**" e **la risoluzione 452** "**Proteggere le elezioni nei Paesi dell'Alleanza**", entrambe approvate dall'Assemblea NATO e trasmesse al Parlamento italiano.