dossier

5 novembre 2021

Documentazione per le Commissioni

RIUNIONI INTERPARLAMENTARI

Riunione interparlamentare della Commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione (INGE) del Parlamento europeo sul tema "Rispondere alle interferenze straniere in cooperazione con democrazie che la pensano allo stesso modo"

Videoconferenza, 9 novembre 2021

Senato della Repubblica

Camera dei deputati

dossier

XVIII LEGISLATURA

Senato della Repubblica

Camera dei deputati

XVIII LEGISLATURA

Documentazione per le Commissioni

RIUNIONI INTERPARLAMENTARI

Riunione interparlamentare della Commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione (INGE) del Parlamento europeo sul tema “Rispondere alle interferenze straniere in cooperazione con democrazie che la pensano allo stesso modo”

Videoconferenza, 9 novembre 2021

SENATO DELLA REPUBBLICA

SERVIZIO STUDI
DOSSIER EUROPEI

N. 142

CAMERA DEI DEPUTATI

UFFICIO RAPPORTI CON
L’UNIONE EUROPEA

N. 71

Senato della Repubblica

Servizio Studi

TEL. 06 6706-2451 - studi1@senato.it - @SR_Studi

Dossier europei n. 142

Camera dei deputati

Ufficio rapporti con l'Unione europea

Tel. 06-6760-2145 - cdrue@camera.it - @CD_europa

Dossier n. 71

La documentazione dei Servizi e degli Uffici del Senato della Repubblica e della Camera dei deputati è destinata alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. Si declina ogni responsabilità per la loro eventuale utilizzazione o riproduzione per fini non consentiti dalla legge. I contenuti originali possono essere riprodotti, nel rispetto della legge, a condizione che sia citata la fonte.

I N D I C E

FOREIGN INTERFERENCE
In all Democratic Processes in The European Union, including Disinformation

TUESDAY,
9 NOVEMBER 2021
13.45 TO 15.45
AND 16.15 TO 18.15
ROOM Spaak 1A002

EUROPEAN PARLIAMENT,
BRUSSELS
& REMOTE PARTICIPATION

INGE

AGENDA

EUROPEAN PARLIAMENT - NATIONAL PARLIAMENTS

Inter-parliamentary Committee Meeting

Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation

With the support of the Directorate
for Relations with National Parliaments

European Parliament

NATIONAL PARLIAMENTS
PARLEMENTS NATIONAUX

Order of Business

13.45 - 13.50 **Introductory remarks by Mr Raphaël GLUCKSMANN**
Chair of the Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE), European Parliament

Session 1: Foreign Interference in Democratic Processes in the EU

13.50 - 14.00 **Introduction by Mr Stefano SANNINO**
Secretary-General of the European External Action Service

14.00 - 14.15 **Presentation of the INGE draft report by Ms Sandra KALNIETE**
EPP, LV and INGE Rapporteur

14.15 - 14.35 **Initial comments by the INGE Shadow Rapporteurs**

14.35 - 15.35 **Exchange of views with INGE MEPs and national MPs**

15.35 - 15.45 **Closing remarks by Ms Sandra KALNIETE**
EPP, LV and INGE Rapporteur

Session 2: Responding to Foreign Interference in Cooperation with Like-Minded Democracies

16.15 - 16.45 **Video message by Senator James PATERSON**
Chair of the Australian Parliament's Joint Committee on Intelligence and Security

Keynote speech by Mr Laurynas KASČIŪNAS
Chair of the Lithuanian Seimas Committee on National Security and Defence

Keynote speech by Ms Lia QUARTAPELLE PROCOPIO
Member of the Italian Parliament's Committee on Foreign and European Community Affairs

16.45 - 18.05 **Exchange of views with INGE MEPs and national MPs**

18.05 - 18.15 **Closing remarks by Mr Raphaël GLUCKSMANN**
Chair of INGE

* * *

The event will be webstreamed on the European Parliament website.

IL PROGRAMMA DELLA RIUNIONE

Il Presidente della Commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione (INGE) del Parlamento europeo, Raphaël Glucksmann (S & D, Francia), ha invitato i parlamenti nazionali a partecipare alla riunione interparlamentare, che si svolgerà in videoconferenza il 9 novembre 2021, sul tema "Rispondere alle interferenze straniere in cooperazione con le democrazie affini".

In base alla bozza di programma, l'incontro sarà articolato nelle seguenti sessioni di lavoro: 1) Le interferenze straniere nei processi democratici nell'Unione europea; 2) Rispondere alle interferenze straniere in cooperazione con le democrazie affini.

I tentativi da parte di attori statali e non statali di interferire nella vita democratica e politica nell'Ue e nei suoi Stati membri sono diventati sempre più comuni, come parte di una tendenza più ampia sperimentata dalle democrazie di tutto il mondo. La Commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Ue è stata istituita per esaminare le diverse forme di interferenza straniera, che vanno dalle campagne di disinformazione agli attacchi informatici e ai finanziamenti illeciti.

La riunione dovrebbe fungere da forum *per un dibattito e uno scambio di informazioni e migliori pratiche su come i diversi Paesi dell'Ue e non Ue - fra cui Stati Uniti, Canada e Australia - affrontano le minacce ibride a livello nazionale e multilaterale e le sfide poste dalle interferenze straniere. L'incontro dovrebbe essere anche un'occasione per approfondire il dialogo sulle ingerenze straniere fra Parlamento europeo, parlamenti nazionali e internazionali in preparazione del vertice internazionale per la democrazia.*

LA COMMISSIONE SPECIALE SULLE INGERENZE STRANIERE IN TUTTI I PROCESSI DEMOCRATICI NELL'UNIONE EUROPEA, INCLUSA LA DISINFORMAZIONE (INGE)

La Commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, compresa la disinformazione (INGE) è stata istituita - con la decisione del Parlamento europeo del 18 giugno 2020[1] - al fine di contrastare gli Stati che cercano di interferire nelle istituzioni e nei processi democratici dell'Ue e dei suoi Stati membri.

Gli europarlamentari italiani che partecipano alla Commissione sono i seguenti: Marco Dreosto (ID); Salvatore de Meo (PPE); Franco Roberti (S&D); Nicola Procaccini (ECR); Silvia Sardone (ID).

Il presidente della Commissione INGE, **Raphaël Glucksmann**, ha dichiarato che intende lavorare al fine di valutare il livello di queste minacce nei diversi ambiti previsti dal mandato.

I lavori della commissione speciale dovrebbero sfociare nell'elaborazione di un "approccio comune, globale e a lungo termine" inteso a far fronte alle manifestazioni di ingerenze straniere nelle istituzioni e nei processi democratici dell'Ue e dei suoi Stati membri, non solo nel periodo che precede tutte le principali **elezioni nazionali ed europee**, ma in maniera continua in tutta l'Ue, sotto molteplici forme, fra cui **campagne di disinformazione** sui media tradizionali e sui social media volte a plasmare l'opinione pubblica, **attacchi informatici mirati a infrastrutture critiche**, sostegno finanziario diretto e indiretto o **coercizione economica** nei confronti di soggetti politici e **atti di sovversione** nei confronti della società civile.

La citata decisione istitutiva precisa le **attribuzioni** della commissione speciale INGE, che dovrà:

a) condurre un'analisi approfondita delle indagini secondo cui sono state violate o eluse **norme elettorali** fondamentali, in particolare le disposizioni vigenti in materia di trasparenza del finanziamento delle campagne elettorali,

[1] L'articolo 207 "Commissioni speciali" del Regolamento del Parlamento europeo prevede che, su proposta della Conferenza dei presidenti, il Parlamento può in qualsiasi momento costituire commissioni speciali le cui attribuzioni, la cui composizione numerica e il cui mandato sono fissati contemporaneamente alla decisione della loro costituzione. Il mandato delle commissioni speciali non può superare i dodici mesi, a meno che il Parlamento non prolunghi questo periodo alla sua scadenza. Le commissioni speciali non sono titolate a formulare pareri destinati ad altre commissioni.

con presunti finanziamenti politici provenienti da varie forme legali e illegali di società di comodo e donatori che utilizzano prestanome provenienti da Paesi terzi;

b) individuare potenziali settori in cui siano necessarie misure legislative e non legislative che possano indurre le **piattaforme dei *social media*** a intervenire al fine di contrassegnare i contenuti condivisi da sistemi automatici (*bot*), di rivedere gli algoritmi per renderli il più possibile trasparenti quanto ai criteri di pubblicazione, priorità, condivisione, retrocessione e rimozione di contenuti, e di chiudere i profili di coloro che intraprendono i cd. "comportamenti non autentici coordinati *online*" o attività illecite per nuocere sistematicamente ai processi democratici o alimentare l'odio, senza per questo compromettere la libertà di espressione;

c) contribuire al dibattito in corso su come rafforzare il **contrasto alle ingerenze straniere** in tutti i processi democratici nell'Unione europea, compresa la disinformazione, non esclusivamente da parte delle autorità pubbliche, ma anche in cooperazione con le imprese del settore tecnologico e dei *social media* e il settore privato in generale, al fine di sensibilizzare in merito al ruolo, ai doveri e alla responsabilità che tali attori hanno nella lotta alle ingerenze straniere, sempre senza compromettere la libertà di espressione;

d) valutare azioni nazionali atte a imporre rigorose restrizioni alle **fonti di finanziamento politico**, dal momento che attori stranieri hanno trovato modalità legali e illegali per eludere le legislazioni nazionali e hanno offerto un sostegno occulto ai propri alleati contraendo prestiti presso banche estere, fornendo oggetti di valore in natura, sottoscrivendo contratti commerciali e di acquisto e ricorrendo a società di comodo, organizzazioni senza scopo di lucro, cittadini donatori prestanome, tecnologie emergenti in grado di assicurare l'anonimato, pubblicità *online* e organi d'informazione estremisti *online*, nonché facilitando attività finanziarie. La commissione dovrà altresì individuare possibili settori in cui siano necessarie azioni in materia di finanziamento dei partiti politici e delle campagne politiche;

e) suggerire un'azione coordinata a livello dell'Ue per affrontare le **minacce ibride**, fra cui gli attacchi informatici rivolti a obiettivi militari e non militari, le operazioni di *hack-and-leak* (intrusione in siti informatici e diffusione di dati riservati) ai danni di legislatori, funzionari pubblici, giornalisti, candidati e partiti politici, come pure lo spionaggio informatico finalizzato al furto di proprietà intellettuale delle imprese e al furto di dati

sensibili dei cittadini. La commissione dovrà inoltre valutare l'aspetto relativo alla sicurezza di tali minacce, che possono avere gravi implicazioni politiche, economiche e sociali per i cittadini europei;

f) esaminare la **dipendenza dell'Ue dalle tecnologie straniere nelle catene di approvvigionamento delle infrastrutture critiche**, compresa l'infrastruttura di internet, e in materia di *hardware*, *software*, applicazioni e servizi, e individuare le azioni necessarie per rafforzare la capacità di contrastare la comunicazione strategica da parte di soggetti terzi ostili e di scambiare informazioni e migliori prassi in tale ambito. La commissione dovrà pertanto sostenere e incoraggiare il coordinamento fra gli Stati membri per quanto riguarda lo scambio di informazioni, conoscenze e buone prassi al fine di contrastare le minacce e affrontare le attuali carenze;

g) individuare, valutare e proporre modalità per affrontare le **violazioni della sicurezza all'interno delle istituzioni dell'Ue**;

h) contrastare le campagne di informazione e la comunicazione strategica di **Paesi terzi malevoli**, comprese quelle che si appoggiano ad attori e organizzazioni stabiliti in Europa, che ledono gli obiettivi dell'Unione europea e che sono concepite per influenzare l'opinione pubblica europea al fine di ostacolare il raggiungimento di una **posizione comune dell'Ue**, anche per quanto riguarda le questioni inerenti alla politica estera e di sicurezza comune (PESC) e alla politica di sicurezza e di difesa comune (PSDC);

i) chiedere la **collaborazione di tutti i servizi e le istituzioni competenti**, a livello dell'Ue e dei suoi Stati membri, che reputi pertinenti ed efficaci per l'adempimento del suo mandato.

DIBATTITO TEMATICO I - LE INGERENZE STRANIERE NEI PROCESSI DEMOCRATICI NELL'UE

Nell'istituire la Commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione, il Parlamento europeo le ha conferito l'incarico di elaborare un approccio a lungo termine inteso a far fronte alle ingerenze straniere nelle istituzioni e nei processi democratici dell'Ue e dei suoi Stati membri.

La commissione speciale presenterà una relazione finale (recante una **proposta** di **risoluzione**) in cui figureranno conclusioni di fatto e raccomandazioni in merito alle misure e alle iniziative da adottare. È stata designata come relatrice **Sandra Kalniete** (EPP, Lettonia).

La relatrice riferisce che il lavoro della commissione si fonda su una stretta cooperazione fra i gruppi politici (i coordinatori hanno deciso di comune accordo con il presidente quali esperti invitare e quali studi commissionare), e di aver regolarmente consultato i relatori ombra durante l'elaborazione del documento.

Dal punto di vista tematico, è stata operata una distinzione fra la fase di diagnosi, nel corso della quale sono stati invitati esperti, e la fase di individuazione delle soluzioni. Sulla base del mandato, sono state organizzate diverse audizioni sulle ingerenze nella sfera pubblica e privata e sono stati analizzati i metodi utilizzati dai diversi attori stranieri. Nella fase dedicata all'individuazione delle soluzioni, la commissione INGE ha tentato di individuare possibili strumenti e strategie per prevenire e contrastare i problemi rilevati. Per la formulazione delle raccomandazioni sono state inoltre presentate due interrogazioni con richiesta di risposta orale: nel luglio 2021 è stato chiesto al VP/AR Josep Borrell come intendeva porre rimedio alla mancanza di risorse e di mandato per le *task force* della *StratCom* del SEAE e alla mancanza di sanzioni adeguate nei confronti di attori stranieri che commettono ingerenze; nell'ottobre 2021 è stato chiesto alla vicepresidente della Commissione europea Věra Jourová come intende garantire che la mancanza di coordinamento fra i diversi settori e livelli politici non aumenti l'esposizione alle ingerenze straniere e come intende migliorare la trasparenza degli algoritmi e sostenere l'alfabetizzazione mediatica.

Per redigere la relazione, la relatrice ha inoltre approntato quattro documenti di lavoro: sullo stato delle ingerenze straniere nell'Unione europea, inclusa la disinformazione; sul finanziamento occulto di attività politiche da parte di donatori stranieri; sulle ingerenze straniere per mezzo delle piattaforme *online*; sul rafforzamento della resilienza dell'Ue contro le minacce ibride.

Alla luce della natura intersettoriale del mandato, la commissione INGE ha invitato cinque commissari per discutere di aspetti diversi delle ingerenze straniere:

Věra Jourová, vicepresidente della Commissione per i Valori e la trasparenza; Margaritis Schinas, vicepresidente per la Promozione dello stile di vita europeo; Josep Borrell, vicepresidente della Commissione/alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza; Thierry Breton, commissario per il Mercato interno; Margrethe Vestager, vicepresidente esecutiva dell'Ue per Un'Europa pronta per l'era digitale e commissaria per la Concorrenza. Sono state inoltre condotte diverse discussioni con il personale della Commissione e del Servizio europeo per l'azione esterna ed è stata indetta una riunione speciale, insieme alla commissione CONT, con la Corte dei conti europea in merito alla sua relazione speciale n. 09/2021: "La disinformazione nell'Ue: combattuta ma non vinta".

Il progetto di relazione - presentato il **18 ottobre 2021 -** delinea un quadro della situazione, della portata e dell'estrema complessità della miriade di forme assunte dalle operazioni di ingerenza aggressive concepite e finanziate da attori stranieri nei confronti dell'Ue.

La relatrice riferisce di aver preso atto, con una certa preoccupazione, della rapida capacità di adattamento, della volatilità e dell'accelerazione di tale fenomeno, attraverso nuovi attori, nuove narrazioni e nuovi strumenti emersi nell'arco di un solo anno. Fra questi si annoverano, infatti: campagne di disinformazione su nuova scala legate al Covid-19; attacchi informatici contro le autorità pubbliche, comprese le infrastrutture di sanità pubblica; strategie di ingerenza che prevedono l'*elite capture* e attività di *lobbying* industriale; il finanziamento occulto delle attività politiche; il controllo di centri accademici e culturali; la strumentalizzazione delle diaspore nazionali.

La relatrice riferisce tuttavia che si è assistito anche alla diffusione di una maggiore consapevolezza in merito alla fondamentale importanza di tali aspetti, e il riconoscimento del fatto che l'Ue e i suoi Stati membri dovrebbero rapidamente introdurre vere e proprie **politiche per la resilienza e strumenti di deterrenza**, sulla base di un approccio che coinvolga la società nel suo insieme, che consentano di affrontare tutti i tipi di minacce ibride e di attacchi, tutelando in tal modo il **funzionamento sostenibile della democrazia**.

Nella risoluzione si invita quindi la **Commissione europea** a proporre, e i **colegislatori** e gli **Stati membri** a sostenere, una **strategia multilivello e intersettoriale** e a stanziare **risorse finanziarie adeguate**, al fine di dotare l'Ue e gli Stati membri di politiche di resilienza e strumenti di deterrenza adeguati.

Tale strategia dovrebbe fondarsi su un approccio basato sui rischi, che coinvolga la società e i governi nel loro insieme e riguardi in particolare gli aspetti di seguito illustrati.

1) Rafforzamento della resilienza dell'Ue attraverso la consapevolezza della situazione, l'alfabetizzazione mediatica e l'istruzione.

Per ottenere la consapevolezza della situazione, la relatrice ritiene importante seguire due direzioni: monitorare, mappare e analizzare i diversi tentativi di ingerenza, in modo da comprendere pienamente la minaccia; assicurarsi che gli interessati siano a conoscenza di tale analisi.

A livello europeo, la relatrice apprezza in particolare il lavoro condotto dalle *task force* della StratCom del **Servizio europeo per l'azione esterna** (SEAE).

Al fine di promuovere la collaborazione in materia di *intelligence*, analisi, condivisione delle migliori pratiche e sensibilizzazione in merito alla manipolazione delle informazioni e alle ingerenze straniere, la risoluzione invita le istituzioni dell'Ue a sviluppare ulteriormente l'importante lavoro della divisione StratCom del SEAE, con le sue *task force*, il Centro Ue di analisi dell'*intelligence* (EU INTCEN) e la cellula dell'Ue per l'analisi delle minacce ibride, il sistema di allarme rapido, la consolidata cooperazione a livello amministrativo fra il SEAE, la Commissione e il Parlamento, la rete contro la disinformazione guidata dalla Commissione, la *task force* amministrativa contro la disinformazione del Parlamento e la cooperazione in corso con la Nato, il G7, la società civile e l'industria privata. Ribadisce tuttavia l'esigenza di conferire al SEAE il mandato di monitorare e contrastare la manipolazione delle informazioni e le ingerenze al di fuori delle regioni attualmente coperte dalle tre *task force*, e di dotarlo delle risorse necessarie; chiede inoltre con particolare urgenza di garantire che il SEAE disponga di capacità adeguate per far fronte alla manipolazione delle informazioni e alle ingerenze da parte della Cina.

La risoluzione:

- esprime apprezzamento per l'indispensabile attività di ricerca e le numerose iniziative di sensibilizzazione e alfabetizzazione mediatica e digitale creative e di successo promosse da singole persone, scuole, università, organizzazioni operanti nel settore dei media, istituzioni pubbliche e organizzazioni della società civile. In tale contesto, invita le istituzioni dell'Ue e gli Stati membri, a tutti i livelli amministrativi, a individuare i settori a rischio di tentativi di ingerenza e a fornire al personale che lavora in questi settori una formazione ed esercitazioni regolari su come rilevare ed evitare i tentativi di ingerenza e sottolinea

che tali sforzi trarrebbero giovamento da un formato standardizzato stabilito dall'Ue;

- chiede **fonti di finanziamento pubblico affidabili e sostenibili** per i verificatori di fatti, i ricercatori, i mezzi di comunicazione di qualità e i giornalisti indipendenti, e per le ONG che indagano sui casi di manipolazione delle informazioni e ingerenze, promuovono l'alfabetizzazione mediatica e altri strumenti per la responsabilizzazione dei cittadini. Accoglie con favore, a tale proposito, le nuove possibilità di finanziamento per l'**alfabetizzazione mediatica** previste nel quadro del programma Europa creativa 2021-2027, nonché le iniziative intraprese dal SEAE, dalla Commissione e dall'amministrazione del Parlamento, quali gli eventi di formazione e sensibilizzazione per giornalisti, insegnanti, influencer, studenti e visitatori, sia *online* che *offline*, a Bruxelles e in altre capitali dell'Ue, e raccomanda di svilupparle ulteriormente;

- esprime grave preoccupazione per le molestie e le **minacce nei confronti dei giornalisti** e invita la Commissione europea a presentare tempestivamente proposte concrete e ambiziose per la sicurezza di giornalisti e professionisti dei mezzi di comunicazione, come previsto dal Piano d'azione per la democrazia europea.

2) Ingerenze straniere per mezzo delle piattaforme *online*.

La relatrice ritiene che l'attuale sistema di divulgazione delle informazioni per mezzo delle piattaforme crei un "clima *online* contorto" in cui la disinformazione e altri tipi di manipolazione delle informazioni possono prosperare. Alla luce delle numerose discussioni avute con gli esperti, la relatrice è giunta alla conclusione che l'attuale metodo di autoregolamentazione non funziona e deve essere sostituito da **norme vincolanti.** Pertanto la risoluzione:

- chiede l'adozione di una regolamentazione che obblighi le piattaforme a fare la propria parte per limitare la manipolazione delle informazioni e le ingerenze, ad esempio utilizzando indicazioni in riferimento ai reali autori dietro agli account, limitando gli account utilizzati regolarmente per diffondere la disinformazione o che violano ripetutamente i termini di utilizzo della piattaforma, sospendendo gli account non autentici utilizzati per campagne di ingerenza coordinate o demonetizzando i siti che diffondono la disinformazione;

- accoglie con favore la proposta di revisione del Codice di buone pratiche sulla disinformazione e le proposte riguardanti la **legge sui servizi digitali**, la **legge sui mercati digitali** e le altre misure legate al piano d'azione per la democrazia europea;
- chiede l'adozione di **norme europee vincolanti** che impongano alle piattaforme di: individuare, valutare e mitigare regolarmente i rischi di manipolazione delle informazioni e di ingerenza associati all'uso dei loro servizi; istituire sistemi di monitoraggio dell'utilizzo dei loro servizi, **almeno in tutte le lingue nazionali e regionali ufficiali**, al fine di rilevare la manipolazione delle informazioni e le ingerenze e di segnalare le sospette ingerenze alle autorità competenti, aumentando i costi sostenuti dai soggetti che favoriscono azioni di questo tipo;
- sottolinea la generale necessità di **trasparenza** per quanto riguarda la persona fisica o giuridica dietro ai contenuti *online* e agli account;
- invita le piattaforme a introdurre meccanismi per individuare e sospendere gli account falsi connessi alle cd. **"operazioni di influenza coordinata"**.

3) Infrastrutture critiche e settori strategici.

Il progetto di relazione sottolinea che le infrastrutture critiche sono essenziali per il funzionamento dell'economia e della società. Data la loro natura interconnessa e transfrontaliera, al fine di garantire una migliore protezione dei settori critici, sarà necessario intraprendere sforzi congiunti e coordinati in tutti i settori e a diversi livelli (dell'Unione, nazionale, regionale e locale). Il quadro attualmente in vigore dovrà pertanto essere rivisto.

A tale riguardo, la risoluzione:

- accoglie con favore la proposta di direttiva sulla **resilienza dei soggetti critici**. È tuttavia del parere che l'elenco delle infrastrutture critiche potrebbe essere esteso ai **mezzi di comunicazione** e alle **infrastrutture per le elezioni**, vista la loro importanza fondamentale nel garantire il funzionamento dell'Ue e degli Stati membri, assicurando una certa flessibilità in relazione all'aggiunta nell'elenco di **nuovi settori strategici** da proteggere. Raccomanda inoltre di adottare un approccio estremamente flessibile che consenta di aggiornare e modificare rapidamente la direttiva proposta, sulla base delle valutazioni delle minacce, dei rischi e delle vulnerabilità

condotte dal Centro comune di ricerca in collaborazione con l'INTCEN del SEAE;

- ritiene che l'Ue e gli Stati membri debbano fornire alternative di finanziamento in modo da impedire che ampie parti delle loro infrastrutture critiche finiscano nelle mani di Paesi terzi, come avvenuto nel caso del porto del Pireo in Grecia e come sta avvenendo con gli investimenti cinesi nella posa in opera di cavi sottomarini nel Mar Baltico, nel Mediterraneo e nel Mar Artico. Accoglie pertanto con favore il regolamento (UE) 2019/452 sul **controllo degli investimenti esteri diretti nell'Unione** quale importante strumento per coordinare le azioni degli Stati membri in relazione agli investimenti stranieri nelle infrastrutture critiche, e invita a elaborare un quadro normativo più rigoroso al fine di garantire un maggiore trasferimento di competenze alle istituzioni europee in materia di controllo degli investimenti esteri diretti. Ritiene che potrebbe essere appropriato includere anche altri settori strategici nel quadro, come le **reti 5G**, in modo da limitare la dipendenza da fornitori ad alto rischio;

- è del parere che l'Ue debba affrontare più sfide a causa della sua dipendenza da **fornitori esteri di tecnologia**. Ritiene che il tentativo dell'Ue di procedere verso una maggiore **autonomia strategica** e una **sovranità digitale** sia molto importante e rappresenti la giusta strada da percorrere. Viene in particolare citata la **legge europea sui semiconduttori**, annunciata dalla Commissione per garantire che le parti essenziali per la produzione dei semiconduttori siano prodotte in Europa, in quanto sarà un passo importante per limitare la dipendenza da Paesi terzi quali la Cina e gli Stati Uniti.

4) Finanziamento occulto di attività politiche da parte di donatori stranieri.

La proposta di risoluzione sottolinea che i finanziamenti stranieri delle attività politiche attraverso operazioni occulte rappresentano una grave compromissione dell'integrità del funzionamento democratico dell'Ue e degli Stati membri, in particolare durante i **periodi elettorali**, in quanto violano il principio di elezioni libere e regolari.

Il testo evidenzia che una parte considerevole dei finanziamenti occulti da parte di attori stranieri non è illegale in senso stretto poiché sono consentiti da numerose lacune derivanti dalle diverse disposizioni relative al finanziamento delle attività politiche previste dalle legislazioni nazionali degli Stati membri in materia

elettorale. Sottolinea che tali **lacune** includono: a) contributi in natura da parte di attori stranieri a favore di partiti polittici, compresi prestiti finanziari da parte di persone fisiche o giuridiche con sede all'estero; b) donatori prestanome con cittadinanza nazionale; c) società di comodo e società controllate nazionali appartenenti a società madri straniere; d) organizzazioni senza scopo di lucro e terze parti, coordinate da attori stranieri e create allo scopo di influenzare i processi elettorali; e) pubblicità politica *online*, che non è soggetta alle norme applicate alla pubblicità televisiva, radiofonica e a mezzo stampa e che in genere non è regolamentata in alcun modo.

Kalniete cita in proposito la relazione del 2020 della *Alliance for Securing Democracy* sui finanziamenti stranieri occulti, la quale evidenzia che negli ultimi dieci anni la Russia, la Cina e altri regimi autoritari hanno distribuito più di 300 milioni di dollari in 33 Paesi per interferire con i processi democratici più di 100 volte e la metà dei casi riguarda **azioni della Russia in Europa**.

Pertanto la risoluzione:

- invita la Commissione europea a presentare proposte concrete per colmare tutte le lacune che danno adito a metodi di finanziamento opachi dei partiti politici da parte di fonti di Paesi terzi e a proporre **norme comuni** a livello dell'Ue che si applicherebbero alle **leggi elettorali nazionali in tutti gli Stati membri**;
- accoglie con favore la revisione in corso del regolamento (UE, Euratom) n.1141/2014 relativo allo **statuto** e al **finanziamento dei partiti politici europei e delle fondazioni politiche europee.**

5) Cibersicurezza e resilienza agli attacchi informatici.

La relatrice sottolinea che la crescente digitalizzazione dei servizi ha comportato una maggiore dipendenza delle **infrastrutture critiche** dai sistemi *online*, fattore che ne ha accresciuto la vulnerabilità ad attacchi informatici e al rischio di esposizione dei dati. Negli ultimi anni sono infatti aumentati gli attacchi informatici indirizzati a settori strategici (la risoluzione indica, fra gli altri, quelli rivolti all'Agenzia europea per i medicinali - EMA e al parlamento norvegese).

Al riguardo la risoluzione:

- esorta le istituzioni europee ad aumentare rapidamente gli investimenti nelle **capacità e competenze digitali strategiche** dell'Unione, quali l'intelligenza artificiale, la comunicazione sicura e le infrastrutture di dati *e cloud*, al fine di migliorare la cibersicurezza dell'Unione; invita inoltre la Commissione a stanziare ulteriori risorse,

sia umane che finanziarie, per la cibersicurezza delle istituzioni europee e degli Stati membri. In tal senso, accoglie con favore le proposte della Commissione riguardanti una nuova strategia per la cibersicurezza e una **nuova direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione**, che abroga la direttiva (UE) 2016/11488 (NIS2)[2]. Sostiene inoltre l'idea della Commissione di elaborare una legge sulla resilienza informatica che vada a integrare la politica europea in materia di **difesa informatica**, poiché l'informatica e la difesa sono interconnesse;

- ritiene opportuno affrontare rapidamente la questione dei ***software* di spionaggio**, come Pegasus, rafforzando il quadro legislativo in modo da chiamare i distributori, gli utilizzatori e quanti abusano di tali *software* a rispondere del proprio operato;
- condanna l'uso massiccio e illecito del *software* di sorveglianza **Pegasus** da parte di soggetti statali nei confronti di giornalisti, difensori dei diritti umani e politici[3].

6) Protezione delle istituzioni europee.

La cibersicurezza non dovrebbe essere migliorata soltanto a livello di Stati membri ma anche nelle istituzioni dell'Ue. La relatrice ricorda che i recenti attacchi informatici indirizzati contro le istituzioni europee hanno evidenziato l'esigenza di una forte **cooperazione interistituzionale** per l'individuazione, il monitoraggio e la condivisione delle informazioni durante gli attacchi informatici e/o per prevenirli.

La risoluzione sottolinea l'importanza del coordinamento fra le diverse istituzioni, gli organi e le agenzie dell'Ue specializzati in cibersicurezza, quali la squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie europee (CERT-UE), unitamente al pieno sviluppo delle relative capacità operative, quali l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) e la futura Unità congiunta per il ciberspazio che garantiranno una risposta coordinata alle minacce per la cibersicurezza su vasta scala nell'Ue.

---

[2] Proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 (COM(2020)823).

[3] Fa, in particolare, riferimento alle sanzioni imposte il 21 giugno 2021 ad Alexander Shatrov, amministratore delegato di un'impresa che produce un *software* di riconoscimento facciale utilizzato da un regime autoritario.

La risoluzione afferma infine che:

- attende con interesse le due proposte di regolamento della Commissione per l'istituzione di un quadro normativo per la sicurezza dell'informazione e la cibersicurezza in tutte le istituzioni, gli organi e le agenzie dell'Ue;
- invita la Commissione e gli Stati membri a destinare ulteriori fondi e risorse alla cibersicurezza delle istituzioni europee, al fine di rispondere alle sfide in un contesto di minacce in costante evoluzione;
- attende con interesse la relazione speciale di *audit* della **Corte dei conti europea** sulla cibersicurezza, prevista per l'inizio del 2022;
- invita tutte le istituzioni dell'Ue a promuovere la sensibilizzazione fra il personale mediante una formazione e orientamenti adeguati, per mitigare e affrontare i rischi per la sicurezza di natura informatica e non informatica.

7) Ingerenze attraverso l'*elite capture*, le diaspore nazionali e le università.

La risoluzione **condanna tutti i tipi di "*elite capture*" e la tecnica della cooptazione di funzionari pubblici di alto livello e di ex politici europei**, utilizzata dalle imprese straniere collegate ai governi impegnati attivamente in azioni di ingerenza contro l'Ue, e deplora la mancanza degli strumenti e delle azioni di contrasto necessari per prevenire tali pratiche. Ritiene che la divulgazione delle informazioni riservate acquisite durante mandati pubblici o nell'esercizio di funzioni pubbliche, **a discapito degli interessi strategici dell'Ue e degli Stati membri**, dovrebbe essere rigorosamente vietata. Esprime inoltre preoccupazione per le **strategie di *lobbying* integrate** che combinano gli interessi industriali e gli obiettivi di politica estera, in particolare se favoriscono gli interessi di uno Stato autoritario.

Un'altra forma di ingerenza attraverso le persone avviene con la crescente influenza, e infine con il controllo, nei confronti delle università, delle scuole e dei centri culturali e religiosi da parte di agenti di Stati stranieri, in relazione ad aspetti rilevanti per un determinato Paese straniero. Tali forme di ingerenza sfruttano principalmente i tentativi di controllare le diaspore nazionali nell'Ue, rappresentano uno strumento potenzialmente molto efficace per esercitare pressioni ai vari livelli delle società europee, e mirano inoltre a ridurre al silenzio gli oppositori politici residenti all'estero.

Nella risoluzione viene espressa preoccupazione per il numero di **università, scuole e centri culturali europei impegnati in partenariati con soggetti cinesi**, compresi

gli Istituti Confucio (noti come "Centri per l'istruzione linguistica e la cooperazione"), che consentono il furto di conoscenze scientifiche e l'esercizio di un rigido controllo nel settore della ricerca e dell'insegnamento, il che costituisce una violazione della protezione della libertà e autonomia accademica prevista dalla Costituzione, e sulle scelte delle attività culturali riguardanti la Cina; deplora, in particolare, la decisione del museo di Nantes di cancellare la mostra su Genghis Kahn nel 2020, a seguito delle forti pressioni esercitate dalla Cina contro la sua organizzazione.

Osserva che le ingerenze straniere possono assumere anche la forma di influenza esercitata negli istituti religiosi, come nel caso dell'**ingerenza russa nelle chiese ortodosse**, in particolare in Serbia e Montenegro, al fine di generare divisioni fra le popolazioni locali, promuovere una ricostruzione storica distorta e un'agenda anti-Ue, e dell'**ingerenza** turca attraverso le moschee in Francia e Germania.

DIBATTITO TEMATICO II - RISPONDERE ALLE INTERFERENZE STRANIERE IN COOPERAZIONE CON LE DEMOCRAZIE AFFINI

1. Principali strumenti normativi e iniziative dell'Unione europea

Le minacce alle reti e ai sistemi informatici

Con l'accelerazione della digitalizzazione, la sicurezza informatica è divenuta una delle componenti più importanti della sicurezza globale. Gli attacchi informatici e la criminalità informatica stanno aumentando in tutta Europa in termini sia di quantità che di sofisticazione; una tendenza destinata a crescere in futuro, visto che il numero dei dispositivi connessi, fra cui macchine, sensori, componenti industriali e reti che costituiscono l'internet degli oggetti (IoT), continua a crescere.

Le minacce alle reti e ai sistemi informatici è una categoria di illeciti considerata di particolare rilievo, attesa la vitale importanza delle reti e dei sistemi informatici rispetto al funzionamento delle **infrastrutture critiche** (fra tutte, il sistema dei trasporti, le strutture ospedaliere, quelle energetiche), la cui sicurezza attiene peraltro al normale **svolgimento della vita democratica di un paese**. L'intervento dell'Ue al riguardo si è sviluppato su diversi piani, inclusa la politica estera, di sicurezza e di difesa europea, stante la natura di vera e propria **minaccia ibrida** di alcune tipologie di attacchi informatici.

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.

In particolare, con la direttiva 2016/1148, sulla **sicurezza delle reti e dell'informazione - direttiva NIS** (recepita in Italia con il Decreto legislativo 18 maggio 2018, n. 65), l'Unione europea ha posto le basi per un miglioramento della cooperazione operativa fra Stati membri in caso di incidenti di cibersicurezza e della condivisione delle informazioni sui rischi. La direttiva definisce obblighi di sicurezza per gli operatori di servizi essenziali (in settori critici come l'energia, i trasporti, l'assistenza sanitaria e la finanza) e i fornitori di servizi digitali (mercati *online*, motori di ricerca e

servizi di *cloud*); inoltre, ogni Paese dell'Ue è tenuto a designare una o più autorità nazionali con il compito, fra l'altro, di monitorare l'applicazione della direttiva, nonché a elaborare una strategia per affrontare le minacce informatiche.

L'Ue ha consolidato tale quadro mediante l'adozione del regolamento (UE) n. 2019/881 sulla **cibersicurezza** (cd. ***cybersecurity act***), recante una serie di disposizioni per:

- il rafforzamento dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (**Enisa**);
- l'introduzione nell'Unione di **sistemi europei di certificazione** della cibersicurezza dei prodotti e dei servizi delle tecnologie dell'informazione e della comunicazione (TIC).

Il 20 maggio 2021 è stato inoltre adottato il regolamento (UE) 2021/887 che istituisce il **Centro europeo di competenza per la cibersicurezza** nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento. La creazione del Centro europeo di competenza per la cibersicurezza dovrebbe contribuire ad aumentare la sicurezza delle reti e dei sistemi informativi, fra cui **internet** e altre **infrastrutture critiche** per il funzionamento della società, come i **trasporti, la sanità, l'energia, le infrastrutture digitali, l'acqua, il mercato finanziario e i sistemi bancari**.

Disposizioni volte alla **sicurezza delle reti** sono altresì contenute nel Codice delle comunicazioni elettroniche.

L'Ue sta inoltre lavorando a due proposte legislative tese ad affrontare i rischi attuali e futuri *online* e *offline*:

- una direttiva aggiornata relativa a **misure per un livello comune elevato di cibersicurezza nell'Unione**, al fine di proteggere meglio la rete e i sistemi informativi. La proposta è volta a sostituire le attuali norme comuni in materia di sicurezza delle **reti** e dei **sistemi informativi** nell'Unione (direttiva NIS) approvate nel 2016; risponde al panorama di minacce in evoluzione e tiene in considerazione la trasformazione digitale della società, che è stata accelerata dalla crisi pandemica. Le nuove norme: mirano a rafforzare gli obblighi di sicurezza per le imprese; riguardano la sicurezza delle **catene di approvvigionamento**; introducono misure di **vigilanza** più rigorose

per le autorità nazionali; accrescono ulteriormente la **condivisione** delle informazioni e la **cooperazione**;

- una nuova direttiva sulla **resilienza dei soggetti critici**. Il regime proposto estende sia l'ambito di applicazione, sia la profondità della direttiva sulle **infrastrutture critiche europee** del 2008. In particolare con la riforma sarebbero contemplati **dieci settori**: energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio. Gli Stati membri adotterebbero una rispettiva **strategia nazionale** per garantire la resilienza dei soggetti critici ed effettuerebbero valutazioni periodiche dei rischi. Tali valutazioni contribuirebbero a individuare un sottoinsieme più ristretto di **soggetti critici** cui incomberebbero **obblighi** volti a rafforzarne la resilienza di fronte ai **rischi non informatici**, comprese le valutazioni dei rischi a livello di soggetto, l'adozione di misure tecniche e organizzative e la notifica degli **incidenti**.

Il Consiglio dell'Ue considera il ciberspazio la quinta dimensione della conflittualità, essenziale per le operazioni militari, insieme a terra, mare, aria e spazio. Tale dimensione comprende tutto quanto va dalle reti e infrastrutture di informazione e telecomunicazione e dai dati che supportano fino ai sistemi informatici, ai processori e ai dispositivi di controllo. In tale contesto, l'Ue coopera in materia di difesa nel ciberspazio attraverso le attività dell'**Agenzia europea per la difesa** (AED), in collaborazione con l'Agenzia dell'Ue per la cibersicurezza ed Europol. L'AED sostiene gli Stati membri nella creazione di una forza militare qualificata nel settore della ciberdifesa e garantisce la disponibilità di tecnologie di ciberdifesa proattive e reattive.

Nel quadro del **programma Europa digitale** per il periodo 2021-2027, l'Ue si è impegnata a investire **1,6 miliardi** di euro in capacità di cibersicurezza e nell'ampia diffusione di infrastrutture e strumenti per la cibersicurezza in tutta l'Ue a favore di pubbliche amministrazioni, imprese e singoli cittadini. La cibersicurezza è presa in considerazione altresì nei programmi quadro di finanziamento dell'UE in materia di ricerca e innovazione **Orizzonte 2020** e il suo successore **Orizzonte Europa**: in particolare, nel maggio 2020 l'Ue ha impegnato 49 milioni di euro per promuovere l'innovazione nei sistemi di cibersicurezza e *privacy*.

Il 19 ottobre 2021 il Consiglio dell'Ue ha adottato conclusioni, che invitano, fra l'altro, l'Ue e gli Stati membri a sviluppare ulteriormente il quadro dell'Ue per la gestione delle crisi di cibersicurezza, anche esplorando il potenziale di un'**Unità congiunta per il ciberspazio** (cui gli Stati membri dovrebbero partecipare o contribuire su base volontaria), la quale dovrebbe rispettare le competenze, i mandati e i poteri legali dei suoi possibili futuri partecipanti.

Da ultimo, il **Consiglio europeo del 21 e 22 ottobre 2021 -** evidenziando il marcato aumento delle attività informatiche malevole volte a minare i valori democratici e la sicurezza delle funzioni fondamentali delle società Ue - ha ribadito l'impegno a perseguire i valori democratici, sia *online* che *offline*. In tale contesto ha ribadito l'impegno dell'Ue a favore di un ciberspazio aperto, libero, stabile e sicuro e ha esortato i Paesi di tutto il mondo ad aderire e a dare applicazione a tali norme.

Ha quindi chiesto di portare avanti i lavori sulla proposta di direttiva riveduta sulla sicurezza delle reti e dei sistemi informativi, sulla proposta di direttiva sulla resilienza dei soggetti critici e sul pacchetto di strumenti della diplomazia informatica. Ha espresso la necessità di un coordinamento e una preparazione efficaci di fronte alle minacce alla cibersicurezza e ha sottolineato l'importanza di sviluppare ulteriormente il quadro di gestione delle crisi di cibersicurezza dell'Ue e un'efficace risposta a livello dell'Ue agli incidenti e alle crisi di cibersicurezza su vasta scala, anche attraverso esercitazioni ed esplorando il ciberspazio, nonché potenziando la cooperazione con i Paesi partner nei consessi multilaterali. (vd. Documenti dell'Unione europea n. 26/DOCUE).

Per approfondimenti sulla **normativa italiana** in materia di cibersicurezza, si rimanda al **Dossier** n. 403 "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale. D.L. 82/2021 - A.C. 3161", del 22 giugno 2021, a cura del Servizio Studi del Senato della Repubblica e del Servizio Studi e dell'Ufficio per i rapporti con l'Unione europea della Camera dei deputati. Si ricorda che l'Agenzia per la cibersicurezza è qualificata quale Autorità nazionale, ai fini del complesso di relazioni e funzioni disegnato dalle norme europee ed interne, incluse quelle di certificazione della cibersicurezza. In tale quadro, predispone in primo luogo la strategia nazionale di cibersicurezza; assume compiti finora attribuiti a diversi soggetti quali il Ministero dello sviluppo economico; la Presidenza del Consiglio; il Dipartimento delle informazioni

e della sicurezza; l'Agenzia per l'Italia digitale; promuove iniziative per lo sviluppo di competenze e capacità.

Da ultimo si segnala che, nel 2020, la III Commissione (Affari esteri e comunitari) della Camera dei deputati ha avviato un'indagine conoscitiva sulle eventuali **interferenze straniere sul sistema delle relazioni internazionali** della Repubblica Italiana.

Il contrasto alle attività di disinformazione

Dal 2015, l'Ue è sistematicamente impegnata nel contrasto alle attività di **disinformazione**, cui sono riconducibili - secondo la definizione impiegata dalla Commissione europea - informazioni verificate come **false** o **fuorvianti** create, presentate e diffuse a scopo di **lucro** o al fine di **ingannare** intenzionalmente il **pubblico**, compreso l'obiettivo di **falsare** il **dibattito pubblico**, minare la **fiducia** dei cittadini nelle istituzioni e nei media e **destabilizzare** i **processi democratici** come le **elezioni**.

Fra i primi strumenti per contrastare la propaganda di enti e organismi situati in **Stati terzi** volta a diffondere informazioni fuorvianti o palesemente false (in particolare, da parte della Russia), vi è la *task force East StratCom*, istituita nel 2015 con il compito di sviluppare prodotti e campagne di comunicazione incentrate sulla spiegazione delle politiche dell'Ue nella regione del **partenariato orientale**. Sono incentrate su altre aree geografiche la *task torce* ***StratCom*** **per i Balcani occidentali** e la ***task torce South Med Stratcom*** per il mondo di lingua araba.

Fra le iniziative più significative per il contrasto alla disinformazione si ricordano:

- la comunicazione dell'aprile 2018, con la quale la Commissione europea ha delineato un approccio comune alla materia e previsto quale misura chiave l'elaborazione da parte dei rappresentanti delle piattaforme *online*, dell'industria della pubblicità e dei principali inserzionisti di un il codice di condotta per lottare contro le forme illegali di **incitamento all'odio *online*** (su cui, da ultimo, il **7 ottobre 2021** la Commissione ha presentato la 6a valutazione);

Il codice è stato adottato, a partire dall'ottobre del 2018, dalle principali piattaforme *online* (fra le quali Facebook, Google, Twitter, YouTube Instagram, Snapchat, Dailymotion, Jeuxvideo.com e TikTok), dalle società di *software* (in particolare, nel maggio 2019, ha aderito al codice la Microsoft) e dalle organizzazioni che rappresentano il settore della

pubblicità. Il codice prevede una serie di impegni, che comprendono la garanzia della trasparenza dei messaggi pubblicitari di natura politica, la chiusura dei profili falsi, l'etichettatura dei messaggi diffusi dai "*bot*" e il miglioramento della visibilità dei contenuti sottoposti a verifica dei fatti.

- il **pacchetto elezioni** (presentato dalla Commissione europea in occasione del discorso sullo Stato dell'Unione del settembre 2018), recante una serie di misure per garantire elezioni libere ed eque;

Si tratta, in particolare, di: una comunicazione della Commissione europea dal titolo "Assicurare elezioni europee libere e corrette; la Raccomandazione (UE) 2018/334 della Commissione, del 1º marzo 2018, sulle misure per contrastare efficacemente i contenuti illegali *online*; gli 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 Parlamento europeo approfittando di violazioni delle norme in materia di protezione dei dati.

Per approfondimenti sulla **legislazione nazionale** si rimanda al Dossier n° 39/3 "Contrasto dei reati contro la pubblica amministrazione, prescrizione e trasparenza dei partiti e movimenti politici A.C. 1189-B, a cura del Servizio Studi della Camera dei deputati. Si veda in particolare l'art. 1, commi 11 e 12, **in materia di trasparenza e controllo dei partiti politici e delle fondazioni**. In particolare, il comma 12 ha introdotto per i partiti e i movimenti politici, nonché per le liste che partecipano alle elezioni nei comuni con più di 15.000 abitanti, il divieto di ricevere contributi, prestazioni o altre forme di sostegno provenienti da Governi o enti pubblici di Stati esteri e da persone giuridiche aventi sede in uno Stato estero non assoggettate ad obblighi fiscali in Italia. Le disposizioni di cui al comma 11 sono state successivamente modificate dall'art. 43, comma 3, lett. a), D.L. 30 aprile 2019, n. 34, convertito, con modificazioni, dalla L. 28 giugno 2019, n. 58 (cfr. il Dossier n. 123/5 "Misure urgenti di crescita economica e per la risoluzione di specifiche situazioni di crisi", a cura del Servizio Studi del Senato e del Servizio Studi della Camera dei deputati).

- il 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 2018.

Il piano è articolato in quattro settori chiave: 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; risposta coordinata, dotando istituzioni Ue e Stati membri di un sistema di allarme rapido per la condivisione e valutazione delle campagne di disinformazione; attuazione efficace da parte delle piattaforme *online* e delle industrie firmatarie degli impegni nell'ambito del codice di buone pratiche; campagne di sensibilizzazione e di responsabilizzazione dei cittadini in particolare mediante l'alfabetizzazione mediatica. Il 14 giugno 2019 è stata pubblicata una relazione sullo stato dell'arte dell'attuazione del piano.

Con particolare riferimento alla **pandemia di Covid-19**, il 10 giugno 2020 la Commissione e l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno pubblicato la comunicazione congiunta "Contrastare la disinformazione sulla Covid-19 – Guardare ai fatti".

Come evidenziato nella sua comunicazione dal titolo "Plasmare il futuro digitale dell'Europa", del 19 febbraio 2020, la Commissione si è impegnata ad aggiornare le norme orizzontali che definiscono **le responsabilità e gli obblighi dei prestatori di servizi digitali**, in particolare delle piattaforme *online*, dichiarando che *"le persone hanno diritto a tecnologie di cui possono fidarsi"* e che "***ciò che è illecito* offline *deve esserlo anche* online**".

Di particolare rilievo in tal senso è la proposta di regolamento relativo a un mercato unico dei servizi digitali (cd. **"legge sui servizi digitali"**), adottata dalla Commissione europea il 15 dicembre 2020, che rappresenta una delle misure chiave nell'ambito della Strategia europea per il digitale. La proposta intende modificare la direttiva 2000/31/CE sul commercio elettronico in quanto, dalla sua adozione, si sono affermati nuovi e innovativi servizi digitali della società dell'informazione che - sottolinea la Commissione nella relazione illustrativa - *"hanno cambiato la vita quotidiana dei cittadini dell'Unione plasmando e trasformando il loro modo di comunicare, connettersi, consumare e svolgere attività economiche (...). Allo stesso tempo, dall'uso di questi servizi sono scaturiti nuovi rischi e nuove sfide, che interessano sia la società nel suo complesso, sia le singole persone che si avvalgono di tali servizi".*

Si ricordano inoltre:

- il Forum dell'Ue su internet avviato nel dicembre 2015 nel quadro dell'Agenda europea sulla sicurezza;
- il regolamento (UE) 2021/784, del **29 aprile 2021**, relativo al **contrasto della diffusione di contenuti terroristici *online*.**

Per approfondimenti sulla normativa e sulle iniziative dell'**Italia** in materia di contrasto all'*hate speech* e di responsabilità dell'*Internet service provider* si rimanda ai relativi capitoli contenuti nel Dossier n. 400 "Il contrasto ai fenomeni di intolleranza, razzismo, antisemitismo e istigazione all'odio e alla violenza. Normativa e attività nazionali e dell'Unione europea", a cura del Servizio Studi del Senato.

Si segnala, infine, che è all'esame del Senato una **proposta di legge** recante l'Istituzione di una **Commissione parlamentare di inchiesta sulla diffusione massiva di informazioni false**, approvata dalla Camera dei deputati il 28 luglio 2020.

Secondo la proposta, la Commissione dovrebbe essere composta da **venti senatori** e da **venti deputati**, nominati dai Presidenti delle rispettive Camere nel rispetto del principio di proporzione tra i gruppi parlamentari, assicurando comunque la presenza di un rappresentante per **ciascun gruppo** esistente in almeno un ramo del Parlamento e favorendo l'**equilibrio** nella rappresentanza dei **sessi.**

Piano d'azione per la democrazia europea

Il 3 dicembre 2020 la Commissione europea ha presenta il piano d'azione per la democrazia europea per **rafforzare la resilienza** delle democrazie in tutta l'Ue.

Il piano d'azione si rivolge alle istituzioni dell'Ue, ai governi e ai parlamenti nazionali - cui spetta in prima istanza la responsabilità di garantire il buon funzionamento della democrazia -, nonché ad altre autorità nazionali, partiti politici, mezzi d'informazione, società civile e piattaforme *online*. Nel pieno rispetto delle competenze nazionali, il piano intende definire un quadro rafforzato delle politiche Ue e misure specifiche allo scopo di:

- **promuovere elezioni libere e regolari** e una forte partecipazione democratica;
- **sostenere mezzi d'informazione liberi e indipendenti**;
- **contrastare la disinformazione**.

Più concretamente, la Commissione intende:

1. proporre atti giuridici in materia di **pubblicità politica**, che avranno a oggetto gli sponsor di contenuti a pagamento e i canali di produzione e distribuzione, fra cui le piattaforme *online*, gli inserzionisti e le società di consulenza politica, chiarendone le rispettive responsabilità. La Commissione proporrà atti legislativi sulla **trasparenza dei contenuti politici sponsorizzati ("pubblicità politica")** e rivedrà inoltre le norme **sul finanziamento dei partiti politici europei**;
2. raccomandare misure per garantire la **sicurezza dei giornalisti** (presenterà fra l'altro un'iniziativa per proteggerli dalle azioni legali strategiche tese a bloccare la partecipazione pubblica);
3. dirigere gli sforzi di **revisione del vigente codice di buone pratiche sulla disinformazione**, rafforzando gli obblighi a carico delle piattaforme *online* e introducendo un monitoraggio e una sorveglianza rigorosi.

La Commissione attuerà gradualmente il piano d'azione per la democrazia europea **entro il 2023**, un anno prima delle elezioni del Parlamento europeo; esaminerà poi i progressi compiuti e valuterà se siano necessarie ulteriori misure.

Proposte contenute nel progetto di relazione della Commissione INGE

Deterrenza e sanzioni collettive

L'Ue e gli Stati membri non dispongono attualmente di un **regime specifico di sanzioni riguardanti le ingerenze straniere** e le campagne di disinformazione orchestrate da attori statali stranieri. La relatrice è consapevole delle problematiche giuridiche che possono emergere istituendo un tale **regime sanzionatorio**, inclusa la necessità di definire con precisione le fattispecie di reato e i loro possibili effetti cumulativi conformemente alle legislazioni dell'Ue e internazionali. Ritiene tuttavia che l'Ue possa trarre un'utile ispirazione dalle esperienze di altri partner a tale riguardo, come ad esempio l'**Australia**, che ha definito in modo specifico che cosa sia un'"ingerenza straniera dolosa" e ha **equiparato a reato le attività occulte e ingannevoli di attori stranieri**.

Nella risoluzione viene evidenziato che i regimi sanzionatori istituiti di recente dall'Ue, come le **misure restrittive contro gli attacchi informatici** che minacciano l'Unione o i suoi Stati membri e il **regime globale di**

sanzioni dell'Ue in materia di diritti umani, adottati rispettivamente il 17 maggio 2019 e il 7 dicembre 2020, abbiano dimostrato un valore aggiunto nel fornire all'Ue preziosi strumenti di deterrenza; e viene ricordato che i regimi sanzionatori contro gli attacchi informatici e le violazioni dei diritti umani sono stati utilizzati due volte, rispettivamente nel 2020 e nel 2021.

La risoluzione quindi:

- invita l'Ue e i suoi Stati membri a intraprendere ulteriori misure contro la disinformazione e le minacce ibride, nel pieno rispetto della libertà di espressione e di informazione, anche introducendo un regime sanzionatorio - a norma dell'articolo 29 del trattato sull'Unione europea (TUE) e dell'articolo 215 del trattato sul funzionamento dell'Unione europea - in materia di ingerenze straniere, compresa la disinformazione, che dovrebbe essere destinato per quanto possibile ai decisori politici e agli organi responsabili di azioni aggressive;
- evidenzia che, al fine di rafforzarne l'impatto, le sanzioni dovrebbero essere irrogate collettivamente, con partner che condividono gli stessi princìpi, coinvolgendo possibilmente le organizzazioni internazionali e mediante la formalizzazione in un accordo internazionale;
- ricorda il comunicato della riunione Nato del 14 giugno 2021, in cui si afferma che una decisione riguardante il ricorso all'articolo 5 del trattato Nato in caso di attacco informatico viene presa dal Consiglio del Nord Atlantico sulla base di un esame caso per caso, e che l'impatto di attività informatiche cumulative dolose potrebbe, in talune circostanze, essere considerato equivalente a un **attacco armato**.

Cooperazione mondiale e multilateralismo

La risoluzione riconosce che molti Paesi democratici in tutto il mondo si trovano ad affrontare operazioni di destabilizzazione simili condotte da Stati stranieri autoritari (da parte di **Cina**, **Russia** o altri **regimi autoritari**, che perseguono lo stesso obiettivo: **minare il funzionamento democratico per rafforzare la propria influenza**). Sottolinea quindi l'esigenza di una cooperazione mondiale fra Paesi che condividono gli stessi princìpi su tali questioni di importanza fondamentale, sotto forma di **partenariato basato su una visione comune e definizioni condivise**, al fine di istituire norme e princìpi internazionali: sulla base di una consapevolezza comune della situazione, i partner che condividono gli stessi princìpi dovrebbero

promuovere lo scambio di migliori pratiche e individuare soluzioni comuni, ivi comprese le **sanzioni collettive**.

La risoluzione invita infine il **Parlamento europeo** a svolgere un **ruolo di guida** nella promozione dello scambio delle informazioni e delle pratiche migliori con i parlamenti partner in tutto il mondo, utilizzando la sua vasta rete di delegazioni interparlamentari nonché le iniziative democratiche e le attività di sostegno coordinate dal Gruppo per il sostegno alla democrazia e il coordinamento elettorale.