Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

digi
DIPARTIMENTO DI GIURISPRUDENZA

**Hybrid threats versus Democratic Resilience:
An analytical and practical toolkit**

Davide Vaira

Trick or T(h)reat: disinformazione online e minacce ibride nel panorama europeo. Alcune considerazioni alla luce dell'annullamento delle elezioni in Romania.

Trick or T(h)reat: disinformazione online e minacce ibride nel panorama europeo. Alcune considerazioni alla luce dell'annullamento delle elezioni in Romania.

Davide Vaira

The present contribution has been published on SIDIBlog.

1. Il giorno 6 dicembre 2024 la Corte costituzionale rumena ha **annullato i risultati delle elezioni presidenziali** per sospette ingerenze da parte della Russia durante la campagna elettorale.

Per comprendere la portata di tale annullamento e inquadrare le connesse problematiche giuridiche, appare opportuno ripercorrere gli accadimenti principali.

Il 2024 è stato un anno fondamentale per la politica internazionale, in quanto ha ospitato un numero di elezioni democratiche insolitamente alto, che hanno coinvolto anche attori di rilievo quali gli Stati Uniti e l'Unione Europea e hanno ridefinito gli equilibri globali (per un approfondimento sull'argomento, in questo blog, si veda Ruotolo, 2024a).

Nei mesi di novembre e dicembre il *focus* si è concentrato sulle elezioni presidenziali in Romania.

Le primarie si sono concluse con l'indicazione di tre diversi candidati: Ion-Marcel Ciolacu, già Primo Ministro del Paese e membro del Partito Social Democratico, Elena Lasconi di estrazione centrista, Călin Giorgescu, indipendente, di orientamento filo-russo e contrario all'erogazione di aiuti all'Ucraina.

Nonostante la maggioranza relativa raggiunta al primo turno dal Partito Social Democratico di Ciolacu, i risultati delle coalizioni di centro e di destra hanno consentito ai rispettivi candidati di giungere al ballottaggio, originariamente previsto per l'8 dicembre.

Al riguardo, particolare interesse ha suscitato il risultato raggiunto dalla coalizione dei tre partiti di estrema destra, sostenitrice di Giorgescu, che ha superato il 31% dei voti, nella misura del triplo rispetto alle precedenti elezioni tenutesi nel 2020.

L'inatteso risultato raggiunto al primo turno dalla coalizione di Giorgescu ha determinato numerose proteste nel Paese e, in data 4 dicembre, la diffusione, da parte del Ministero dell'Interno, di documenti classificati provenienti dal Servizio di Intelligence estero, dal Servizio di Intelligence

rumeno e dal Servizio Speciale di Telecomunicazioni, a dimostrazione di **ingerenze di uno Stato terzo** sull'esito delle elezioni.

La diffusione dei documenti classificati ha determinato l'intervento della Corte costituzionale rumena, quale garante della correttezza del processo elettorale ai sensi dell'art. 146 lett. f) della Costituzione, che, con la decisione 32/2024 del 6 dicembre 2024 (qui tradotta), ha annullato l'intero procedimento elettorale per sospette ingerenze da parte della Russia e, in applicazione dell'art. 83 par. 2 della Costituzione, ha confermato il mantenimento in carica del Presidente uscente fino all'elezione del successivo.

Nella sentenza la Corte ha motivato la decisione affermando che «assicurare il rispetto del procedimento per l'elezione del Presidente» non deve essere inteso in senso restrittivo, ma, al contrario, consente finanche l'annullamento *tout court* delle elezioni in caso di sospette irregolarità.

Il sospetto di un'indebita ingerenza da parte della Russia è dipeso dalla circostanza che, a differenza della campagna elettorale condotta dai candidati Ciolacu e Lasconi in modo tradizionale, diversamente, quella di Giorgescu si è svolta quasi completamente **attraverso piattaforme online** e, in particolare, *TikTok*.

La scelta, che ha consentito a Giorgescu di dichiarare una spesa elettorale pari a zero, ha suscitato diversi interrogativi in quanto, contemporaneamente, proprio sulla piattaforma *TikTok,* era divenuta virale una **campagna filorussa** contro gli aiuti a Kiev, che si basava principalmente sul risentimento della popolazione rumena per il trattamento preferenziale riservato ai rifugiati ucraini e sul timore di un'espansione del conflitto anche in territorio rumeno in caso di mantenimento del supporto all'Ucraina, attesa la rilevanza strategica della Romania dovuta alla vicinanza geografica a quest'ultima.

Alla campagna filorussa si è affiancata la campagna elettorale di Giorgescu, i cui contenuti sono stati più difficilmente verificabili dagli algoritmi, in quanto i video spesso erano inseriti nella categoria 'intrattenimento', invece che nella categoria 'politica'.

La Corte costituzionale, ribadendo il diritto alle libere elezioni come uno degli elementi fondamentali delle democrazie occidentali, ha focalizzato due particolari aspetti.

Per un verso ha affermato la violazione di norme di legge sul finanziamento delle campagne elettorali, evidenziando che «[…] una campagna elettorale comporta costi e spese rilevanti, e la situazione analizzata rivela un'evidente incongruenza tra la portata della campagna svolta e l'inesistenza assunta dal candidato in merito alle spese sostenute», da cui il sospetto di finanziamenti illeciti; per altro verso ha sottolineato il sospetto di una campagna di disinformazione e di **uso non trasparente di tecnologie digitali,** con le quali sono state «distort[e] la natura libera e corretta dell'esperienza di voto espressa dai cittadini e le pari opportunità dei concorrenti elettorali».

La Corte ha così evidenziato, quali requisiti necessari delle elezioni democratiche, la libertà di opinione ed espressione, legate al diritto all'informazione, il diritto di voto, come libero da ingerenze illecite di Paesi terzi, e la trasparenza e pari opportunità tra i candidati.

Il caso in esame presta il fianco a riflessioni sotto diversi profili.

Al di là della questione relativa alla trasparenza dei finanziamenti in periodo elettorale e all'interesse manifestato dalla Commissione Europea in merito agli obblighi di sorveglianza disposti dal Digital Services Act (DSA) in capo alle Piattaforme online di dimensioni molto grandi (Very Large Online Platforms – VLOPs) – tra le quali rientra anche TikTok – sui contenuti caricati dagli utenti, sui quali, per esigenze di concisione non è possibile soffermarsi, l'attenzione verrà focalizzata sugli spunti offerti dalla pronuncia della Corte costituzionale in tema di indebita ingerenza di Stati terzi e di strumenti attraverso i quali gli Stati *target* possono difendersi ed esercitare la resilienza democratica, problematiche che verranno affrontate con riferimento al diritto dell'Unione Europea, non tralasciando alcuni richiami al diritto internazionale.

Così ricostruiti gli avvenimenti del caso in esame, si procede ad analizzare la possibilità di inquadrare la disinformazione online, già utilizzata dalla Russia in passato, come minaccia ibrida (2).

Successivamente, l'attenzione si focalizzerà sul *target* delle minacce ibride e sulla definizione e tutela dei valori democratici e dei diritti fondamentali a questi collegati (3).

Infine, si tenterà una riflessione sugli strumenti di cui dispongono gli Stati per contrastare la disinformazione online e tutelare i principi democratici, in particolare sul *Democracy Shield* (4).

2. La definizione di **minaccia ibrida**, intesa in senso generico, non è agevole in quanto ricomprende un ampio ed eterogeneo ventaglio di comportamenti che possono essere esercitati da uno Stato – o da attori privati – al fine di indebolire un altro Paese (per una ricostruzione approfondita si veda Giannopoulos et al.).

Il concetto di minaccia ibrida è in parte ricollegabile anche a quello di guerra ibrida, che ha avuto la sua maggiore diffusione nel 2014, a seguito dell'annessione della Crimea al territorio russo.

In merito alla minaccia ibrida, la NATO ha ripreso la definizione già utilizzata dall'Unione Europea, secondo cui «le minacce ibride combinano attività convenzionali e non convenzionali, militari e non militari, che possono essere usate in modo coordinato dagli Stati o da attori non statali per raggiungere specifici obiettivi politici [...] [e che] prendono di mira le vulnerabilità critiche e cercano di creare confusione che impedirebbe un processo decisionale rapido ed efficace».

Successivamente, nel 2022, il The Hague Centre for Strategic Studies (HCSS) e, nel 2023, l'European Centre of Excellence for Countering Hybrid Threats (Hybrid Coe) hanno definito la nozione di minaccia ibrida sottolineando l'idea che il *target* possa essere rappresentato sia dagli Stati che dalle Istituzioni democratiche.

Nel concetto di minaccia ibrida è possibile far rientrare la disinformazione, non solo perchè così espressamente definita dalle istituzioni europee (si veda ad esempio il par. 63 della comunicazione della Commissione C/2024/3014), ma anche perchè la stessa, negli anni, si è rivelata come strumento utile alla destabilizzazione dei Paesi.

Quanto all'uso di minacce ibride durante le campagne elettorali, occorre operare una distinzione tra misinformazione, disinformazione e propaganda.

La misinformazione ricomprende informazioni false o fuorvianti che, tuttavia, non sono state diffuse con l'intento di nuocere, sicchè, pur rientrando tra i fattori di rischio per i procedimenti democratici (si vedano al riguardo i punti 27 a) e 40 a) della comunicazione della commissione), non è generalmente ritenuta minaccia ibrida, in quanto non cagionata volontariamente.

La disinformazione, invece, riguarda informazioni false o manipolate, diffuse al preciso scopo di cagionare un danno e può essere considerata come una derivazione della propaganda (Jones, p. 7, si veda inoltre anche Castellaneta) che, a sua volta, originariamente nata con una connotazione neutrale (in tal senso l'art. 20 par. 1 del Patto internazionale sui diritti civili e politici – ICCPR), ha assunto poi una connotazione negativa (Ivancìk, p. 44; Whitton, p. 550).

Il *discrimen* tra misinformazione e disinformazione, pertanto, attiene all'intenzionalità di quest'ultima, che la eleva al rango di minaccia ibrida.

Appare utile precisare che, nel presente elaborato, con la definizione di disinformazione si intendono non solo le informazioni false *tout court*, ma anche la manipolazione di informazioni, ritenuta altrettanto grave.

Per quel che qui rileva, in periodo elettorale la disinformazione rappresenta una minaccia soprattutto quando le notizie false o fuorvianti vengono diffuse da Paesi stranieri, poichè in tal caso, oltre alla violazione del diritto all'informazione e alla libertà di espressione, si configurano anche violazioni del **principio di non ingerenza** che permea il diritto internazionale.

Il divieto di ingerenza di Paesi stranieri negli affari interni di un altro Stato si è ampliato, da un punto di vista pratico, in quanto le piattaforme digitali, che consentono la diffusione globale e immediata delle informazioni grazie all'ubiquità dei dati, rappresentano un veicolo attraverso il quale operare "da remoto" anche in territori esteri; da un punto di vista concettuale, in quanto l'ingerenza non è più riferibile solo

all'uso della forza, ma a qualsiasi strumento che impedisca a uno Stato di agire liberamente (sull'argomento, su questo blog, si veda Ruotolo, 2024a).

Ne deriva che, in periodo elettorale, il libero e ininterrotto flusso di informazioni costituisce, per un verso, un aspetto fondamentale per la corretta partecipazione dei cittadini ai dibattiti, per altro verso uno dei principali strumenti attraverso i quali manipolare le opinioni (in tal senso Bradshaw e Howard hanno parlato di «minaccia critica»).

L'ingerenza e la manipolazione delle informazioni sono strumenti che la Russia ha utilizzato per rafforzare la propria posizione nel **conflitto con l'Ucraina**, anche mediante l'Internet Research Agency (IRA), agenzia che, grazie a finanziamenti statali, ha il preciso compito di diffondere disinformazione e manipolare l'opinione pubblica online, con lo scopo di indebolire i Paesi terzi (al riguardo si veda DiResta et al.).

Sospetti di ingerenza, non sempre provati, da parte della Russia nei confronti delle democrazie occidentali, si sono alimentati in occasione di eventi sensibili, quali la Brexit, il referendum sull'indipendenza della Catalogna, le elezioni statunitensi del 2016.

In generale, in merito alla guerra in Ucraina, sospetti di manipolazione delle informazioni da parte della Russia hanno avuto portata globale (ad esempio, in America Latina).

3. In periodo elettorale, la disinformazione tende a influenzare il dibattito pubblico e a coinvolgere la **libertà di espressione, di opinione e di informazione,** che rappresentano il bagaglio di diritti fondamentali riconosciuti agli individui a livello sia internazionale (si pensi all'art. 19 della Dichiarazione Universale dei Diritti Umani o all'art. 19 della Convenzione Internazionale sui Diritti Civili e Politici), sia europeo.

Negli Stati Uniti l'operatività degli strumenti di contrasto alla disinformazione è limitata dal primo emendamento, che garantisce l'assolutezza della libertà di espressione e dall'approccio *multi-stakeholder* che lascia ampio margine di manovra alle piattaforme online (sul punto Pollicino).

Diversamente, nell'Unione Europea, la tutela del fondamentale diritto del singolo a una **corretta informazione** consente agli Stati maggiori e più incisive possibilità di intervento.

Invero, l'art. 6 TUE recepisce i diritti, le libertà e i principi sia della Carta dei diritti fondamentali dell'Unione Europea, la quale all'articolo 11 prevede la «libertà di opinione e la libertà di ricevere o comunicare informazioni o idee senza che vi possano essere ingerenze da parte di autorità pubbliche e senza limiti di frontiera», sia della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, che, pur richiamando anch'essa il diritto alla libertà di espressione, opinione e informazione, tuttavia, all'art. 10 ne prevede possibili restrizioni qualora necessarie alla tutela della società democratica e, all'art. 17, individua limiti agli abusi del diritto stesso.

Si tratta di forme di tutela che si configurano anche come divieto di manipolazione fraudolenta delle opinioni durante le elezioni.

Nonostante a livello europeo la problematica della disinformazione attraverso le VLOPs sia recente e la tutela di tali diritti online sia poco discussa, si può ritenere che, quanto a quest'ultima, operi il **principio di neutralità tecnologica,** introdotto alla fine dello scorso millennio dalla Commissione Europea, secondo cui i diritti *offline* degli individui e il loro corrispettivo *online* sono equiparabili (sul punto, Ruotolo, 2024b).

In genere, in materia di informazione, i social network e le VLOPs sono sempre stati considerati neutrali, in quanto, pur potendo rappresentare un veicolo di disinformazione, sono uno strumento fondamentale per la tutela dei diritti umani e della democraticità e, in periodo elettorale, per la tutela del libero scambio di idee tra candidati e cittadini.

Da ciò, consegue la necessità di rafforzare il *fact-checking*, vale a dire l'utilizzo, da parte delle piattaforme, di strumenti utili a discernere i contenuti informativi da quelli disinformativi, così da garantire una risposta rapida ed efficace alle minacce ibride, strumenti che, ad oggi, vengono principalmente adoperati sia tramite algoritmi e Intelligenza artificiale (sul punto, in questo blog, si veda Ruotolo, 2023), sia tramite la componente umana, con l'auspicio, per il futuro, della realizzazione

di *board* indipendenti e di un maggiore coinvolgimento degli Stati mediante un *enforcement* pubblico.

Sotto altro profilo è necessario che, nel bilanciamento tra il contrasto alla disinformazione e la tutela della libertà di espressione online, sia rispettato il **principio di proporzionalità**, come già evidenziato nel 2017 a livello internazionale da una dichiarazione congiunta tra l'Organizzazione delle Nazioni Unite (ONU), l'Organizzazione per la Sicurezza e la Cooperazione in Europa (OSCE), l'organizzazione degli Stati Americani (OAS) e la Commissione Africana sui Diritti Umani e dei Popoli (ACHPR) e, prima ancora, da considerazioni sull'art. 19 dell'ICCPR, espresse dal Comitato per i Diritti Umani delle Nazioni Unite.

In ambito europeo, l'operazione di **bilanciamento** tra la libertà di espressione e il contrasto alla disinformazione trova il suo fondamento nei già richiamati art. 10 e 17 della CEDU.

Da un punto di vista teorico, la libertà di espressione, diritto fondamentale dell'individuo, si configura come abuso ai sensi dell'art. 17 CEDU o soccombe nell'operazione di bilanciamento di cui all'art. 10 CEDU solo nel caso in cui la veridicità dell'informazione sia manifestamente esclusa.

Tuttavia, sotto un profilo pratico, l'attuale orientamento è quello di contrastare in via preventiva la disinformazione attraverso l'individuazione di restrizioni anche in ipotesi di mero 'sospetto', di cui la sentenza della Corte costituzionale rumena rappresenta un esempio (sul punto, in questo blog, seppur con riferimento alla diversa ipotesi di incitamento all'odio, si vedano De Sena e Castellaneta).

Di qui, tuttavia il rischio di eccedere nelle restrizioni, arrivando a configurare una «collateral censorship» che, in periodo elettorale, finirebbe con il rappresentare un'eventualità ancora maggiore dovuta alla difficoltà di distinguere tra disinformazione e semplice diffusione di materiale o opinioni di parte.

4. A livello europeo, si riscontra un sempre maggiore impegno nella lotta alla disinformazione come minaccia ibrida da parte delle Istituzioni e degli Stati.

Infatti, mentre fino al 2020 i tentativi di contrasto alla disinformazione hanno avuto un taglio prevalentemente volontario, in epoca successiva la maggiore attenzione al problema ha determinato l'individuazione di strumenti di soft law e normative.

Di recente, a livello europeo, ha assunto rilevanza il *Democracy Shield*, iniziativa che, proposta in via informale nel dicembre 2023, ha poi assunto veste ufficiale nel luglio 2024, con l'inserimento da parte della Commissione Europea nelle proprie linee guida 2024-2029. Successivamente, nel dicembre 2024, la stessa è stata recepita dal Parlamento europeo, andando ad arricchire il Democracy Action Plan europeo, volto a promuovere, contrastando la disinformazione e le ingerenze di Stati terzi nei processi democratici, elezioni libere e corrette.

Il *Democracy Shield,* a seguito della circostanza che, nell'ambito del report sui rischi redatto dal *World Economic Forum* 2024, le minacce ibride in materia di informazione sono state indicate come il principale rischio che incombe sulle democrazie occidentali, ha suscitato un interesse, ulteriormente aumentato dal recente annullamento delle elezioni in Romania.

In particolare, il *Democracy Shield* si sviluppa in cinque ambiti, riorganizzando idee e proposte avanzate talora in precedenza.

Il primo ambito riguarda il **monitoraggio**, rispetto al quale si è evidenziata la necessità di combattere la disinformazione in maniera preventiva e proattiva, auspicando l'individuazione di un sistema di monitoraggio dei contenuti caricati online dagli utenti, indipendente dalle piattaforme e più facilmente gestibile dagli Stati membri. A tal fine si mira a incrementare le risorse per i *fact-checkers*, in modo da migliorare l'efficacia del loro operato e a uniformare le modalità di monitoraggio attraverso la creazione di apposite *task forces* composte da soggetti pubblici e privati, quali ad esempio il Counter Disinformation Network.

L'idea di creare *task forces* per uniformare il monitoraggio delle minacce ibride e, in particolare, della disinformazione, non è recente.

Infatti, già nel 2015, era stata istituita, da parte dell'European External Action Service (EEAS), l'East Stratcom, cui il Consiglio Europeo aveva dato mandato di contrastare le campagne di disinformazione russe.

L'operato dell'East Stratcom è poi proseguito con l'istituzione, nel 2023, del Foreign Information Manipulation and Interference – Information Sharing and Analysis Centre (FIMI-ISAC), da parte dello stesso EEAS.

Un secondo ambito attiene agli **strumenti** con i quali contrastare in concreto la disinformazione.

La maggiore innovazione in materia è costituita dall'Intelligenza Artificiale, utile ad accelerare e semplificare l'individuazione di contenuti di disinformazione sulle piattaforme online.

Secondo il progetto del *Democracy Shield*, l'IA, già utilizzata in alcune piattaforme, sarà utile non solo a distinguere i contenuti di disinformazione da quelli legittimamente rientranti nella libertà di espressione, ma anche a identificare gli attori e i canali della disinformazione e a distinguere quest'ultima dalla misinformazione, così da consentire agli Stati di assumere i provvedimenti del caso.

Altri strumenti utili per il contrasto alla disinformazione sono quelli volti alla condivisione delle informazioni tra i Paesi, tra i quali il Rapid Alert System (RAS) del 2018, che consente di creare una rete di informazioni condivisa non solo tra gli Stati membri dell'Unione Europea, ma anche tra questi e gli attori privati, così facilitando una risposta coordinata alle minacce ibride.

Non ultimi, tra gli strumenti di contrasto alle minacce ibride, sono le sanzioni che l'Unione Europea applica al fine di eliminare, o quantomeno ostacolare, ingerenze negli affari interni degli Stati membri (*ex multis*, nel mese di ottobre 2024 è stato approvato il regolamento (UE) 2024/2642 che riprende la decisione PESC 2024/2643 in tema di misure restrittive destinate ad arginare l'attività di destabilizzazione da parte della Russia).

Il terzo ambito in cui il *Democracy Shield* intende operare è relativo alla **governance**.

Si auspica, infatti, un aggiornamento della normativa europea e degli strumenti di soft law al fine di ricomprendere al loro interno previsioni volte a contrastare la disinformazione online.

Sull'argomento, oltre all'intento di orientare il Digital Markets Act, il Digital Services Act e l'AI Act verso un più efficace contrasto alla disinformazione, numerose iniziative e previsioni si sono sviluppate nel corso degli anni.

Mentre inizialmente i codici di condotta prevedevano una sorta di autoregolamentazione volontaria in capo alle piattaforme, successivamente, alla *self-regulation* si sono affiancati alcuni obblighi imposti a livello normativo, che hanno consentito di imporne il rispetto a livello europeo, con conseguenti limiti alla discrezionalità dei *service providers*.

In ambito europeo, oltre alle nuove norme, tra le quali ad esempio il regolamento (UE) 2024/900 relativo alla trasparenza e al *targeting* della pubblicità politica e il regolamento (UE) 2024/1083 sulla libertà dei media, sono stati elaborati anche codici di condotta e di buone pratiche, pacchetti di misure (sia sulla protezione dell'integrità delle elezioni che, più in generale, sulla difesa della democrazia), orientamenti che hanno chiarito le modalità applicative delle previsioni in materia di processi elettorali, così rafforzando il contrasto alla disinformazione online nel settore.

Il quarto ambito riguarda il **pluralismo** e la cooperazione tra Istituzioni, Stati e attori non statali.

Al fine di contrastare la disinformazione, infatti, è stata ritenuta necessaria una cooperazione volta a permettere ai cittadini di acquisire maggiore consapevolezza in materia e a rafforzare la diffusione delle informazioni veritiere, attraverso la chiusura di account falsi e la promozione di fonti affidabili, quali quelle giornalistiche.

Nel settore, iniziative sono state assunte da Organizzazioni non governative (si pensi, ad esempio, alla Journalism Trust Initiative), da Stati (come la proposta di un'Agenzia Europea per la Protezione delle Democrazie effettuata dalla Francia) o, ancora, dalle stesse Istituzioni

europee (ad esempio il Joint Action Plan on Disinformation proposto dalla Commissione e dall'Alto Rappresentante o, ancora, le risoluzioni del Parlamento europeo del 2022 e del 2023 in materia di tutela dei processi democratici dalle ingerenze straniere).

Accanto a tali iniziative, la promozione delle fonti affidabili e della veridicità delle informazioni è stata auspicata anche da una risoluzione con la quale, nel 2021, il Parlamento Europeo ha invitato la Commissione Europea a proporre un pacchetto di misure, vincolanti e non, per contrastare il fenomeno degli **SLAPPs**

Per SLAPPs (Strategic Lawsuit Against Public Participation) si intendono quelle azioni legali strategiche tese a bloccare la partecipazione pubblica, avviate da soggetti influenti o finanziariamente forti – tra cui esponenti russi –, che pongano il destinatario in una condizione di svantaggio tale da indurlo all'autocensura o a impedire la partecipazione pubblica dello stesso, attraverso la promozione di procedimenti giudiziari abusivi che vanno a incidere negativamente sulle finanze o sulla reputazione del convenuto.

Sul tema, di particolare interesse, è la Direttiva 2024/1069, definita anche direttiva 'anti-SLAPPs', volta a garantire la partecipazione pubblica, intesa come comprensiva delle libertà di espressione e di informazione, e a tutelare la questione pubblica, inclusiva della lotta alla disinformazione e alle ingerenze illecite nei processi democratici da parte di Paesi terzi, nel rispetto del valore di democrazia, di cui all'art. 2 TUE e del diritto di partecipazione alla vita democratica dell'Unione, stabilito dall'art. 10 par. 3 TUE.

La direttiva riconosce l'esigenza di garantire – a giornalisti, Organizzazioni non governative, accademici e società civile in generale – uno spazio che consenta un «dibattito aperto, libero ed equo per contrastare la disinformazione, la manipolazione delle informazioni e le ingerenze […]», nel quale è ricompresa anche l'informazione via internet (Considerando 8 e ss. della direttiva).

A tal fine, la direttiva invita gli Stati ad adottare nei processi civili validi ed efficaci strumenti, idonei ad evitare procedimenti multipli, a

consentire il rigetto anticipato di domande manifestamente infondate, a imporre cauzioni a garanzia della copertura delle spese legali da parte dell'attore che intenda ostacolare la pubblicazione di contenuti informativi o, ancora, a tutelare il convenuto in caso di procedimenti proposti dinanzi all'organo giudiziario di un Paese extra-europeo.

Il pluralismo ora evidenziato si ricollega poi al quinto e ultimo ambito, che si concentra sulla necessità di favorire la **partecipazione** dei cittadini su larga scala, al fine di adeguare le misure di contrasto alla disinformazione alle esigenze realmente percepite dagli individui.

In conclusione, alla luce dei recenti avvenimenti accaduti in Romania, se per un verso la disinformazione si è confermata come un mezzo efficace per la destabilizzazione delle democrazie, per altro verso gli strumenti che i Paesi target e le Organizzazioni Internazionali hanno per difendersi si sono dimostrati ancora in fase embrionale, anche in ragione della difficoltà di definire in maniera esatta cosa si intenda per minaccia ibrida.

Sulla scia delle iniziative intraprese si inserisce il *Democracy Shield* che, da un lato mira alla razionalizzazione, al fine di aumentarne l'efficacia, degli strumenti volti a contrastare la disinformazione e, dall'altro lato, evidenzia come sia gli Stati, sia le Organizzazioni Internazionali stiano cercando di adeguare il proprio operato al nuovo panorama, quello digitale, divenuto il principale campo sul quale vengono condotte attività di fondamentale importanza per le democrazie, come le campagne elettorali.

Il presente contributo è stato realizzato grazie al finanziamento del Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) per il progetto di ricerca PRIN 2022 PNRR F53D23011940001 intitolato «Minacce ibride e resilienza democratica: un pacchetto di strumenti analitici e pratici (HYDRA)»