dossier

XIX Legislatura

17 novembre 2025

Forum sulla democrazia parlamentare nell'UE

Bruxelles, 19 novembre 2025

Senato della Repubblica

Camera dei deputati

Senato della Repubblica

Camera dei deputati

XIX LEGISLATURA

Documentazione per le Commissioni
RIUNIONI INTERPARLAMENTARI

Forum sulla democrazia parlamentare nell'UE

Bruxelles, 19 novembre 2025

SENATO DELLA REPUBBLICA

SERVIZIO STUDI

SERVIZIO DEGLI AFFARI INTERNAZIONALI
UFFICIO DEI RAPPORTI CON LE ISTITUZIONI DELL'UNIONE EUROPEA

N. 148

CAMERA DEI DEPUTATI

SERVIZIO PER I RAPPORTI CON L'UNIONE EUROPEA

N. 82

Senato della Repubblica

SERVIZIO STUDI

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

Dossier n. 148

SERVIZIO DEGLI AFFARI INTERNAZIONALI

Ufficio dei rapporti con le istituzioni dell'Unione Europea

TEL. 06 6706 5785 – affeuropei@senato.it

Camera dei deputati

SERVIZIO PER I RAPPORTI CON L'UNIONE EUROPEA

TEL. 06 6760 2145 – rue_segreteria@camera.it - @CD_europa - europa.camera.it.

Dossier n. 82

Servizio Studi – Dipartimento istituzioni

TEL. 06 6760 3855 – st_istituzioni@camera.it

I N D I C E

European Parliament | Hemicycle | 19 November 2025

Programme

09:00 – 11:00 | Registration of participants and welcome coffee

11:00 – 11:30 | Opening Session: "The Role of Parliaments in Defending Democracy"

Opening addresses:

- **Roberta Metsola**, President of the European Parliament
- **Søren Gade**, Speaker of the Danish Parliament

Family Photo

Keynote intervention:

- **María Ressa**, Journalist and Nobel Peace Prize Laureate (online)

11:30 – 13:00 | Session I: Strengthening Parliamentary Democracy through Citizen Engagement

Exploring strategies and best practices to strengthen trust in democracy and its institutions, with a focus on grassroots movements, citizen participation, and youth engagement in democratic processes.

Scene setter:

- **Kalypso Nicolaidis,** Chair in Global Affairs at the School of Transnational Governance (EUI)

Open debate with keynote remarks by:

- **Sven Simon,** Chair of the Committee on Constitutional Affairs (AFCO), European Parliament
- **Nicolae Ștefănuță,** Vice-President for Relations with European civil society organisations, including the European Citizens' Initiative, European Parliament
- **José Pedro Correia de Aguiar-Branco,** President of the Assembly of the Republic of Portugal

Moderated by:

- **Emilie Tournier,** Deputy Spokesperson, Directorate-General for Communication, European Parliament
- **David Lundy,** Communications Advisor, Directorate-General for Parliamentary Democracy Partnerships, European Parliament

13:00 – 14:30 | Lunch Break

14:30 – 16:00 | Session II – Overcoming Political Polarisation

Exploring the causes and consequences of deepening ideological divisions within democratic societies; examining the rise in violence against politicians; discussing measures, including the role of parliamentarians, to reduce polarisation and promote democratic dialogue.

Scene setter:

- **Ken Godfrey,** Executive Director of the European Partnership for Democracy (EPD)

Open debate with keynote remarks by:

- **Javier Zarzalejos**, Chair of the Committee on Civil Liberties, Justice and Home Affairs (LIBE), European Parliament
- **Raya Nazaryan,** President of the National Assembly of the Republic of Bulgaria
- **Katarina Barley,** Vice-President for Relations with National Parliaments, European Parliament
- **Kamzy Gunaratnam,** Member of the Parliament of the Kingdom of Norway

Moderated by:

- **Sarah Sheil**, Director for Members' Research Service, Directorate-General for Parliamentary Research Services, European Parliament
- **James Maher,** Deputy Spokesperson, Directorate-General for Communication, European Parliament

16:00 – 16:40 | Conversation with Michael McGrath, Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection

Chaired by:

- **Esteban González Pons**, Vice-President for Relations with National Parliaments, European Parliament

16:40 – 17:10 | Coffee Break

17:10 – 18:40 | Session III – Building Resilience

Exploring tools and policies, aligned with the European Democracy Shield, to protect democracies against hybrid threats, foreign interference, disinformation, cyber threats, and other vulnerabilities, while also examining the role of technology in strengthening democratic processes.

Scene setter:

- **Paula Gori,** Secretary-General and Coordinator of the European Digital Media Observatory (EDMO)

Open debate with keynote remarks by:

- **Nathalie Loiseau,** Chair of the Special Committee on the European Democracy Shield (EUDS), European Parliament
- **Radu Marian,** Chair of the Economic, Budget and Finance Committee, Parliament of the Republic of Moldova
- **Peeter Tali,** Chair of the EU Affairs Committee**,** Parliament of the Republic of Estonia
- **George Papandreou,** General Rapporteur on Democracy for the Parliamentary Assembly of the Council of Europe (PACE)

Moderated by:

- **Delphine Colard,** Spokesperson, Directorate-General for Communication, European Parliament
- **Philip Tulkens,** Director for ICT Infrastructure and Security Operations, Directorate-General for Information Technologies and Cybersecurity, European Parliament

18:40 – 19:00 | Closing Session: "Towards a Partnership on Parliamentary Democracy"

Speakers:

- **Esteban González Pons,** Vice-President for Relations with National Parliaments, European Parliament
- **Katarina Barley,** Vice-President for Relations with National Parliaments, European Parliament

Moderated by:

- **Sanna Lepola,** Director-General for Parliamentary Democracy Partnerships, European Parliament

19:00 – 20:00 | Networking Reception ***(by registration only)***

SESSIONE I – RAFFORZARE LA DEMOCRAZIA PARLAMENTARE ATTRAVERSO IL COINVOLGIMENTO DEI CITTADINI

Gli strumenti di partecipazione diretta ai processi decisionali europei

Ai sensi degli articoli 20, 24 e 227 del **Trattato sul funzionamento dell'Unione europea** (TFUE) e articolo 44 della **Carta dei diritti fondamentali dell'Unione europea**, i cittadini dell'Unione godono di una serie di diritti che rafforzano il legame tra istituzioni e società civile. Essi comprendono il diritto di presentare **petizioni al Parlamento europeo**, di ricorrere al **Mediatore europeo**, nonché di rivolgersi alle **istituzioni** e agli **organi consultivi dell'Unione** in una qualsiasi delle lingue ufficiali dei trattati, ricevendo risposta nella stessa lingua.

Il diritto di petizione

Il diritto di petizione mira a offrire ai cittadini dell'Unione europea e a coloro che vi risiedono un mezzo semplice per rivolgersi alle istituzioni dell'UE, al fine di formulare denunce o richieste di intervento.

Il diritto di petizione è **accessibile** a qualsiasi cittadino dell'Unione e a ogni persona fisica o giuridica che risieda o abbia la sede sociale in uno Stato membro, individualmente o in associazione con altri. Per essere **ricevibili**, le petizioni devono riguardare materie che rientrano nel campo di attività dell'Unione europea e che la concerna direttamente: quest'ultima condizione è applicata in senso molto ampio (articolo 227 del TFUE).

In base ai Trattati, il **Parlamento europeo** è il destinatario delle petizioni e pertanto su di esso ricade la responsabilità di garantire che le questioni sollevate in tali petizioni siano tenute pienamente in considerazione in seno all'UE. A tale scopo, è stata istituita una commissione apposita, la **Commissione per le petizioni** (PETI), con il compito di gestire le petizioni e coordinare le attività connesse. Come evidenziato nelle sue relazioni annuali della Commissione PETI[1], il Parlamento ha sempre considerato le petizioni un elemento fondamentale della democrazia partecipativa. Ha altresì sottolineato la loro importanza nel segnalare casi di recepimento e attuazione non corretti del diritto dell'UE da parte degli Stati membri. Infatti,

[1] Le relazioni annuali sulle deliberazioni della Commissione per le petizioni comprendono informazioni sul numero delle petizioni ricevute, sul loro formato, stato, esito, paese, lingua, nazionalità e argomento, sul portale web, sulle relazioni con la Commissione, il Consiglio e il Mediatore, sulle missioni di informazione, le audizioni pubbliche, gli studi commissionati e altre questioni fondamentali.

diverse petizioni hanno dato luogo ad azioni legislative o politiche, pronunce pregiudiziali o procedure di infrazione.

La **Commissione per le petizioni** ricopre dunque un ruolo fondamentale per la piena attuazione dell'istituto in esame. Nello specifico la Commissione PETI è competente per:

1. Le **petizioni**;
2. L'organizzazione di **audizioni pubbliche** relative alle iniziative dei cittadini (ICE) ai sensi dell'articolo 236 del Regolamento del Parlamento europeo;
3. Le **relazioni con il Mediatore europeo**.

Per assicurare che le questioni oggetto delle petizioni siano trattate e risolte, è disponibile un'ampia gamma di strumenti: le missioni di informazione, le audizioni pubbliche, i seminari, la realizzazione di studi, la creazione nel 2016 di una rete per le petizioni, tesa a garantire una maggiore cooperazione con le altre commissioni in relazione alle petizioni, così come la cooperazione e il dialogo con i Parlamenti e le Autorità nazionali, nonché con le altre istituzioni dell'UE (in particolare la Commissione e il Mediatore europeo).

Nel **2014** il Parlamento ha inoltre lanciato il portale *web* per le petizioni, che ha migliorato il profilo pubblico e la trasparenza nella trattazione delle petizioni.

La **procedura per il trattamento delle petizioni** è stabilita dagli articoli da 226 a 230 e dall'allegato VI (XX) del regolamento del Parlamento europeo.

Il monitoraggio dell'applicazione del diritto UE da parte della Commissione PETI

PETI svolge un ruolo fondamentale nello stimolo e nel controllo dell'applicazione del diritto dell'UE: nella trattazione delle petizioni ricevute, valuta se esse rientrino nelle competenze legislative europee e se inviare una segnalazione alla Commissione europea per ulteriori indagini.

Inoltre, la Commissione PETI può anche dare impulso all'avvio di **procedure di "EU Pilots"** trasmettendo le questioni denunciate nelle petizioni alla Commissione europea, la quale, eventualmente, attiva il meccanismo pre-contenzioso[2].

[2] **EU Pilot** è una procedura informale di dialogo tra la Commissione europea e lo Stato membro interessato, volta a chiarire e risolvere rapidamente possibili violazioni del diritto dell'Unione senza dover ricorrere immediatamente alla procedura d'infrazione: la Commissione formula domande e richieste di chiarimento allo Stato membro, che deve rispondere entro termini stabiliti e proporre eventuali misure correttive.

Il ruolo dei cittadini nel processo di monitoraggio e applicazione del diritto UE è infatti ritenuto fondamentale in quanto **fonte diretta di informazioni** per la Commissione in merito alle violazioni del diritto europeo o alla sua non corretta applicazione.

L'attività di controllo e stimolo alla produzione del diritto europeo, così come alla valutazione della sua applicazione, si evince anche dai numerosi **rapporti pubblicati** dalla Commissione PETI relativi alle attività svolte dalla Commissione stessa, dal Mediatore europeo o alle Iniziative Cittadine Europee (ICE).

L'attività della commissione PETI

Durante la 9ª legislatura (2019-2024), un numero significativo di petizioni esaminate dalla commissione PETI hanno spesso contribuito ad avviare azioni legislative o politiche, procedure EU Pilot e, in alcuni casi, procedure di infrazione. Nell'ottobre 2023 PETI ha interrogato la Commissione europea sulla **gestione delle violazioni del diritto UE**, ribadendo il ruolo delle petizioni nella segnalazione delle irregolarità.

Tra le attività più rilevanti rientrano il contributo alla tutela dei diritti dei cittadini nei **negoziati sulla Brexit** e l'attenzione all'impatto sui diritti fondamentali delle **misure adottate in conseguenza della pandemia** Covid. Particolare impegno è stato dedicato alla tutela ambientale, con una missione in Romania, nel maggio 2023, sul **disboscamento illegale** che ha portato all'apertura di una procedura di infrazione, e con un'audizione, insieme alla Commissione giuridica (JURI), nel marzo 2022, per verificare **l'applicazione del diritto penale ambientale dell'UE** ed esaminare l'adozione di nuovi strumenti per combattere i reati ambientali.

Nel campo dei **diritti fondamentali** PETI ha svolto iniziative significative. Nell'ottobre 2023 la Presidente della Commissione ha visitato **Famagosta**, **a Cipro,** per ribadire la **condanna delle violazioni dello status quo** e sostenere la richiesta di restituire l'area ai suoi cittadini sotto amministrazione ONU, come previsto dalle risoluzioni europee e internazionali.

Nell'ambito della **lotta contro le discriminazioni**, la Commissione ha organizzato audizioni sulla tutela delle diversità culturali e linguistiche e sui diritti delle famiglie arcobaleno, sostenendo le relative risoluzioni del Parlamento europeo, tra cui quella sui **diritti LGBTI+**. Inoltre, ha svolto un ruolo decisivo nel promuovere l'istituzione di una **Carta europea della disabilità**.

La Commissione PETI ha svolto un ruolo rilevante anche in materia di **diritti del lavoro**, sollecitando la Commissione europea ad avviare una **procedura di infrazione contro l'Italia** per le condizioni di impiego dei magistrati onorari.

Nel settore delle **piccole e medie imprese**, la sua iniziativa è stata determinante per l'adozione della risoluzione che ha istituito la Capitale europea del commercio locale, presentata ufficialmente dalla Commissione europea a Barcellona nel dicembre 2023. Parallelamente, PETI ha promosso diverse azioni a tutela della **libertà di movimento**, intervenendo sulla protezione dei diritti dei passeggeri aerei, in particolare per i rimborsi dei voli cancellati durante la pandemia, e monitorando il rispetto dei principi Schengen, con particolare attenzione alla rimozione dei controlli "temporanei" alle frontiere. Infine, nel 2023 è stato lanciato un **nuovo portale web** per semplificare e rendere più immediato l'esercizio del diritto di petizione da parte dei cittadini.

Il mediatore europeo

Fra i diritti dei cittadini dell'Unione europea, vi è quello di rivolgersi al Mediatore europeo ("*European Ombudsman*") per trasmettere denunce relative a casi di cattiva amministrazione delle istituzioni, degli organi e degli organismi dell'Unione europea. L'organo è disciplinato dal **Trattato sul funzionamento dell'Unione Europea** (TFUE) all'art. 228 e dal Regolamento (UE, Euratom) 2021/1163 del Parlamento europeo che fissa lo **statuto** del Mediatore codificando molte sue prassi, fra cui il potere di avviare indagini di propria iniziativa.

L'introduzione del Mediatore europeo nell'ordinamento comunitario risale, tuttavia, al 1992, con il Trattato di Maastricht, al fine di **migliorare la protezione di qualsiasi persona fisica o giuridica** che risieda in uno Stato membro in relazione a casi di cattiva amministrazione nell'azione degli organismi dell'UE, nonché di **potenziare la trasparenza e la responsabilità democratica** del processo decisionale e dell'amministrazione delle istituzioni.

Il Mediatore europeo è **eletto dal Parlamento europeo**, per tutta la durata della legislatura, con la possibilità di rinnovo del mandato. Anche la **Commissione PETI** svolge un ruolo importante nella sua elezione, essendo la **responsabile per l'audizione dei candidati**. Nello svolgere le sue funzioni, il Mediatore deve essere indipendente e rimanere assolutamente imparziale; inoltre, ha l'obbligo di astenersi da atti incompatibili con il suo mandato e non può esercitare qualsiasi altra funzione politica o amministrativa, o qualsiasi altra attività professionale.

Il Mediatore europeo può essere dichiarato **dimissionario** dalla Corte di Giustizia dell'UE (CGUE), su richiesta del Parlamento europeo, qualora non risponda più alle condizioni necessarie all'esercizio delle sue funzioni o abbia commesso una colpa grave.

Conformemente alle sue funzioni, il mediatore conduce le indagini che ritiene giustificate, **di propria iniziativa** o a seguito di una **denuncia per casi di cattiva amministrazione** delle istituzioni dell'Unione. L'unica eccezione per cui il mediatore non può recepire una denuncia, si verifica nei casi in cui essa sia rivolta contro la CGUE nell'esercizio delle sue funzioni giurisdizionali. Inoltre, non gli è possibile mettere in discussione la fondatezza delle decisioni di un organo giurisdizionale o la sua competenza a emettere una decisione.

Le denunce al Mediatore possono essere **esposte direttamente** - quindi da qualsiasi cittadino dell'UE o da qualsiasi persona, fisica o giuridica, che risieda o abbia sede sociale in uno Stato membro - o **tramite un membro del Parlamento europeo**. I denuncianti hanno la facoltà di rivolgersi al Mediatore solo dopo aver contattato l'ente di riferimento per la risoluzione del caso. I denuncianti, entro due anni dalla presa conoscenza dei fatti, possono rivolgersi al mediatore tramite posta o attraverso un sistema online raggiungibile tramite una pagina *web* dedicata.

La procedura d'indagine del Mediatore europeo

La prima fase delle indagini sul caso proposto è relativa alla **verifica di validità della denuncia presentata**. Se il mediatore ritiene quindi che il problema rientri nelle sue competenze, apre l'indagine.

Nel corso delle indagini il mediatore ha la facoltà di **chiedere informazioni alle istituzioni europee**, nonché alle autorità degli Stati membri. Se l'assistenza richiesta non viene fornita, il mediatore informa il Parlamento europeo, che prenderà le opportune iniziative sul caso. Il Mediatore ha anche la possibilità di cooperare con le autorità corrispondenti degli Stati membri. Se l'oggetto della cooperazione, a parere del mediatore, ha rilevo penale, dovrà essere comunicato immediatamente alle autorità nazionali competenti e all'Ufficio europeo per la lotta antifrode (OLAF).

Se il Mediatore consta un effettivo caso di cattiva amministrazione da parte di un organismo europeo, sarà suo compito **contattare l'ente interessato** e con esso cercare una soluzione atta a risolvere la questione. L'organo interessato entro tre mesi dovrà fornire una **risposta ufficiale** in cui giustifichi o spieghi le proprie azioni.

Qualora l'organo interessato non accetti le raccomandazioni proposte, il Mediatore europeo redige una relazione speciale da presentare al Parlamento europeo e informa il denunciante sull'esito delle indagini e sulle eventuali raccomandazioni proposte per sanare la situazione denunciata. I cittadini hanno il diritto di **accedere ai documenti**, ad eccezione di quelli ottenuti nel corso di un'indagine e conservati dal Mediatore durante o dopo la conclusione della stessa.

Il Mediatore presenta **ogni anno** al Parlamento europeo una **relazione** sulle indagini condotte e sui relativi risultati.

L'iniziativa dei cittadini europei (ICE)

Un altro importante strumento di democrazia partecipativa nell'UE è rappresentato dall'istituto dell'Iniziativa dei cittadini europei (ICE), grazie al quale è possibile per i cittadini europei presentare alla Commissione europea una proposta di atto giuridico.

La base giuridica di riferimento per tale strumento è individuata in:

- l'art.11, par. 4 del Trattato sull'Unione Europea (TUE);
- l'art. 24, par.1 del Trattato sul Funzionamento dell'Unione Europea (TFUE);
- i regolamenti (UE) n. 211/2011 e (UE) n.2019/788;
- l'art. 236 del regolamento del Parlamento europeo.

È opportuno distinguere le ICE dalle petizioni: quest'ultime sono istanze individuali di natura propositiva rivolte al Parlamento europeo, che possono avere un carattere pubblico o comunque essere relative ad una pluralità di oggetti, ma sono svincolate dal procedimento legislativo. Al contrario, le ICE sono **richieste dirette**, indirizzate alla Commissione Europea - che detiene nell'ordinamento europeo il potere di iniziativa legislativa - e finalizzate alla **produzione di un atto giuridico europeo**. L'iniziativa popolare è pertanto espressione di più diretta partecipazione dei cittadini europei alle dinamiche legislative dell'UE

Le differenti fasi dell'ICE

Per poter avviare una procedura ICE deve esserci un comitato organizzativo, denominato "**comitato dei cittadini**", composto da almeno sette cittadini residenti in almeno sette Stati membri diversi, con diritto di voto per le elezioni europee. Tale comitato, prima di poter raccogliere le dichiarazioni di sostegno dei cittadini, deve registrare l'iniziativa presso la Commissione europea sottoforma di documento indicante il titolo, l'oggetto e la descrizione dell'iniziativa stessa, nonché la sua base giuridica.

La Commissione ha **due mesi** per decidere in merito alla **registrazione della proposta**. In particolare, la proposta non sarà recepita qualora manchino dei requisiti procedurali, esuli dai poteri della Commissione in materia di iniziativa legislativa o, infine, sia manifestamente irrilevante, ingiuriosa, vessatoria o contraria ai valori dell'Unione. Si segnala, inoltre, che la Commissione può registrare parzialmente le iniziative. Le iniziative registrate sono pubblicate sul portale *web* della Commissione.

Dopo la registrazione, entro **12 mesi**, è possibile per gli organizzatori raccogliere (in formato cartaceo o online) il sostegno di **almeno 1 milione di cittadini europei**, con un numero minimo di firme in **almeno 7 paesi dell'UE**. I firmatari devono compilare un apposito modulo di dichiarazione di sostegno. Concluso tale passaggio, gli organizzatori devono presentare le dichiarazioni alle autorità nazionali competenti per la loro certificazione.

L'ultima fase dell'ICE è relativa alla presentazione e all'esame. Dopo aver ricevuto l'iniziativa, la Commissione la pubblica in un registro e incontra i presentatori. È altresì possibile che il Parlamento europeo organizzi un'audizione pubblica. Entro **sei mesi**, la Commissione deve rispondere ad un'iniziativa legittimamente presentata, fornendo un elenco concreto delle azioni che intende intraprendere.

Ad oggi, **undici iniziative** hanno raggiunto la soglia minima di firme richiesta e hanno ricevuto una risposta formale da parte della Commissione europea. Per ciascuna di esse, il Parlamento europeo ha organizzato audizioni pubbliche con i rappresentanti delle iniziative.

Un'ulteriore iniziativa, *My Voice, My Choice: For Safe and Accessible Abortion* (La mia voce, la mia scelta: per un aborto sicuro e accessibile), è attualmente all'esame della Commissione europea, mentre per altre tre iniziative è in corso la verifica delle firme da parte degli Stati membri: *Stop Destroying Videogames* (Mettiamo fine alla distruzione dei videogiochi), *Ban on Conversion Practices in the European Union* (Vietare le pratiche di conversione nell'Unione europea) e *Stop Extremism* (Ferma l'estremismo).

Misure esistenti per il coinvolgimento dei giovani nei processi democratici dell'UE

L'Unione ha promuove il dialogo, l'ascolto e la creazione di politiche mirate, di strategie e di strumenti per il coinvolgimento e la partecipazione dei giovani al processo decisionale europeo, al fine di renderlo più inclusivo e rappresentativo.

Tra gli strumenti più consolidati figura il **Dialogo dell'UE con i giovani** (*EU Youth Dialogue*), che costituisce il principale canale di confronto politico tra le istituzioni europee e le nuove generazioni. Nato nell'ambito della Strategia dell'UE per la gioventù 2019–2027, il Dialogo mira ad attuare gli obiettivi strategici della politica giovanile europea, promuovendo la partecipazione civica e la cittadinanza attiva. Il processo si articola in **cicli di 18 mesi**, ciascuno dedicato a un tema politico specifico: quello corrente (1° gennaio 2025 - 30 giugno 2026) è intitolato "*Connecting EU with Youth*" ("Connettere l'UE con i giovani").

Il Dialogo è strutturato in **Gruppi di lavoro nazionali** che organizzano consultazioni, eventi e attività di scambio con decisori politici e organizzazioni giovanili. Il coordinamento è assicurato dal **trio delle Presidenze del Consiglio dell'UE**, in collaborazione con la **Commissione europea** e le **Agenzie nazionali per la gioventù**. Nel 2018, questo processo ha avuto come esito l'elaborazione degli 11 Obiettivi europei per la gioventù (*Youth Goals*), che sono stati successivamente integrati - a seguito di un negoziato politico in seno al Consiglio - nella **Strategia dell'UE per la gioventù.**

Le **Conferenze europee sulla gioventù** (*European Youth Conferences*, EYC), organizzate due volte l'anno, rappresentano il momento culminante del Dialogo. Esse riuniscono giovani delegati e rappresentanti delle istituzioni al fine di discutere i risultati delle consultazioni nazionali e tradurli in **raccomandazioni comuni**. Le conclusioni di ciascuna conferenza vengono presentate al Consiglio dell'UE, che può farne oggetto di un documento politico di sintesi. Un esempio recente è la Conferenza europea sulla gioventù svoltasi a **Copenaghen** (21-23 settembre 2025), che ha offerto una piattaforma di confronto tra i Consigli nazionali della gioventù e le organizzazioni giovanili internazionali.

Tra le occasioni più significative di partecipazione diretta figura inoltre lo "***European Youth Event***" (EYE), organizzato annualmente dal Parlamento europeo a **Strasburgo**. L'evento riunisce migliaia di giovani europei per discutere proposte, scambiare esperienze e confrontarsi con deputati, esperti e attivisti. L'edizione 2025 ha visto la partecipazione di 2.586 giovani e lo svolgimento di oltre 400 attività in presenza e *online*, tra dibattiti, laboratori, incontri, momenti artistici e sportivi.

La partecipazione giovanile è promossa anche attraverso iniziative periodiche come la **Settimana europea della gioventù**, organizzata ogni due anni dalla Commissione europea. L'edizione 2024, dedicata al tema "*Voice your vision*" ("*Dai voce alla tua visione*"), ha posto l'accento sulla democrazia e sulle elezioni europee, coinvolgendo oltre 1,8 milioni di partecipanti in 39 paesi.

In un'ottica di cooperazione interistituzionale e paneuropea, il **Partenariato giovanile UE-Consiglio d'Europa** (*EU-Council of Europe Youth Partnership*), istituito nel **1998**, svolge un ruolo di rilievo nel sostegno allo sviluppo delle politiche giovanili. Attraverso attività di ricerca, formazione e scambio di buone pratiche, il partenariato contribuisce ad accrescere la conoscenza condivisa e a rafforzare la coerenza tra le iniziative delle due organizzazioni in materia di gioventù.

In questo contesto si inserisce anche il **Forum europeo della gioventù** (*European Youth Forum*, EYF), piattaforma *non profit* che riunisce oltre cento organizzazioni giovanili di tutta Europa. Il Forum opera per rafforzare il ruolo dei giovani come partner a pieno titolo nei processi decisionali europei e internazionali, collaborando attivamente con l'UE, il Consiglio d'Europa e le Nazioni Unite.

Più in generale, l'impegno dell'UE nel favorire la partecipazione giovanile ha conosciuto un rinnovato slancio dopo la **pandemia di COVID-19**, che ha inciso profondamente sulle prospettive sociali, economiche e professionali dei giovani europei. Nel suo discorso sullo **Stato dell'Unione del 2021**, la Presidente della Commissione europea **Ursula von der Leyen** ha annunciato la proclamazione del 2022 "**Anno europeo dei giovani**" (*European Year of Youth*, EYY), con l'obiettivo di valorizzare la voce delle nuove generazioni nel processo di sviluppo dell'Unione europea.

I giovani e la Conferenza sul Futuro dell'Europa

La **Conferenza sul Futuro dell'Europa** (CoFE), svoltasi tra il **2021** e il **2022**, ha rappresentato un'esperienza molto qualificante di coinvolgimento diretto dei cittadini, e in particolare dei giovani, nei processi democratici dell'Unione. L'iniziativa ha introdotto un modello innovativo di democrazia partecipativa, fondato sui ***panel*** **dei cittadini europei**, concepiti per elaborare proposte concrete in diversi ambiti di politica pubblica.

La composizione dei *panel* è stata definita per assicurare una **rappresentanza equilibrata delle società europee** in termini di nazionalità, genere, età, background socioeconomico e livello di istruzione, con una **sovrarappresentazione dei giovani**: almeno un terzo dei partecipanti aveva meno di 25 anni. Tale scelta ha contribuito a garantire che le priorità e le prospettive giovanili fossero pienamente integrate nei lavori della Conferenza.

I risultati della CoFE includono **raccomandazioni** mirate ai bisogni delle nuove generazioni, come la richiesta di **tirocini retribuiti**, **maggiori tutele sociali** e **politiche abitative accessibili**. È stata inoltre avanzata la proposta di introdurre una valutazione d'impatto giovanile per le nuove normative e strategie dell'UE, al fine di assicurare che ogni politica sia esaminata anche attraverso la lente delle esigenze dei giovani europei.

Strumenti di democrazia partecipativa nell'ordinamento italiano *(a cura del Servizio Studi della Camera dei deputati)*

L'iniziativa legislativa popolare

L'iniziativa legislativa popolare è prevista dall'articolo 71, secondo comma, Cost., come un'ipotesi di esercizio diretto, da parte di una frazione del corpo elettorale (almeno **cinquantamila elettori**), di una funzione istituzionale (presentazione di un progetto di legge, redatto in articoli) che interviene nel procedimento di formazione delle leggi, ma solo limitatamente alla fase dell'iniziativa.

Per l'esame parlamentare dei progetti di legge di iniziativa popolare si seguono le **normali procedure** previste per tutti gli altri progetti di legge. Il regolamento del Senato (art. 74, comma 3) prevede tuttavia una **procedura accelera**ta per l'inizio dell'esame in **sede referente**: le competenti Commissioni debbono avviare l'esame dei progetti di iniziativa popolare **entro un mese** dal deferimento e concluderlo **entro 3 mesi** dall'assegnazione. Decorso tale termine, il disegno di legge è **iscritto d'ufficio** nel calendario dei lavori dell'Assemblea.

Il Regolamento della Camera, a sua volta, richiama i progetti di legge di iniziativa popolare nelle disposizioni relative alla programmazione dei lavori (art. 24, comma 4) prevedendo che degli stessi non si tiene conto ai fini del **calcolo della quota** del tempo disponibile per gli argomenti indicati dai gruppi dissenzienti e di opposizione.

I regolamenti di entrambe le Camere prevedono inoltre procedure particolari per l'esame dei progetti di legge di iniziativa popolare presentati nella precedente legislatura (c.d. **repêchage**) e il cui esame non si sia potuto in essa concludere: tali progetti si considerano **automaticamente presentati nella successiva legislatura** e per il loro esame si possono applicare le procedure accelerate previste in via generale per l'esame di progetti già approvati nella precedente legislatura.

Nelle ultime legislature il **numero** di progetti di iniziativa popolare presentati alla Camera o al Senato è stato: **33 progetti** nella XIII; **34** nella XIV; **20** nella XV; **27** nella XVI; **46** nella XVII; **32** nella XVIII.

Solamente una **esigua minoranza** di questi sono stati approvati definitivamente, e tutti **abbinati** ad altri disegni o proposte di legge.

Nella legislatura in corso, al 12 novembre 2025, risultano presentate **21 proposte di legge** di iniziativa popolare: **13** alla Camera e **8** al Senato.

Di queste una è diventata legge: si tratta della proposta di legge A.C. 1573, approvata, con modificazioni, dalla legge 15 maggio 2025, n. 76 recante

disposizioni per la **partecipazione dei lavoratori** alla **gestione**, al **capitale** e agli **utili** delle **imprese**.

Delle altre proposte di legge di iniziativa popolare alcune sono in corso di discussione.

Le petizioni

Il **diritto di petizione** è attribuito dall'art. 50 Cost. a tutti i cittadini "per chiedere provvedimenti legislativi o esporre comuni necessità".

La petizione si configura, analogamente all'iniziativa legislativa popolare, come atto di **impulso** dell'attività parlamentare, potendosi però riferire, a differenza della prima, anche ad **attività di indirizzo politico o di controllo**. La limitata efficacia dell'istituto riscontrata è tra l'altro connessa al fatto che dalla presentazione di una petizione **non consegue** per le Camere **l'obbligo** di adottare alcuna decisione.

Il regolamento della Camera infatti, pur configurando come **obbligatorio** l'esame delle petizioni (l'art. 109, comma 1 prevede che "le petizioni pervenute alla Camera sono esaminate dalle Commissioni competenti") lascia **libere** le **Commissioni** di **decidere** sia sul se che sul come deliberare in merito alla petizione (ai sensi del comma 2 dell'art. 109 "l'esame in Commissione **può concludersi** con una **risoluzione** diretta ad interessare il Governo alle necessità esposte nella petizione ovvero con una decisione di **abbinamento** con un eventuale progetto di legge all'ordine del giorno"); il regolamento del Senato attribuisce invece alle Commissioni la **facoltà**, per le petizioni non attinenti a disegni di legge già assegnati alle stesse, di **deliberare** la presa in considerazione o l'archiviazione della petizione (art. 141 reg. Senato).

Le petizioni possono essere presentate alla Camera dei deputati:

- tramite l'apposita piattaforma "Petizioni online", se in possesso di **SPID** o **carta d'identità elettronica**;
- per **posta** ordinaria o elettronica;
- consegnandole **a mano** presso gli uffici.

Al 12 novembre 2025 risultano assegnate alla Camera 1301 petizioni. Di queste la petizione n. 302 per chiedere norme per contrastare la pratica della maternità surrogata è stata abbinata all'esame della proposta di legge A.C. 887 "Modifica all'articolo 12 della legge 19 febbraio 2004, n. 40, in materia di perseguibilità del reato di surrogazione di maternità commesso all'estero da cittadino italiano", poi approvata con la legge 4 novembre 2024, n. 169.

Al Senato risultano presentate 1514 petizioni.

Le consultazioni pubbliche

Negli ultimi anni si vanno sempre più diffondendo **procedure di consultazione pubblica** effettuate prevalentemente dalle amministrazioni centrali, in relazione a documenti contenenti la definizione di obiettivi, scelte di fondo e azioni prioritarie che si vorrebbero quanto più possibile condivisi, nell'interesse generale del Paese.

In generale lo scopo della consultazione è esplicitato dai soggetti che le promuovono nel senso di acquisire elementi di valutazione, spunti di riflessione, osservazioni e proposte da parte di tutti gli interessati.

Tra i benefici dell'apertura ai contributi esterni di coloro che hanno un interesse nei confronti della decisione pubblica vengono di solito evidenziati:

- **trasparenza**: maggiore partecipazione alla costruzione dei contenuti delle decisioni significa assicurare ai cittadini uno strumento ulteriore di controllo sull'attività delle amministrazioni.
- **accessibilità**: per i cittadini, un governo più inclusivo e disposto ad ascoltare, e accogliere, le opinioni dei destinatari delle decisioni. A sua volta, dalla partecipazione il Governo trae indicazioni preziose, utili a modellare la propria attività sulla base delle esigenze concrete della "base", i cittadini e le imprese.
- allineamento ai **principi generali europei** in tema di consultazioni pubbliche.

L'importanza di questo strumento di valutazione per le decisioni relative delle politiche pubbliche è testimoniata dalla adozione, da parte del Governo, delle Linee guida sulla consultazione pubblica in Italia nel marzo 2017, che fornisce alcuni principi generali, ispirate alle raccomandazioni e alle migliori pratiche internazionali, finalizzati ad affinare i processi di consultazione pubblica in modo che siano in grado di condurre a decisioni informate e di qualità e siano il più possibile inclusivi, trasparenti ed efficaci.

Iniziative di consultazione pubblica sono state avviate anche dal Parlamento.

La **Camera dei deputati** ha avviato lunedì 27 ottobre 2014 la consultazione pubblica sulla bozza della Dichiarazione dei diritti in Internet elaborata dalla Commissione per i diritti e i doveri relativi ad Internet istituita dalla Presidente della Camera Boldrini. La Dichiarazione è stata approvata dalla Commissione e pubblicata il 28 luglio 2015.

Sempre su iniziativa della Presidente della Camera si è svolta nel 2016 la consultazione pubblica on line su Lo stato e le prospettive dell'Unione europea. Si tratta di un questionario in sette domande, elaborato in

collaborazione con l'Istat, al quale è stato possibile accedere attraverso il sito della Camera da febbraio ad agosto 2016. I risultati della consultazione, cui hanno preso parte oltre 10mila persone, sono stati presentati il 15 settembre 2016.

Il **Senato** ha adottato nel settembre 2017 le Linee guida per le consultazioni pubbliche che definiscono i princìpi e le procedure per garantire e facilitare una partecipazione corretta ed efficace dei cittadini all'attività parlamentare.

La Commissione Ambiente del Senato ha svolto nella XVII legislatura una consultazione pubblica per acquisire informazioni e valutazioni delle parti interessate al pacchetto di misure sull'economia circolare. L'iniziativa della Commissione Ambiente del Senato è stata aperta a tutti coloro - cittadini, autorità, imprese, Università, centri di ricerca - che desiderassero partecipare al processo decisionale europeo con osservazioni sul merito delle proposte legislative.

Sulle consultazioni pubbliche del Senato si veda la pagina dedicata sul sito del Senato.

SESSIONE II - SUPERARE LA POLARIZZAZIONE POLITICA

La seconda sessione del Forum è dedicata al tema del **superamento** della **polarizzazione politica**, anche con riferimento alle varie forme di violenza che si registrano nei confronti di esponenti politici.

Secondo una breve nota predisposta dal Servizio di ricerca e documentazione del Parlamento europeo (ERPS) in vista del Forum, il termine "polarizzazione" descrive la divisione della società in gruppi contrapposti e l'acuirsi dei conflitti ideologici, politici, sociali ed emotivi. Negli anni recenti, rileva la nota, l'**insoddisfazione dei cittadini** per la situazione economica, sociale e ambientale e la **sfiducia nella capacità delle élite politiche** di risolvere i problemi hanno alimentato la polarizzazione e rafforzato i movimenti populisti. I media, e in particolare i ***social media***, sono da più parti considerati i principali responsabili di questa situazione, poiché spesso favoriscono la polarizzazione e contribuiscono a una retorica divisiva nel confronto politico. Anche **l'interferenza straniera** è spesso alla base di campagne *online* che promuovono disinformazione e narrazioni polarizzanti.

La scheda ricorda anche che in materia l'UE detiene la **competenza di monitorare** il rispetto dei valori fondamentali sanciti all'articolo 2 del Trattato sull'Unione Europea (TUE), quali la democrazia, lo Stato di diritto e i diritti umani. In questo ambito, l'UE ha istituito meccanismi e adottato regolamentazioni per affrontare la polarizzazione e la violenza che ne deriva. Ha infatti istituito un meccanismo per il regolare monitoraggio sullo Stato di diritto in ciascuno Stato membro, allo scopo di contribuire a prevenire gli effetti dannosi della polarizzazione sulle norme democratiche fondamentali e sui meccanismi istituzionali. Ha inoltre regolamentato i media audiovisivi e le piattaforme digitali al fine tra l'altro di ridurre l'incitamento all'odio e i discorsi discriminatori contro i gruppi minoritari. Sta infine lavorando all'istituzione di un altro meccanismo specifico per scoraggiare la disinformazione e la manipolazione estera.

L'uso della violenza nei confronti dei politici

In uno studio più approfondito specificamente dedicato alla violenza e alla intimidazione verso i politici nell'UE, anch'esso redatto dall'ERPS del Parlamento europeo, si evidenzia come l'UE sia segnata da una **polarizzazione** crescente: negli ultimi anni si è registrata una **crescita** nell'uso della violenza ai danni di figure politiche, sia come strumento di **coercizione** mirato alla tutela degli interessi degli autori, sia come valvola di sfogo derivante dalla crescente **sfiducia** e disaffezione nei confronti delle istituzioni e del processo democratico. Sebbene nel territorio dell'UE gli episodi **di violenza fisica** siano relativamente rari, forme aggressione non fisica – quali **minacce**, **intimidazioni** o **violenza verbale** – sono sempre più diffuse, acuite inoltre dal progredire della tecnologia che le rende più pervasive.

Lo studio sottolinea infine come comprendere il fenomeno dell'uso della violenza in politica sia fondamentale per promuovere un ambiente più **sicuro** e **partecipativo**, tutelando la qualità, la resilienza e il pluralismo delle democrazie.

La risoluzione del **Parlamento europeo** del settembre 2025 relativa alle elezioni europee dell'anno precedente sottolinea l'importanza di **combattere il fenomeno della violenza politica** promuovendo la sensibilità sul tema.

Definire la violenza politica

Il termine "violenza politica", sempre secondo lo studio va inteso in senso ampio, includendo le sue **molteplici manifestazioni** quali:

- violenza fisica: comprende aggressioni che vanno fino all'omicidio, considerato l'atto estremo;
- violenza psicologica: include abuso verbale, minacce, intimidazioni, stalking e campagne diffamatorie;
- violenza economica: si manifesta tramite la distruzione di proprietà personale, ricatti relativi a finanziamenti per cause o campagne o, nel caso di stati autoritari, privazione di finanziamenti *tout court* per partiti di opposizione;
- violenza sessuale: si tratta di una forma di violenza che colpisce principalmente le donne ed è spesso usata come strumento di controllo e intimidazione.

La violenza come strumento politico può essere usata da **attori statuali** nel caso di regimi autoritari o da **attori non statuali** come crimine organizzato o gruppi radicalizzati. Dove i primi hanno interesse a limitare e reprimere l'opposizione, i secondi perseguono interessi particolari. Ad es., i gruppi radicalizzati possono impiegare la violenza come mezzo di perseguimento di un'agenda politica, mentre il crimine organizzato può farvi leva per tutelare i propri interessi economici.

L'Italia meridionale è particolarmente colpita da quest'ultimo tipo di fenomeno: uno studio dell'*Armed Conflict Location & Event Data Project* ha rilevato che nel 2024 la regione sia stata teatro di più della metà degli atti di intimidazione ai danni di politici locali.

Polarizzazione e violenza

Una ricerca condotta dal progetto *Varieties of Democracy* evidenzia l'andamento crescente, sia pur con livelli di gravità variabile, della **polarizzazione** in tutti gli Stati membri dell'Unione.

La ricerca distingue tra più forme di polarizzazione: politica, ideologica, sociale e affettiva. Il livello più critico, come rilevato anche dallo studio sopra citato del Parlamento europeo, è rappresentato dalla **polarizzazione affettiva**, condizione in cui gli individui sviluppano una forte identificazione personale con i propri riferimenti politici, arrivando a nutrire **sfiducia** nei

confronti di chi non condivide le medesime idee e posizioni. In tale scenario, la qualità del **dialogo politico** di un Paese assume un ruolo determinante, e particolare rilevanza è attribuita al **comportamento delle figure di riferimento**. Un leader politico che giustifica atti di violenza o che in prima persona assume atteggiamenti violenti può contribuire, sempre a giudizio del *report*, a creare un clima di impunità percepita, dando il via a un **circolo vizioso**.

L'impatto della violenza

Oltre alle conseguenze personali che le vittime di violenza in ambito politico subiscono – tra cui gli **effetti psicologici** di lungo periodo che le aggressioni, le molestie o lo stalking possono provocare – è fondamentale sottolineare come, secondo lo studio sopra richiamato del Parlamento europeo, un ambiente politico violento abbia un impatto negativo sulla **qualità delle democrazie**, in termini di dibattito politico e partecipazione alla vita pubblica.

Un sondaggio condotto tra i membri della camera bassa del Parlamento dei Paesi Bassi ha rilevato che **un quarto** di questi hanno in passato **evitato di esprimere la propria opinione** su determinati temi per paura di ricevere minacce; il numero sale al **40%** per i membri del Parlamento irlandese.

Lo studio del Parlamento europeo cita inoltre i risultati di un sondaggio condotto in **Germania** da cui risulta che l'81% dei politici locali tedeschi riferisce di aver riportato **conseguenze psichiche e fisiche** nella propria vita quotidiana dopo aver subìto aggressioni scritte o verbali. Inoltre, l'83% degli intervistati ha dichiarato di temere, per la propria vita personale e carriera politica, le campagne di disinformazione e la produzione di "*deep fake*" generati dall'intelligenza artificiale. Sempre lo studio riporta che in Germania, nel 2024, il 56% dei politici vittima di violenza ricopriva cariche a livello federale.

Questi dati, insieme alle evidenze relative alla sproporzione della violenza diretta verso minoranze e gruppi vulnerabili, mettono in luce il legame diretto tra aumento della violenza e diminuzione della qualità del processo democratico. Poiché la democrazia trae forza dalla **pluralità** di opinioni e attori che vi partecipano, una riduzione quantificabile e significativa in questi fattori – come osservato negli studi citati – costituisce un danno per l'intera collettività degli Stati democratici.

Radicalizzazione politica e media

La progressiva erosione della fiducia nelle **istituzioni pubbliche**, così come nei **media tradizionali**, rappresenta un fattore cruciale per

comprendere i processi di radicalizzazione politica. Lo studio "*The Media and Polarisation in Europe: Strategies for Local Practitioners to Address Problematic Reporting*" della Commissione europea evidenzia come il **calo dell'interesse verso le notizie**, passato a livello globale dal 63% nel 2017 al 51% nel 2022, sia indicativo di una crescente selettività nell'accesso all'informazione.

Questa dinamica ha determinato un forte aumento dell'uso di **piattaforme digitali alternative**, spesso caratterizzate dalla veicolazione di contenuti polarizzanti. Il documento sottolinea che tali piattaforme contribuiscono a consolidare **narrazioni ostili** verso personaggi politici percepiti come contrapposti alla propria posizione, creando un contesto che potrebbe favorire comportamenti aggressivi. I dati riportati di seguito testimoniano tale scenario.

La Tabella 1 mostra che, nel 2022, la **fonte principale** dalla quale i cittadini europei hanno seguito le **notizie** siano stati **internet e i *social media***, canali che favoriscono l'informazione selettiva e la formazione di bolle informative, amplificando narrazioni polarizzanti tra individui già predisposti.

Table 1: Where Europeans get their media in 2022 (average per region[30])[31]

Region	Internet	TV	Social media	Print
Central Europe	79.7 %	65.2 %	87.3 %	50.2 %
Northern Europe	85 %	63.3 %	44.3 %	25.3 %
Southern & south-eastern Europe	83.1 %	69.9 %	79 %	59.3 %
Western Europe	76.5 %	60.3 %	41.8 %	26.8 %

The Media and Polarisation in Europe: Strategies for Local Practitioners to Address Problematic Reporting, p. 10

La Tabella 2 mostra che i cittadini europei hanno mediamente **bassa fiducia nei media tradizionali**, circostanza che determina un significativo aumento dell'utilizzo dei social media, che facilitano l'accesso selettivo a contenuti coerenti con le proprie convinzioni.

Table 2: Europeans who trust the media, by region in 2022 (Reuters, 2022)

Region[91]	Overall trust	Country	Overall trust
Central Europe (without Germany)	34 %	Germany	50 %
Northern Europe	58.3 %	Portugal	78 %
Southern/south-eastern Europe (without Portugal)	33.3 %	France	29 %
Western Europe (without the UK or France)	51.3 %	UK	34 %

The Media and Polarisation in Europe: Strategies for Local Practitioners to Address Problematic Reporting, p. 16

Considerando il crescente numero di persone che si rivolge ai **social media** come strumento di informazione, è importante sottolineare, secondo il citato *report* della Commissione europea, come questi intensifichino l'effetto della polarizzazione affettiva proponendo contenuti basati sugli interessi rilevati, creando così un effetto di **cassa di risonanza**, incoraggiando il naturale **pregiudizio di conferma** e radicando ulteriormente le posizioni polarizzate.

Un ulteriore elemento problematico, secondo il *report* "*Violence and intimidation against politicians in the EU*" è costituito dal presunto **anonimato** garantito dai *social media*: la percezione di protezione personale riduce i disincentivi ad assumere comportamenti offensivi, abusivi o minatori, *a fortiori* quando la vittima è una persona mediaticamente esposta, come ad esempio una figura impegnata in politica. È però importante sottolineare che, secondo i dati raccolti nel *report* della Commissione europea, non esistono prove certe che i media generino **automaticamente** polarizzazione. Questi possono tuttavia amplificarla tra **individui già predisposti**. In particolare, la polarizzazione dell'*élites* può essere trasferita alla società nel complesso, contribuendo a normalizzare sentimenti ostili verso figure politiche percepite come appartenenti al campo avverso.

Oltre al fattore ambientale, la polarizzazione può incoraggiare atti di violenza in base a fattori **intrinseci** e **individuali** come genere o etnia: secondo un sondaggio condotto in Svezia, le figure politiche provenienti da un contesto di **migrazione** subiscono violenza fisica e psicologica in maniera sproporzionata; mentre un altro studio, condotto in Belgio, mostra come la violenza psicologica, così come la quella sessuale si manifestino principalmente ai danni di giovani **donne** impegnate in politica.

Possibili misure di risposta alla violenza politica

Si è da più parti osservato che uno degli ostacoli principali nella gestione del fenomeno è costituito dalle **poche denunce** alle autorità competenti. Tale reticenza può derivare dalla sottovalutazione delle diverse forme di violenza oppure dal timore che queste non vengano adeguatamente prese in considerazione dalle autorità pubbliche.

Una proposta strutturata è offerta dallo studio dell'OSCE "***Addressing Violence Against Women in Politics***", che, pur se con un *focus* sulla questione delle donne in politica, offre soluzioni applicabili universalmente.

Nello studio si evidenzia la necessità di agire su più livelli per ottenere un impatto significativo nell'eliminazione del fenomeno della **violenza nei confronti delle donne in politica**.

Secondo l'OSCE, la violenza contro le donne in ambito politico rappresenta un **problema peculiare** nell'ambito della più generale problematica della violenza rivolta contro i rappresentanti politici. La prima si caratterizza infatti per essere rivolta contro le donne non in ragione delle loro posizioni politiche, ma

semplicemente in quanto donne. Questa pratica può assumere diverse forme: fisica, sessuale, psicologica, economica e simbolica, e mira ad ostacolare l'ingresso e la permanenza delle donne nella vita pubblica e a delegittimarne ruolo ed operato politico. Tale forma di violenza costituisce pertanto una **minaccia diretta ai principi democratici e alla parità di rappresentanza** in quanto limita la piena partecipazione di altre la metà della popolazione mondiale.

Data la portata del fenomeno, il *report* dell'OSCE evidenza la necessità di agire su più livelli per ottenere un impatto significativo nell'eliminazione del fenomeno della violenza politica, secondo quello che viene definito **"approccio delle quattro P"** Prevenzione, Protezione, Persecuzione e Politiche coordinate. Ciò richiede interventi integrati volti a:

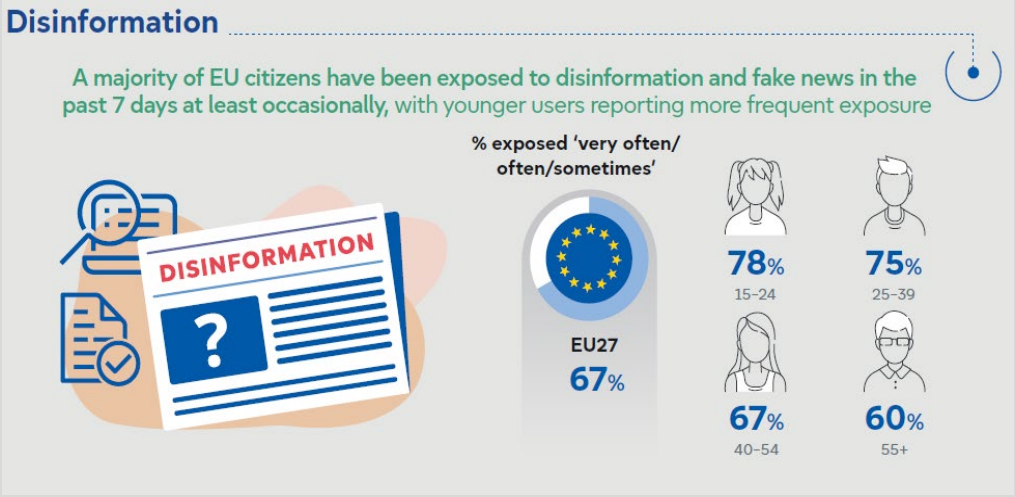
- **prevenire** la violenza attraverso interventi volti a ridurre le cause profonde della violenza, affrontando stereotipi di genere e discriminazioni, promuovendo la parità di accesso alla politica e sensibilizzando l'opinione pubblica. Questa costituisce la via più efficace per estirpare il fenomeno alla radice;
- **proteggere** le vittime di violenza attraverso l'adozione di misure e servizi idonei a tale scopo, come la possibilità di accesso a meccanismi di denuncia e tutela della privacy o al supporto psicologico e legale;
- **perseguire** in maniera adeguata i responsabili, garantendo procedimenti giudiziari centrati sulla vittima, sanzioni proporzionate e meccanismi per prevenire l'impunità;
- adottare **politiche coordinate** e strategie integrate per assicurare una risposta coerente, collaborativa e sostenibile.

Un simile approccio, secondo l'OCSE, permetterebbe di affrontare un fenomeno radicato in maniera strutturale, intervenendo sulle cause profonde ed offrendo soluzioni applicabili in maniera trasversale ai diversi contesti e alle diverse tipologie di violenza politica. risolvendo alla radice intervenendo sulle sue cause profonde e offrendo **soluzioni applicabili in maniera trasversale** ai diversi contesti e tipologie di violenza politica.

SESSIONE III – RAFFORZARE LA RESILIENZA

Nelle note di accompagnamento alla riunione, predisposte dal Parlamento europeo, si sottolinea che la democrazia parlamentare all'interno dell'Unione europea si trova ad affrontare **gravi minacce**, che vanno dalle **divisioni interne** e le **interferenze straniere** all'impatto delle **tecnologie digitali** e al declino della **partecipazione civica**. Il forum intende quindi esplorare le tendenze in atto nelle democrazie parlamentari dell'Unione, esaminando sia le sfide che minano la *governance* democratica sia le migliori pratiche che potrebbero rafforzare i processi democratici.

Le sfide sono particolarmente evidenti nel settore dell'informazione: in un sondaggio Eurobarometro del 2023, l'81% degli intervistati ritiene l'ingerenza straniera nelle democrazie un problema grave e molti hanno espresso preoccupazione per l'impatto della disinformazione, degli attacchi ibridi e dell'influenza straniera occulta sulle elezioni. Un recente sondaggio Eurobarometro, pubblicato il 16 ottobre 2025, indica che i due terzi (66%) degli intervistati ritengono di essere stati esposti alla disinformazione almeno alcune volte nell'ultima settimana. Mentre sei su dieci sono sicuri di poter riconoscere la disinformazione, tre su dieci non lo sono.



Inoltre, l'evoluzione tecnologica, come l'**intelligenza artificiale generativa** (*Gen AI*), rende più difficile per i singoli cittadini riconoscere la disinformazione. La tecnologia *deepfake* confonde i confini fra realtà e finzione, e gli strumenti per utilizzarla sono ampiamente accessibili. I *chatbot Gen AI* alimentati da modelli linguistici di grandi dimensioni (*Large Language Models* - LLMs) stanno cambiando il modo in cui accediamo ed elaboriamo le informazioni. Possono rendere difficile la verifica delle fonti, contribuendo anche a erodere ulteriormente i modelli di *business* di chi produce informazioni e notizie credibili. Gli algoritmi possono prevedere quali contenuti diventeranno virali, puntando sulle vulnerabilità emotive. Tutto questo può creare nuove possibilità di manipolazione del comportamento politico a livello individuale e sociale. La *Gen AI* ha infatti la

capacità di potenziare le campagne di manipolazione delle informazioni. Allo stesso tempo, l'IA viene utilizzata anche per consentire e facilitare gli **attacchi informatici**.

In particolare, nel corso della terza sessione si discuterà degli strumenti e delle misure volti a difendere le democrazie dalle diverse tipologie di minacce (che possono essere ibride, informatiche, interferenze straniere, disinformazione), nonché dell'utilizzo di tecnologie conformi allo **Scudo europeo per la democrazia** (*European Democracy Shield*). L'obiettivo è analizzare l'attuale andamento della *governance* democratica, con una valutazione sia dei reali pericoli che incombono sui processi che la determinano, sia delle innovazioni che la stanno ridisegnando, nonché confrontarsi con il ruolo centrale assunto oggi dal moderno parlamentarismo nell'affrontare sfide che possono essere superate grazie alla cooperazione, a strategie mirate e a sinergie efficaci.

Norme e iniziative dell'Unione europea in materia di resilienza

La resilienza dei soggetti critici

La direttiva (UE) 2022/2557 relativa alla resilienza dei soggetti critici contiene norme volte a garantire che settori critici quali **l'energia, l'acqua, i trasporti e la sanità** siano in grado di prevenire, proteggersi, rispondere, resistere e riprendersi in caso di: **attacchi ibridi**; **catastrofi naturali**; **minacce terroristiche**; **emergenze di sanità pubblica**. Le norme mirano a **ridurre le vulnerabilità** e a **rafforzare la resilienza fisica** dei soggetti critici.

Sono considerati '**soggetti critici**' i soggetti che forniscono servizi essenziali di importanza fondamentale per il mantenimento di funzioni vitali della società, delle attività economiche, della sicurezza e della salute pubbliche e dell'ambiente. Una delle componenti chiave di un soggetto critico è la sua infrastruttura, che può includere un elemento, un impianto, un'attrezzatura, una rete o un sistema necessari per la fornitura di un servizio essenziale. I soggetti critici vengono individuati dagli Stati membri come appartenenti a una delle categorie di cui all'allegato della direttiva 2022/2557. Inoltre, ai fini della direttiva, per '**infrastruttura critica**' si intende un elemento, un impianto, un'attrezzatura, una rete o un sistema o una parte di un elemento, di un impianto, di un'attrezzatura, di una rete o di un sistema, necessari per la fornitura di un servizio essenziale.

La direttiva 2022/2557 è stata recepita nell'**ordinamento italiano** attraverso il decreto legislativo 4 settembre 2024, n. 134.

In base alla direttiva (UE) 2022/2557, i soggetti critici sono tenuti a: individuare eventuali rischi rilevanti che potrebbero perturbare in modo significativo la fornitura di servizi essenziali; adottare misure adeguate a garantire la propria resilienza; notificare gli eventi perturbatori alle autorità competenti.

Nello specifico, la direttiva 2022/2557 prevede che, a seguito di una valutazione dei rischi, gli Stati membri dell'Unione **individuino i soggetti critici** che forniscono servizi essenziali per il mantenimento di funzioni vitali per la società, l'economia, la sanità pubblica e la sicurezza o l'ambiente, e individuino i casi in cui un incidente potrebbe avere notevoli effetti negativi su tali servizi essenziali. La previsione riguarda soggetti operanti nei seguenti settori:

- **energia**, compresi gli operatori dei settori dell'energia elettrica, del teleriscaldamento, del petrolio, del gas e dell'idrogeno;

- **trasporto** aereo, ferroviario, per via d'acqua e su strada, compresi i trasporti pubblici;

- **banche**, soggette anche al regolamento (UE) 2022/2554 (regolamento sulla resilienza operativa digitale nel settore finanziario);

- **infrastrutture dei mercati finanziari**, comprese le sedi di negoziazione, soggette anch'esse al regolamento sulla resilienza operativa digitale;

- **sanità**, compresi i prestatori di assistenza sanitaria, i produttori di articoli farmaceutici di base e di dispositivi critici, nonché le infrastrutture di ricerca e sviluppo di medicinali;

- fornitori e distributori di **acqua potabile**;

- smaltimento e trattamento delle **acque reflue**;

- **infrastrutture digitali**, compresi i servizi di comunicazione elettronica e i centri di calcolo, soggetti anche alla direttiva (UE) 2022/2555 (vedi *infra*);

- enti della **pubblica amministrazione** a livello di governo centrale, esclusi la sicurezza nazionale, la pubblica sicurezza, la difesa e l'applicazione della legge;

- **operatori spaziali** di infrastrutture terrestri;

- imprese del **settore alimentare** impegnate esclusivamente nella logistica, nella distribuzione all'ingrosso e nella produzione e trasformazione industriali su larga scala.

Gli Stati membri devono quindi:

- adottare una **strategia nazionale** ed effettuare **valutazioni periodiche dei rischi**;
- tenendo conto dei risultati di tali valutazioni, **individuare i soggetti** che fanno affidamento sulle infrastrutture critiche per fornire servizi essenziali alla società, all'economia, alla sanità pubblica e alla sicurezza o all'ambiente;
- sostenere i soggetti critici individuati nel **miglioramento della propria resilienza**, ad esempio con materiali di orientamento, esercitazioni, consulenze e formazione;
- garantire che le autorità nazionali abbiano i poteri, le risorse e i mezzi per effettuare i propri compiti di vigilanza, compreso lo svolgimento di **ispezioni in loco di soggetti critici** e l'introduzione di **sanzioni in**

caso di mancato rispetto nell'ambito di un meccanismo di applicazione della legge;
- specificare le **condizioni** in base alle quali un soggetto critico può presentare richieste di controlli dei precedenti sul personale che detiene ruoli sensibili.

Gli Stati membri sono tenuti a individuare i soggetti critici per i settori e i sottosettori di cui all'allegato della direttiva entro il **17 luglio 2026** (per l'**Italia**, vedi l'Allegato A del citato decreto legislativo 4 settembre 2024, n. 134).

I soggetti critici a loro volta hanno l'obbligo di:

- **effettuare valutazioni dei propri rischi** per individuare quelli che potrebbero ostacolarne la capacità di fornire servizi essenziali;
- **adottare misure tecniche, organizzative e di sicurezza** per aumentare la resilienza;
- **riferire gli incidenti negativi di rilievo** alle autorità nazionali.

La direttiva stabilisce inoltre norme per l'individuazione dei soggetti critici di particolare **rilevanza europea**. Un soggetto critico è considerato di particolare rilevanza europea se fornisce un servizio essenziale a **sei o più Stati membri**.

Strategia europea per l'Unione della preparazione

Il 26 marzo 2025 la Commissione europea e l'Alto rappresentante dell'UE per gli affari esteri e la politica di sicurezza hanno presentato una comunicazione congiunta dal titolo "Strategia europea per l'Unione della preparazione", con l'obiettivo di sostenere gli Stati membri e rafforzare la capacità dell'Europa nel prevenire e rispondere alle minacce emergenti.

La comunicazione sottolinea che l'UE si trova ad affrontare crisi e sfide sempre più complesse che non possono essere ignorate, che comprendono la **guerra di aggressione della Russia** nei confronti dell'Ucraina, crescenti **tensioni e conflitti geopolitici**, **attacchi ibridi e informatici**, la **manipolazione delle informazioni**, **ingerenze straniere**, i **cambiamenti climatici** e l'**aumento delle catastrofi naturali**. Per colmare le attuali lacune e progredire verso un'autentica Unione della preparazione, la strategia muove dai seguenti principi:

- approccio multirischio integrato al fine di coprire l'intero spettro dei rischi e delle minacce naturali e provocate dall'uomo e e di riunire tutti gli strumenti disponibili;
- approccio esteso a tutta l'amministrazione al fine di promuovere la collaborazione, la coerenza delle politiche e la condivisione delle risorse fra tutti i soggetti di interesse a tutti i livelli dell'amministrazione (locale, regionale, nazionale e unionale);

- approccio esteso a tutta la società che promuova una cultura della preparazione e della resilienza improntata all'inclusione nella quale siano coinvolti cittadini, comunità locali e società civile, imprese e parti sociali e le comunità scientifica e accademica.

Per ottemperare a tali principi, la strategia si basa sugli obiettivi di resilienza alle calamità (*European disaster resilience goals*) e propone azioni in sette ambiti: 1)·**previsione e anticipazione**; 2) **resilienza delle funzioni sociali vitali**; 3) **preparazione della popolazione**; 4) **cooperazione pubblico-privato**; 5) **cooperazione civile-militare**; 6) **coordinamento della risposta alle crisi**; 7) **resilienza mediante partenariati esterni**.

Vengono definite **30 azioni chiave** e un **piano d'azione** (in allegato alla comunicazione), anche al fine di sviluppare una "cultura della preparazione e della resilienza" in tutte le politiche dell'UE. Gli **obiettivi** e le **azioni principali** della strategia sono indicati di seguito.

1. Previsione e anticipazione attraverso: la messa a punto di una valutazione completa di rischi e minacce a livello di UE; la creazione di un "quadro operativo di crisi" per i responsabili politici; il potenziamento del Centro di coordinamento della risposta alle emergenze (*Emergency Response Coordination Centre* - ERCC); la compilazione di un catalogo dell'UE sulla formazione e sullo sviluppo di una piattaforma sugli insegnamenti tratti dalle crisi passate; l'istituzione di un servizio governativo dell'UE di osservazione della Terra.

2. Resilienza delle funzioni essenziali della società europea attraverso: l'integrazione del principio di "preparazione fin dalla progettazione" nelle politiche e nelle azioni dell'UE; l'adozione di criteri minimi di preparazione per **servizi essenziali quali ospedali, scuole, trasporti e telecomunicazioni**; la revisione del meccanismo di protezione civile dell'UE; la proposizione di una strategia di costituzione delle scorte a livello di Unione (per migliorare l'accesso alle cd. risorse critiche); l'istituzione di un piano di adattamento ai cambiamenti climatici; la garanzia dell'approvvigionamento di acqua e di altre risorse naturali critiche.

3. Preparazione della popolazione attraverso: il miglioramento dei sistemi di allarme rapido; la sensibilizzazione su rischi e minacce; l'elaborazione di orientamenti per arrivare a un'autosufficienza della popolazione di almeno 72 ore; l'inclusione della preparazione nei programmi scolastici e nella formazione del personale didattico; la promozione della preparazione nei programmi destinati ai giovani; il richiamo di talenti per migliorare la preparazione dell'UE.

4. Cooperazione pubblico-privato attraverso: la costituzione di una *task force* pubblico-privato per la preparazione; la definizione di protocolli pubblico-privato per le emergenze (dovranno esservi eccezioni giustificate e circoscritte nel tempo per garantire la disponibilità in tempi rapidi dei materiali, beni e servizi critici e per mantenere **in sicurezza le linee di produzione critiche**); la revisione della disciplina degli appalti pubblici; l'istituzione di un Centro europeo di competenza sulla sicurezza della ricerca.

5. Cooperazione civile-militare attraverso: la definizione di accordi globali civili-militari sulla preparazione (nella maggior parte degli scenari di crisi la

competenza primaria spetta alle autorità civili nazionali, ma sono sempre più numerose le circostanze in cui risulta necessario il supporto delle forze armate, ad es. per emergenze sanitarie, eventi meteorologici estremi, attacchi ibridi e informatici); la definizione di norme per la pianificazione e per gli investimenti a duplice uso civile-militare (l'UE deve integrare gli aspetti collegati al duplice uso in tutti gli investimenti nelle infrastrutture e nella pianificazione delle capacità - laddove l'espressione 'duplice uso' indica l'idoneità a scopi sia militari sia civili - quali la mobilità militare, le evacuazioni di massa, le comunicazioni e la connettività sicure, la sicurezza marittima, le capacità informatiche e le risorse e i servizi spaziali); l'organizzazione di esercitazioni periodiche dell'UE per promuovere la preparazione globale (la Commissione e l'Alto rappresentante organizzeranno periodicamente esercitazioni globali e intersettoriali di preparazione a livello di UE, finalizzate a testare il processo decisionale, il coordinamento e le risposte operative all'interno dell'UE e trasversalmente ai settori, anche nell'ambito dell'articolo 42, paragrafo 7, del Trattato sull'Unione europea e dell'articolo 222 del Trattato sul funzionamento dell'Unione europea).

6. Risposta alle crisi attraverso: l'istituzione di un **polo di coordinamento dell'UE per le crisi** (il polo di coordinamento dell'UE per le crisi, nell'ambito dell'ERCC sopra citato, svolgerà sia un ruolo all'interno della Commissione sia una funzione di sostegno agli interlocutori negli Stati membri, prestando particolare attenzione all'anticipazione e alla gestione delle conseguenze delle crisi nei diversi settori); il potenziamento di *rescEU* (muovendo dai risultati positivi ottenuti con lo sviluppo dei mezzi aerei antincendio e di altre risorse di *rescEU*, la Commissione garantirà il mantenimento e l'eventuale potenziamento delle capacità esistenti, che comprendono la lotta aerea contro gli incendi e le minacce chimiche, biologiche, radiologiche e nucleari, assistenza medica, ripari, trasporti, energia).

7. Resilienza mediante partenariati esterni attraverso: la promozione della reciprocità della resilienza con i Paesi candidati; l'integrazione degli aspetti di preparazione e resilienza nei partenariati bilaterali e nelle istituzioni multilaterali; l'integrazione degli aspetti di preparazione e resilienza nella cooperazione con la NATO.

La protezione delle reti e dei sistemi informativi

La sicurezza informatica comporta la protezione delle reti e dei sistemi informativi (*Network and Information Security* - NIS), dei loro utenti e di altre persone interessate da incidenti e minacce informatiche. Come riportato sul sito del Consiglio dell'UE, **settori critici** quali i **trasporti**, l'**energia**, la **sanità** e la **finanza** dipendono sempre di più dalle tecnologie digitali per la gestione delle loro attività principali; la digitalizzazione offre peraltro opportunità e soluzioni a molte delle sfide che l'Europa deve affrontare, esponendo tuttavia l'economia e la società a **minacce informatiche**. Gli attacchi informatici e la criminalità informatica sono infatti in aumento in tutta Europa in termini sia di quantità che di sofisticazione: tendenza destinata a crescere in futuro, visto che il numero di dispositivi connessi in

tutto il mondo dovrebbe quasi raddoppiare, passando dai 15,9 miliardi del 2023 a oltre 32,1 miliardi nel 2030.

La direttiva NIS 2

Nel 2016 l'Unione europea aveva adottato la direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi (NIS), la prima misura legislativa a livello di Unione volta ad accrescere la cooperazione fra gli Stati membri sulla questione della cibersicurezza. Tale direttiva è stata abrogata dalla direttiva (UE) 2022/2555 relativa a **misure per un livello comune elevato di cibersicurezza nell'Unione (NIS 2)**, mentre il regolamento di esecuzione (UE) 2024/2690 ha abrogato il regolamento di esecuzione (UE) 2018/151, che stabiliva le norme per l'applicazione della direttiva (UE) 2016/1148.

La direttiva 2022/2555 è stata **recepita nell'ordinamento italiano** con il *decreto legislativo 4 settembre 2024, n. 138*.

Obiettivo della direttiva NIS2 è innalzare il livello dell'UE in materia di cibersicurezza, attraverso un ambito di applicazione più ampio, norme più chiare e strumenti di vigilanza più solidi. Le nuove norme intendono infatti garantire un **livello comune elevato di cibersicurezza nell'UE**, rispondendo al panorama di minacce in evoluzione e tenendo in considerazione la trasformazione digitale, accelerata dalla pandemia di Covid-19.

La direttiva impone agli Stati membri di **rafforzare le loro capacità in materia di cibersicurezza**, introducendo nel contempo misure di gestione dei rischi e obblighi di segnalazione a soggetti di più settori e stabilendo norme per la cooperazione, la condivisione delle informazioni, la vigilanza e l'applicazione delle misure di cibersicurezza. Gli Stati membri devono inoltre redigere e aggiornare regolarmente un elenco di operatori di servizi essenziali, garantendo che tali soggetti rispettino i requisiti della direttiva.

Nello specifico, la direttiva (UE) 2022/2555:

- stabilisce **norme minime** per il nuovo quadro normativo;
- definisce **meccanismi per una cooperazione** efficace fra le autorità competenti di ciascun Paese dell'UE;
- aggiorna l'**elenco dei settori** e delle attività soggetti agli obblighi in materia di cibersicurezza.

Oltre ai settori già contemplati dalla direttiva NIS, quali l'energia, i trasporti, l'assistenza sanitaria, la finanza, la gestione delle risorse idriche e le infrastrutture digitali, le nuove norme si applicano ai fornitori di servizi pubblici di comunicazione elettronica, a un maggior numero di servizi digitali quali le piattaforme sociali, la gestione delle acque reflue e dei rifiuti,

la fabbricazione di prodotti critici, i servizi postali e di corriere, la pubblica amministrazione, sia a livello centrale che regionale, lo spazio.

Inoltre la direttiva:

- comprende disposizioni in materia di vigilanza, applicazione e **valutazioni *inter pares* volontarie** per rafforzare la fiducia reciproca, e introduce la responsabilità dell'alta dirigenza per il mancato rispetto delle misure di gestione dei rischi di cibersicurezza;
- ha istituito una rete di gruppi di intervento per la sicurezza informatica in caso di incidente (*CSIRTs network*) al fine di scambiare informazioni sulle minacce informatiche e rispondere agli incidenti;
- ha istituito la rete europea delle organizzazioni di collegamento per le crisi informatiche (*European cyber crisis liaison organisation network* - EU-CyCLONe). Tale rete è volta a sostenere una gestione coordinata delle crisi informatiche fra le autorità nazionali degli Stati membri e garantire uno scambio regolare di informazioni con le istituzioni dell'UE in caso di incidenti e crisi su vasta scala.

Parallelamente, il gruppo di cooperazione NIS è una piattaforma istituita dalla direttiva NIS per facilitare la cooperazione strategica e lo scambio di informazioni fra gli Stati membri dell'UE, la Commissione europea e l'Agenzia dell'UE per la cibersicurezza (*European Union Agency for Cybersecurity* - ENISA).

La strategia dell'UE in materia di cibersicurezza

Nel dicembre 2020 la Commissione europea e il Servizio europeo per l'azione esterna (SEAE) hanno presentato una "Strategia dell'UE in materia di cibersicurezza per il decennio digitale". Obiettivo della strategia è **rafforzare la resilienza dell'Europa** di fronte alle minacce informatiche e garantire che tutti i cittadini e le imprese possano beneficiare di servizi e strumenti digitali affidabili e attendibili. La strategia include inoltre proposte volte a introdurre nuovi **strumenti normativi, strategici e di investimento**.

Coerentemente con quanto prospettato nella comunicazione della Commissione europea dal titolo "Plasmare il futuro digitale dell'Europa", nel Piano per la ripresa dell'Europa e in "*ProtectEU*: strategia europea di sicurezza interna" (del 1° aprile 2025), la strategia in materia di cibersicurezza intende rafforzare la resilienza collettiva dell'Europa contro le minacce informatiche e contribuire a garantire che tutti i cittadini e tutte le imprese possano beneficiare appieno di servizi e strumenti digitali affidabili. La cibersicurezza è parte integrante della sicurezza degli europei e, come sottolineato dalla la Commissione, "che si tratti di utilizzare dispositivi connessi o reti elettriche, oppure di usufruire dei servizi di banche, trasporti aerei, amministrazioni pubbliche o ospedali i cittadini devono avere la

garanzia di essere protetti dalle minacce informatiche. **L'economia, la democrazia e la società dell'UE dipendono, ora più che mai, da strumenti digitali e connettività sicuri e affidabili**".

La nuova strategia per la cibersicurezza intende far sì che l'UE rafforzi la *leadership* su **norme e standard internazionali nel ciberspazio** e intensifichi la collaborazione con i partner in tutto il mondo al fine di promuovere un ciberspazio globale, aperto, stabile e sicuro, fondato sullo Stato di diritto, sui diritti umani, sulle libertà fondamentali e sui valori della democrazia. A tal fine, la strategia mira a preservare un'Internet globale e aperto, offrendo nel contempo un meccanismo di salvaguardia, non solo per garantire la sicurezza ma anche per proteggere i valori europei e i diritti fondamentali.

Basandosi sui risultati conseguiti negli anni, la strategia contiene inoltre proposte per iniziative politiche, di regolamentazione e di investimento in tre aree d'azione dell'UE.

1) Resilienza, sovranità tecnologica e *leadership*. La Commissione ha proposto di riformare le norme sulla sicurezza delle reti e dei sistemi informatici nell'ambito della direttiva sulle misure per un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista o 'NIS 2', su cui vd. *supra*), al fine di aumentare il livello di ciberresilienza dei settori pubblici e privati essenziali: strutture ospedaliere, reti energetiche, ferrovie, ma anche centri dati, amministrazioni pubbliche, laboratori di ricerca e produzione di dispositivi medici e medicinali, nonché altre infrastrutture e servizi essenziali che devono rimanere impermeabili in un contesto di minacce sempre più repentine e complesse. La Commissione ha inoltre proposto di avviare una rete di centri operativi per la sicurezza in tutta l'UE, alimentati dall'intelligenza artificiale (IA), che dovrebbe costituire per l'UE una vera e propria barriera di cibersicurezza in grado di rilevare tempestivamente i segnali di un attacco informatico e consentire un'azione proattiva prima che si verifichino danni. Ulteriori misure comprendono un sostegno dedicato alle piccole e medie imprese (PMI) nel quadro dei 'poli dell'innovazione digitale' e maggiori sforzi per migliorare le competenze della forza lavoro, attirare e trattenere i talenti in materia di cibersicurezza e investire per una ricerca e un'innovazione aperta, competitiva e basata sull'eccellenza.

2) Sviluppo della capacità operativa di prevenzione, deterrenza e risposta. Nell'ambito di un processo progressivo e inclusivo portato avanti con gli Stati membri, la Commissione pone l'attenzione su una nuova Unità congiunta per il ciberspazio allo scopo di rafforzare la collaborazione fra gli organismi dell'UE e le autorità degli Stati membri responsabili della prevenzione, della deterrenza e della risposta agli attacchi informatici, comprese le comunità civili, diplomatiche, di contrasto e di difesa informatica. A tal riguardo, l'Alto rappresentante ha presentato proposte per rafforzare il pacchetto di strumenti della diplomazia informatica dell'UE al fine di prevenire, dissuadere e rispondere in modo efficace alle attività informatiche dolose, in particolare quelle che interessano le nostre **infrastrutture**, le **catene di fornitura**, le **istituzioni** e i **processi democratici essenziali**. L'UE mira inoltre a rafforzare ulteriormente la collaborazione in materia di ciberdifesa e

a sviluppare capacità di ciberdifesa all'avanguardia, basandosi sul lavoro svolto dall'Agenzia europea per la difesa e incoraggiando gli Stati membri a sfruttare appieno la cooperazione strutturata permanente e il Fondo europeo per la difesa;

3) Promozione di un ciberspazio globale e aperto grazie a una maggiore cooperazione. L'UE ritiene importante intensificare la collaborazione con i partner internazionali per rafforzare l'ordine mondiale basato su regole, promuovere la sicurezza e la stabilità nel ciberspazio e proteggere i diritti umani e le **libertà fondamentali *online***. Intende inoltre promuovere norme e standard internazionali che riflettano tali valori dell'UE cooperando con i partner internazionali nell'ambito delle Nazioni Unite e in altri contesti pertinenti. L'UE è tesa quindi a rafforzare ulteriormente il suo pacchetto di strumenti della **diplomazia informatica** e intensificare gli sforzi per la creazione di capacità informatiche nei Paesi terzi sviluppando un'apposita agenda esterna dell'UE.

L'UE si è impegnata a sostenere la nuova strategia per la cibersicurezza con **investimenti nella transizione digitale dell'UE**, attraverso il bilancio a lungo termine dell'UE, in particolare tramite il programma Europa digitale, Orizzonte Europa e il Piano per la ripresa dell'Europa. Gli Stati membri sono pertanto incoraggiati a utilizzare appieno il dispositivo per la ripresa e la resilienza dell'UE per rafforzare la cibersicurezza. L'obiettivo è raggiungere fino a 4,5 miliardi di euro di investimenti combinati da parte dell'UE, degli Stati membri e dell'industria, in particolare nell'ambito del Centro di competenza sulla cibersicurezza e della rete dei centri di coordinamento e garantire che una parte importante degli investimenti siano effettivamente attribuiti alle PMI.

La Commissione mira inoltre a rafforzare le capacità industriali e tecnologiche dell'UE in materia di cibersicurezza, anche tramite **progetti finanziati congiuntamente dall'UE e dai bilanci nazionali**, cogliendo l'opportunità di condividere le proprie risorse per rafforzare la sua autonomia strategica e promuovere la sua *leadership* nel campo della cibersicurezza lungo tutta la catena di fornitura digitale (compresi dati e *cloud*, tecnologie per processori di prossima generazione, connettività ultrasicura e reti 6G), in linea con i suoi valori e le sue priorità.

Nell'ambito della strategia per la cibersicurezza e con il sostegno della Commissione e dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA), gli Stati membri sono stati incoraggiati a portare a termine, entro il 2025, quanto previsto nel pacchetto di strumenti dell'UE per le reti 5G, che definisce un approccio globale e basato sui rischi oggettivi per la **sicurezza delle reti 5G e di prossima generazione**.

Il 13 maggio 2025, l'ENISA ha lanciato la Banca dati europea delle vulnerabilità, che raccoglie **informazioni sulle vulnerabilità relative alla sicurezza delle infrastrutture digitali**. Essa dovrebbe aiutare le parti interessate (enti del settore pubblico e privato, mondo accademico) a soddisfare i requisiti della gestione della catena di approvvigionamento e delle vulnerabilità in settori quali l'energia, i trasporti e la sanità, in linea con le disposizioni della direttiva 'NIS 2' sulla sicurezza delle reti e dell'informazione.

Italia - Strategia nazionale di cybersicurezza 2022 - 2026

La Strategia nazionale di cybersicurezza 2022-2026 ha individuato tre obiettivi e due fattori abilitanti al fine di rendere il Paese più sicuro e resiliente di fronte alle nuove sfide poste dallo sviluppo tecnologico e dalla trasformazione digitale. Il piano di implementazione, correlato alla strategia, trasforma obiettivi e fattori abilitanti in 82 misure da realizzare coinvolgendo tutta la pubblica amministrazione e, a seguire, le imprese e i cittadini.

Le amministrazioni responsabili dell'attuazione possono far ricorso a fondi dedicati all'attuazione della strategia, alle risorse rese disponibili dall'Investimento 1.5 "*Cybersecurity*" del piano nazionale di ripresa e resilienza (PNRR) o ai propri fondi ordinari.

Il regolamento sulla cibersicurezza

Il regolamento sulla cibersicurezzaè entrato in vigore nel giugno 2019 e prevede:

- un sistema europeo di certificazione della cibersicurezza dei prodotti, dei servizi e dei processi delle tecnologie dell'informazione e della comunicazione (TIC) e dei servizi di sicurezza gestiti;
- un nuovo e più forte mandato per l'Agenzia dell'UE per la cibersicurezza (ENISA).

Con tale regolamento, l'UE ha dunque introdotto un **quadro unico di certificazione in tutta l'UE** volto a: stimolare la fiducia nei fornitori di servizi digitali e nel mercato unico digitale stesso, soprattutto fra i consumatori; favorire la crescita del mercato della cibersicurezza; agevolare il commercio in tutta l'Unione. A tal fine, il quadro fornisce un insieme di norme, requisiti tecnici, standard e procedure.

Nel dicembre 2024 l'UE ha adottato una modifica mirata del regolamento sulla cibersicurezza che riguarda i cosiddetti 'servizi di sicurezza gestiti'. Il regolamento (UE) 2025/37 introduce infatti la definizione di **servizi di sicurezza gestiti** ed estende l'ambito di applicazione del quadro europeo di certificazione della cibersicurezza includendovi i servizi di sicurezza gestiti (ampliando pertanto **il mandato e i compiti di ENISA**). Si tratta di una modifica mirata che persegue la finalità generale di garantire la **resilienza dell'UE agli attacchi informatici** e prevenire eventuali vulnerabilità del mercato interno. Il regolamento è in vigore dal 4 febbraio 2025.

La legge di delegazione europea 2025, attualmente all'esame del Parlamento, contiene i principi di delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2025/37.

L'Agenzia dell'UE per la cibersicurezza

La nuova Agenzia dell'UE per la cibersicurezza si basa sulle strutture dell'Agenzia europea per la sicurezza delle reti e dell'informazione, che l'ha preceduta e di cui mantiene l'acronimo (ENISA), ma con un ruolo rafforzato e un mandato permanente. L'agenzia **sostiene gli Stati membri**, le istituzioni dell'UE e altri portatori di interessi nella **gestione degli attacchi informatici**.

Il 6 dicembre 2024 il Consiglio ha approvato conclusioni volte a rafforzare ulteriormente il ruolo dell'Agenzia all'interno dell'ecosistema digitale dell'UE. Nelle conclusioni si pone l'accento sull'importanza della cooperazione dell'ENISA con altri attori dell'**ecosistema della cibersicurezza**, ad esempio il **Servizio per la cibersicurezza delle istituzioni dell'UE** (CERT-UE), il **Centro europeo di competenza per la cibersicurezza** (*European Cybersecurity Competence Centre* – ECCC) ed **Europol**, ma anche con organizzazioni e partner internazionali e con il settore privato.

Agenzia per la cybersicurezza nazionale

Per quanto riguarda l'**Italia**, l'Agenzia per la cybersicurezza nazionale (ACN) è volta alla tutela degli interessi nazionali nel campo della cybersicurezza, ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria.

All'agenzia spetta in particolare il compito di predisporre la strategia nazionale di cybersicurezza. L'agenzia inoltre assume le iniziative idonee a valorizzare la crittografia come strumento di cybersicurezza, provvede alla qualificazione dei servizi *cloud* per la pubblica amministrazione, promuove iniziative di partenariato pubblico-privato, onde rendere effettive le capacità di prevenzione e rilevamento e risposta a incidenti e attacchi informatici, sostiene negli ambiti di competenza lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche, assicura il necessario raccordo con le altre amministrazioni cui la legge attribuisca competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti alla ricerca militare.

Essa assume compiti in precedenza 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. Ad esempio, all'ACN sono stati trasferiti i compiti già dell'AgID relativi alla sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico e alla protezione dalle minacce informatiche delle comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone altresì la resilienza (D.Lgs. 207/2021, Codice europeo delle comunicazioni elettroniche, art. 6, comma 1). L'art. 7 del D.L. 152/2021 - convertito con modificazioni dalla L. 29 dicembre 2021, n. 233 - prevede che Sogei S.p.A. eroghi servizi in qualità di infrastruttura *cloud* nazionale a favore di diversi soggetti fra cui l'agenzia per la cybersicurezza nazionale.

Il Centro di competenza per la cibersicurezza

Nell'aprile 2021 il Consiglio ha adottato il regolamento 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**. Bucarest è stata selezionata dagli Stati membri dell'UE come sede del nuovo centro. Suoi obiettivi principali sono: migliorare ulteriormente la ciberresilienza; contribuire alla diffusione delle tecnologie più recenti nel settore della cibersicurezza; sostenere le *start-up* e le PMI nel settore della cibersicurezza; rafforzare la ricerca e l'innovazione in materia di cibersicurezza; contribuire a colmare il divario di competenze in materia di cibersicurezza.

Il programma Europa digitale 2025-2027

Il 28 marzo 2025 è stato pubblicato il programma Europa digitale 2025-2027 (DIGITAL). Esso si concentrerà sull'implementazione dell'intelligenza artificiale e sul suo utilizzo da parte delle imprese e della pubblica amministrazione, sul *cloud computing* e sui dati, sulla **resilienza informatica** e sull'**alfabetizzazione digitale**, nonché sulla **lotta alla disinformazione**. Il programma fornisce finanziamenti strategici attraverso una rete di poli europei dell'innovazione digitale (EDIH), con un bilancio complessivo di oltre 8,1 miliardi di euro (all'interno del quadro finanziario pluriennale 2021-2027).

Il regolamento sulla cibersolidarietà

Il 2 dicembre 2024 il Consiglio ha adottato il regolamento sulla cibersolidarietà, che stabilisce le misure intese a rafforzare le capacità dell'UE di **rilevamento delle minacce e degli incidenti informatici** e di preparazione e risposta agli stessi per rendere l'Europa più resiliente e reattiva, rafforzando nel contempo i meccanismi di cooperazione.

I suoi obiettivi principali sono:

- sostenere il rilevamento e la conoscenza delle minacce e degli incidenti di cibersicurezza significativi o su vasta scala;
- rafforzare la preparazione e **proteggere i soggetti critici e i servizi essenziali**, come gli ospedali e i servizi pubblici;
- rafforzare la **solidarietà a livello dell'UE**, la gestione concertata delle crisi e le capacità di risposta in tutti gli Stati membri;
- contribuire a garantire un panorama digitale sicuro per i cittadini e le imprese.

L'articolo 1 specifica che l'**oggetto** e le **finalità** del regolamento (UE) 2025/38 dovranno essere attuati mediante l'istituzione di:

- una **rete paneuropea di poli informatici** (il 'sistema europeo di allerta per la cibersicurezza'), volta a sviluppare e potenziare 'capacità coordinate' in materia di rilevamento e 'capacità comuni' in materia di conoscenza situazionale;

- un **meccanismo per le emergenze di cibersicurezza**, che sostenga gli Stati membri nella preparazione e nella risposta agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza su vasta scala, nella mitigazione del loro impatto, e che sostenga gli altri utenti nella risposta agli incidenti di cibersicurezza significativi e agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala;

- un **meccanismo europeo di riesame degli incidenti di cibersicurezza** finalizzato al riesame e alla valutazione di incidenti di cibersicurezza significativi o su vasta scala.

In particolare, il **sistema europeo di allerta per la cibersicurezza** sarà una rete paneuropea di infrastrutture costituita da **poli informatici nazionali e poli informatici transfrontalieri**, i quali aderiranno su base volontaria per sostenere lo sviluppo di capacità avanzate affinché l'Unione migliori le capacità di rilevamento, analisi e trattamento dei dati in relazione alle minacce informatiche. I poli informatici nazionali potranno cooperare con soggetti del settore privato scambiando dati e informazioni pertinenti al fine di individuare e prevenire minacce e incidenti informatici, anche con le comunità settoriali e intersettoriali di soggetti essenziali e importanti, di cui all'articolo 3 della direttiva (UE) 2022/2555.

L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) dovrà preparare, almeno ogni due anni, una mappatura dei servizi necessari agli utenti. Nel preparare tale mappatura, l'ENISA dovrà consultare, fra gli altri, il gruppo di cooperazione NIS, la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), la Commissione e, se del caso, il comitato interistituzionale per la cibersicurezza (*Interinstitutional Cybersecurity Board* - IICB), istituito a norma dell'articolo 10 del regolamento (UE, Euratom) 2023/2841. Un **Paese terzo** associato al programma Europa digitale potrà richiedere il sostegno della riserva dell'UE per la cibersicurezza se l'accordo attraverso cui è associato al programma Europa digitale prevede la partecipazione alla riserva dell'UE per la cibersicurezza.

La legge di delegazione europea 2025, attualmente all'esame del Parlamento, contiene i principi di delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2025/38 sulla cibersolidarietà.

Le minacce ibride

L'Unione europea e il suo vicinato sono chiamati a confrontarsi con l'aumento delle minacce ibride che mirano o comunque rischiano di destabilizzare la regione europea e il suo vicinato nel suo complesso. La natura transnazionale di tali minacce ha posto la questione di un'azione comune condotta a livello europeo, volta a coordinare e supportare l'azione degli Stati membri, ai quali compete la responsabilità principale nel contrasto alle minacce ibride.

Nell'aprile 2016 la Commissione e l'Alto rappresentante hanno adottato un Quadro congiunto per contrastare le minacce ibride, con il quale sono state individuate una serie di iniziative, e nel giugno 2018 una comunicazione congiunta sul rafforzamento della resilienza e potenziamento delle capacità di affrontare minacce ibride, nella quale si propone di adottare misure nelle seguenti aree: conoscenza situazionale; ampliamento della cellula per l'analisi delle minacce ibride, istituita dal Servizio europeo per l'azione esterna; sviluppo delle capacità di comunicazione strategica dell'UE; **resilienza e dissuasione nel settore della sicurezza informatica**; resilienza alle attività di *intelligence* ostile, promuovendo il coordinamento fra gli Stati membri e altre organizzazioni internazionali, in particolare la NATO.

Le iniziative avviate dall'UE al fine di rafforzare la capacità di risposta alle minacce ibride comprendono:

- il protocollo (*EU-Playbook*), presentato dalla Commissione europea e dall'Alto rappresentante il 5 luglio 2016, che individua le **modalità operative** in caso di minacce ibride, garantendo il coordinamento delle azioni di contrasto alle minacce ibride, fra i vari livelli decisionali, operativi e tecnici e con partner esterni, in particolare in ambito NATO;
- la **cellula dell'UE per l'analisi delle minacce ibride** presso il **Centro dell'UE di analisi dell'*intelligence*** (*EU Intelligence and Situation Centre* - EU INTCEN), costituita a partire dal 2016;
- il Centro europeo per la lotta contro le minacce ibride, istituito nel 2017 con sede a **Helsinki** sulla base di una iniziativa congiunta di **9 Stati membri dell'UE** (Finlandia, Francia, Germania, Lettonia, Lituania, Polonia, Regno unito, Estonia), al quale partecipano **Norvegia** e **Stati Uniti** e, dal 27 aprile 2018, anche **l'Italia.** Il Centro è aperto a tutti i Paesi dell'UE e della NATO e il numero di Stati partecipanti è cresciuto fino a comprendere attualmente 36 Stati.

Priorità della "bussola strategica" per il contrasto alle minacce ibride

La "bussola strategica per la sicurezza e la difesa" è stata approvata dal Consiglio dell'UE il 21 marzo 2022 e avallata dal Consiglio europeo del 24 e 25 marzo 2022. Per quanto riguarda in particolare il contrasto alle minacce ibride, questa sottolinea la necessità di:

- riunire gli strumenti esistenti dell'UE ed eventuali nuovi strumenti al fine di fornire un quadro per una risposta coordinata alle campagne ibride che interessano l'UE, i suoi Stati membri e i suoi partner;

- rafforzare la capacità di individuare, identificare e analizzare le minacce ibride e la loro fonte, per una migliore comprensione e valutazione comuni di tali minacce. La **capacità unica di analisi dell'*intelligence*** (SIAC), in particolare la cellula per l'analisi delle minacce ibride, fornirà previsione e conoscenza situazionale;

- rafforzare la resilienza sociale ed economica, **proteggere le infrastrutture critiche** nonché **le democrazie e i processi elettorali** dell'UE e nazionali;

- istituire gruppi di risposta rapida dell'UE alle minacce ibride, che siano adattabili alla minaccia e si avvalgano delle pertinenti competenze settoriali civili e militari a livello nazionale e dell'UE, per sostenere gli Stati membri, le missioni e le operazioni PSDC e i Paesi partner;

- rafforzare la capacità di **individuare e analizzare gli attacchi informatici in modo coordinato**, attraverso il ricorso agli strumenti della diplomazia informatica dell'UE e ad altri suoi strumenti, comprese misure preventive e sanzioni nei confronti di attori esterni per attività informatiche malevole contro l'Unione e i suoi Stati membri;

- sviluppare un pacchetto di **strumenti contro la manipolazione delle informazioni e l'ingerenza straniere** ("*Foreign Information Manipulation and Interference* - *FIMI Toolbox*"), che rafforzerà la capacità dell'UE e dei suoi Stati membri di individuare, analizzare e rispondere alla minaccia, anche imponendo costi ai responsabili di tali attività.

In applicazione del mandato della bussola strategica, il **Consiglio dell'UE** ha adottato il 21 giugno 2022 conclusioni su un **quadro per una risposta coordinata dell'UE alle campagne ibride** e il 13 dicembre 2022 conclusioni su orientamenti di attuazione di tale quadro. Il polo operativo per la mobilitazione nei Paesi partner è individuato nel **Centro di coordinamento della risposta alle emergenze** (*Emergency Response Coordination Centre* - ERCC) del **meccanismo di protezione civile dell'Unione** (*rescEU*).

La lotta alla disinformazione

Dal 2015 l'UE è sistematicamente impegnata nel contrasto alle attività di disinformazione, cui è riconducibile - secondo la definizione impiegata dalla Commissione europea - **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**.

Il Consiglio europeo del 19 e 20 marzo 2015, sottolineando l'esigenza di contrastare le campagne di disinformazione in corso da parte della Russia, ha incaricato l'Alto rappresentante di predisporre, in collaborazione con le istituzioni europee e gli Stati membri, un piano d'azione sulla comunicazione strategica e di prevedere l'istituzione di una *task force* sulla comunicazione strategica. Il Piano d'azione sulla comunicazione strategica è stato presentato nel giugno 2015 e indica tre principali obiettivi: efficace comunicazione e promozione delle politiche dell'UE nei confronti del vicinato orientale; rafforzamento della libertà dei media nel vicinato orientale; miglioramento delle capacità dell'UE di rispondere alle attività di disinformazione da parte di attori esterni.

La *Task Force EastStracom*, operativa dal settembre 2015, ha il compito di sviluppare **prodotti e campagne di comunicazione** incentrate sulla spiegazione delle politiche dell'UE nella regione del **partenariato orientale**. Si tratta in particolare di: campagne di comunicazione strategica; comunicazione *ad hoc* su questioni attuali di politica UE; attività volte a sfatare miti. Oltre alla *Task Force EastStracom* sono state istituite altre due *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.

Su invito del Consiglio europeo del 28 e 29 giugno 2018, la Commissione e l'Alto rappresentante hanno presentato il 5 dicembre 2018 un Piano d'azione contro la disinformazione, nel quale si indica che la **disinformazione proveniente dalla Federazione russa rappresenta la minaccia più grave per l'UE** in quanto è sistematica, ben finanziata e condotta su una scala diversa rispetto ad altri Paesi.

Il Codice di condotta per le piattaforme *online*

Il 16 giugno 2022 un Codice rafforzato di buone pratiche è stato firmato da 34 piattaforme e imprese. Sono previsti 44 impegni e 127 misure specifiche con l'obiettivo di: applicare misure più incisive per demonetizzare la disinformazione; accrescere la trasparenza della pubblicità politica e tematica; garantire una copertura completa dei comportamenti manipolatori attuali ed emergenti; ampliare gli strumenti che consentono agli utenti di individuare e segnalare contenuti falsi o fuorvianti; aumentare la copertura delle azioni di verifica dei fatti in tutti i Paesi dell'UE e nelle rispettive lingue; fornire ai ricercatori un maggiore accesso ai dati; istituire un quadro di monitoraggio e comunicazione, con informazioni qualitative e quantitative a livello dell'UE e degli Stati membri; istituire un centro per la trasparenza; creare una *task force* permanente per l'evoluzione e l'adeguamento del codice. Il **13 febbraio 2025** la Commissione e il Comitato europeo per i servizi digitali hanno approvato l'integrazione del codice di buone pratiche sulla disinformazione del 2022 con il Codice di condotta sulla disinformazione, nel quadro della legge sui servizi digitali.

Le Commissioni speciali del Parlamento europeo sulle ingerenze straniere e sui processi democratici nell'Unione europea

Nella scorsa legislatura europea, il Parlamento europeo ha costituito una Commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'UE, inclusa la disinformazione INGE (vd. la sua decisione del 18 giugno 2020) la cui relazione finale è stata adottata in plenaria il 9 marzo 2022.

La risoluzione ha individuato e mappato le minacce di ingerenza straniera in tutte le sue forme, compresi la disinformazione, la manipolazione delle piattaforme dei *social media* e dei sistemi di pubblicità, gli attacchi informatici, le minacce e le vessazioni nei confronti dei giornalisti, il finanziamento occulto dei partiti politici,

nonché l'*elite capture* e la cooptazione. Contiene altresì una diagnosi delle vulnerabilità dell'Unione e raccomandazioni su come rafforzarne la resilienza, con un regime di sanzioni specifico da applicare contro le ingerenze straniere nonché campagne di disinformazione.

Il 10 marzo 2022 il Parlamento ha deciso di istituire una nuova **Commissione speciale sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, compresa la disinformazione (ING2)**, incaricata, in particolare, di dare seguito alla precedente relazione della commissione INGE, di determinare "la base giuridica appropriata per qualsiasi atto giuridico necessario" e di preparare il terreno per "soluzioni istituzionali dell'UE permanenti intese a far fronte alle ingerenze straniere malevole e alla disinformazione", anche in vista delle elezioni europee del 2024.

La relazione finale, approvata dai membri della commissione ING2 il 26 aprile 2023 (con 27 voti favorevoli, un voto contrario e un'astensione), contiene raccomandazioni e aggiornamenti sulla strategia coordinata dell'UE, sul rafforzamento della resilienza, sulle ingerenze straniere, sulla cibersicurezza, sulle ingerenze durante i processi elettorali, sul finanziamento occulto di attività politiche da parte di attori e donatori stranieri, sulla deterrenza, l'imputazione e le contromisure collettive, comprese le sanzioni, nonché sulla politica di vicinato, la cooperazione globale e il multilateralismo.

Il 18 dicembre 2024 il Parlamento ha votato l'istituzione di una Commissione speciale sullo scudo europeo per la democrazia (*European Democracy Shield* - EUDS), che è stata costituita il 3 febbraio 2025. L'EUDS è incaricata di proporre soluzioni per rafforzare la resilienza dell'UE alle minacce e agli attacchi ibridi e migliorare il quadro giuridico e istituzionale dell'UE in una prossima relazione d'iniziativa. Un documento di lavoro dell'EUDS, pubblicato nell'aprile 2025, ha chiesto di potenziare i media indipendenti e la società civile, la difesa contro le minacce informatiche e ibride e di aiutare i paesi vicini dell'UE, in particolare i Paesi candidati, nei loro sforzi per contrastare la FIMI.

Lo 'scudo europeo per la democrazia'

Il **12 novembre 2025** la Commissione e l'Alto rappresentante hanno presentato una comunicazione sullo 'scudo europeo per la democrazia' (*European Democracy Shield: Empowering Strong and Resilient Democracies*), in cui vengono definite una serie di misure concrete volte a proteggere e promuovere **democrazie forti e resilienti in tutta l'UE**.

Nella stessa data, la Commissione ha inoltre presentato una comunicazione sulla strategia dell'UE per la società civile, con l'intento di rafforzare la protezione e il sostegno alle organizzazioni della società civile che svolgono un ruolo essenziale nella società. Entrambe le iniziative erano state delineate negli orientamenti

politici 2024-2029 e nel discorso sullo stato dell'Unione 2025 pronunciato dalla presidente della Commissione europea, Ursula **von der Leyen.**

Le azioni annunciate nell'ambito dello scudo europeo per la democrazia si propongono di rafforzare ulteriormente la capacità collettiva dell'Unione di **contrastare la manipolazione delle informazioni e la disinformazione**. Fra i principali risultati attesi dallo scudo per la democrazia europea sarà la creazione di un **Centro europeo per la resilienza democratica** che dovrebbe riunire le competenze e le risorse dell'UE e degli Stati membri così da incrementare la capacità collettiva di anticipare, individuare e rispondere alle minacce rivolte contro le nostre democrazie. Il centro dovrebbe quindi fungere da nucleo di condivisione delle informazioni e da sostegno per lo sviluppo di capacità in grado di far fronte all'evoluzione delle minacce comuni, **in particolare la manipolazione delle informazioni, le ingerenze da parte di attori stranieri** (*foreign information manipulation and interference* - FIMI) **e la disinformazione. C**on il sostegno e in stretto coordinamento con il sistema di allarme rapido gestito dal Servizio europeo per l'azione esterna, il Centro collegherà le reti e le strutture esistenti. All'interno del Centro sarà inoltre istituita **una piattaforma delle parti interessate** per facilitare il dialogo con le organizzazioni della società civile, i ricercatori e il mondo accademico, *fact-checkers* e i fornitori di media. Vengono a tal fine indicati tre obiettivi principali.

1) La salvaguardia dell'integrità dello spazio informativo. La Commissione intende rafforzare la collaborazione con i firmatari del codice di condotta sulla disinformazione e predisporre un ***Digital Services Act incidents and crisis protocol*** per facilitare il coordinamento fra le autorità competenti e garantire reazioni rapide alle operazioni di informazione su larga scala e potenzialmente transnazionali. Sarà istituita una **rete europea indipendente di verificatori di fatti** (*European Network of Fact-Checkers*) per rafforzare la capacità di verifica dei fatti in tutte le lingue ufficiali dell'UE, mentre l'**Osservatorio europeo dei media digitali** (*European Digital Media Observatory* - EDMO) svilupperà nuove capacità di monitoraggio e analisi indipendenti per la conoscenza situazionale delle elezioni o in situazioni di crisi.

2) Il rafforzamento delle nostre istituzioni, elezioni eque e libere e media liberi e indipendenti. Sebbene l'organizzazione e lo svolgimento delle elezioni siano di competenza degli Stati membri, la Commissione sottolinea la necessità di una cooperazione rafforzata a livello dell'UE per affrontare le sfide comuni in tale settore. La Commissione intende pertanto incrementare i lavori nell'ambito della **rete europea di cooperazione in materia elettorale** (*European cooperation network on elections* - ECNE), organizzando scambi sistematici su temi chiave per l'integrità dei processi elettorali. La Commissione presenterà inoltre orientamenti **sull'uso responsabile dell'IA nei processi elettorali** e aggiornerà il kit di strumenti

per le elezioni della legge sui servizi digitali. Al fine di affrontare la crescente violenza contro i candidati politici e i rappresentanti eletti, la Commissione presenterà una raccomandazione e una guida sulle migliori pratiche negli Stati membri in materia di sicurezza degli **attori politici**.

Un sostegno finanziario rafforzato per il giornalismo indipendente e locale sarà fornito nell'ambito del nuovo **programma per la resilienza dei media,** che dovrà integrare l'attuale sostegno ai media con i programmi di finanziamento proposti nel nuovo quadro finanziario pluriennale. Nell'imminente revisione della direttiva sui servizi di media audiovisivi, la Commissione valuterà come rafforzare l'importanza dei servizi di media di interesse generale e modernizzare le norme in materia di pubblicità per promuovere la sostenibilità dei media nell'UE. La Commissione presenterà inoltre un aggiornamento della raccomandazione (UE) 2021/1534, del 16 settembre 2021, relativa alla garanzia della protezione, della sicurezza e dell'*empowerment* dei giornalisti e degli altri professionisti dei media nell'Unione europea e intensificherà le azioni a sostegno del quadro vigente nell'UE per il contrasto alle **azioni legali strategiche** tese a bloccare la partecipazione pubblica.

3) Promuovere la resilienza della società e l'impegno dei cittadini. Per riconoscere e contrastare la manipolazione delle informazioni, la Commissione dichiara che porrà in atto misure volte a promuovere l'alfabetizzazione **mediatica e digitale per tutte le età**. La Commissione elaborerà inoltre un quadro delle competenze in materia di cittadinanza dell'UE insieme a orientamenti per rafforzare l'**educazione civica** nelle scuole. Secondo quanto dichiarato, la Commissione supporterà il coinvolgimento dei cittadini nella vita democratica dell'Unione attraverso **strumenti partecipativi** e processi decisionali consultivi, prestando **particolare attenzione al livello locale e ai giovani**, e promuoverà l'innovazione nelle piattaforme *online* che consentiranno la partecipazione democratica, attraverso un nuovo **polo tecnologico civico**. Per promuovere la consapevolezza dei diritti democratici dei cittadini ai sensi del diritto dell'UE, la Commissione presenterà quindi una **guida dell'UE alla democrazia**. La Commissione intende infine promuovere processi decisionali basati su dati concreti, anche mediante l'adozione di una raccomandazione sul supporto delle **prove scientifiche nell'elaborazione delle politiche**.

L'Unione europea ha sviluppato alcune misure per contrastare le pressioni sulle democrazie e sui nostri ecosistemi informativi. Gli strumenti legislativi e non legislativi dell'UE comprendono principalmente: un pacchetto di misure presentato nel 2023 sulla **difesa della democrazia**; azioni per far fronte alle minacce ibride; un *toolbox* sulle manipolazioni e le ingerenze straniere nell'informazione (*Foreign Information Manipulation and Interference*).

Tenendo conto del ruolo chiave che mezzi di informazione indipendenti e di alta qualità svolgono a tutela delle democrazie, l'UE ha adottato le seguenti norme (sopra citate): il regolamento europeo sulla libertà dei media; la direttiva sulla protezione delle persone attive nella partecipazione pubblica da domande manifestamente infondate o procedimenti giudiziari abusivi; la revisione della direttiva sui servizi di media audiovisivi. Inoltre, l'**Osservatorio europeo dei media digitali** (*European Digital Media Observatory* - EDMO), con 15 centri nazionali e regionali, si occupa di identificare e analizzare le campagne di manipolazione dell'informazione e di studiare come utilizzare le nuove tecnologie, compresa l'intelligenza artificiale, in tale processo. Infine, il regolamento relativo alla **trasparenza e al *targeting* della pubblicità politica** mira a frenare la diffusione della manipolazione delle informazioni e delle interferenze nei processi normativi ed elettorali.

Il **regolamento sui servizi digitali** (*Digital Services Act* - DSA), contiene norme che impongono alle piattaforme e ai motori di ricerca di rendere lo spazio *online* trasparente e sicuro per gli utenti, di proteggere i diritti fondamentali e di combattere la disinformazione. Sono inoltre stabiliti obblighi aggiuntivi a carico delle piattaforme *online* di dimensioni molto grandi per la gestione dei rischi sistemici; la soglia operativa riguardante i prestatori di servizi che rientrano nell'ambito di applicazione di tali obblighi comprende le piattaforme *online* con un ampio raggio d'azione nell'Unione, stimato a oltre 45 milioni di destinatari dei servizi.

Per approfondimenti, si rimanda al dossier europeo n. 147/DE *Conferenza interparlamentare sul tema: "Verso un'Europa digitale più sicura e innovativa: mantenere le promesse del Digital Services Act (DSA) per i cittadini e i mercati"* - Billund, 3-4 novembre 2025, a cura dei Servizi del Senato e della Camera dei deputati.

Di rilievo, è il regolamento sull'**intelligenza artificiale** (IA), che affronta la questione della manipolazione delle informazioni facilitata dall'IA, attraverso un approccio basato sul rischio.

Per approfondimenti, si veda il dossier n. 289/4 *Disposizioni e delega al Governo in materia di intelligenza artificiale*, a cura dei Servizi del Senato e della Camera dei deputati.