

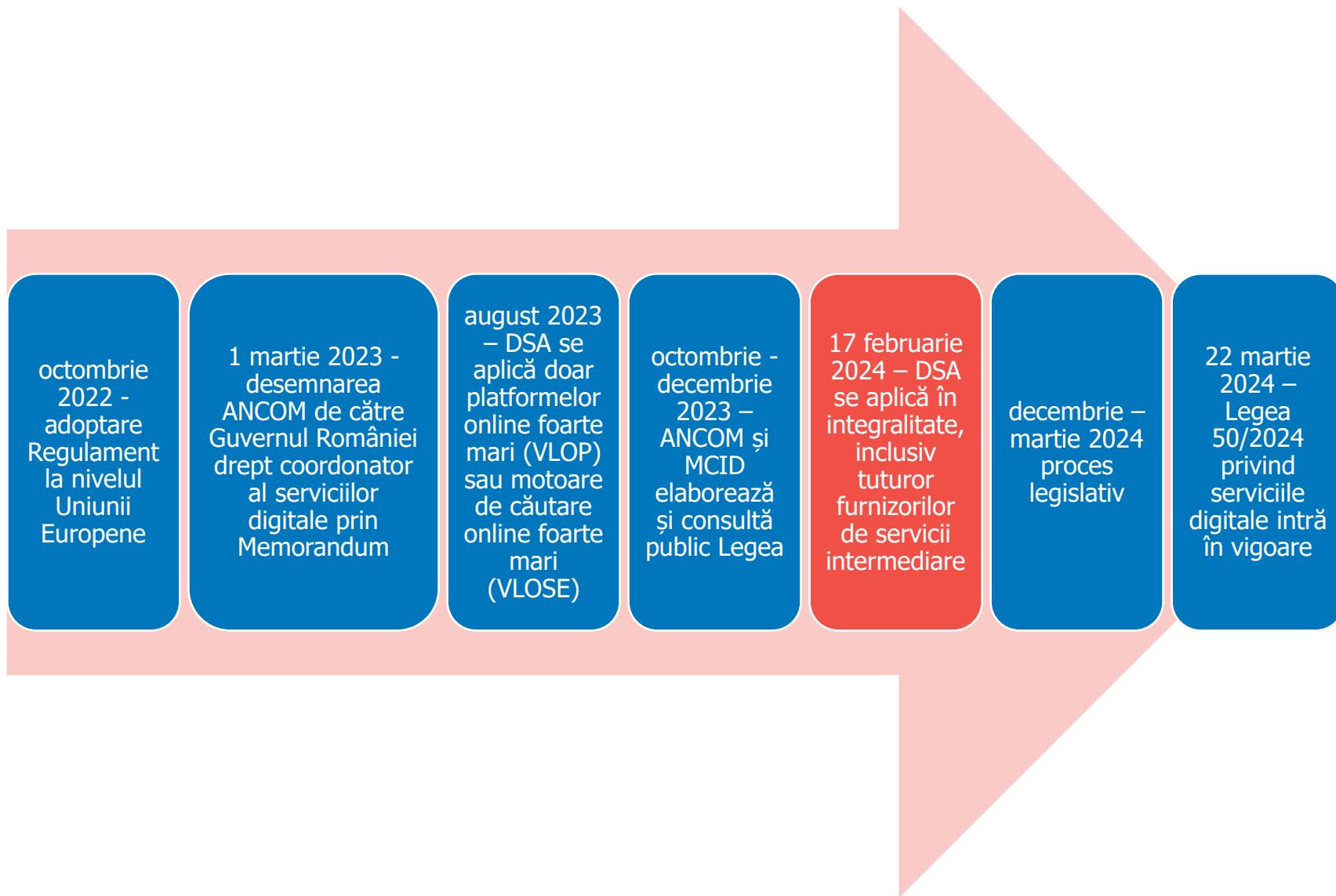


Autoritatea Națională pentru Administrare  
și Reglementare în Comunicații

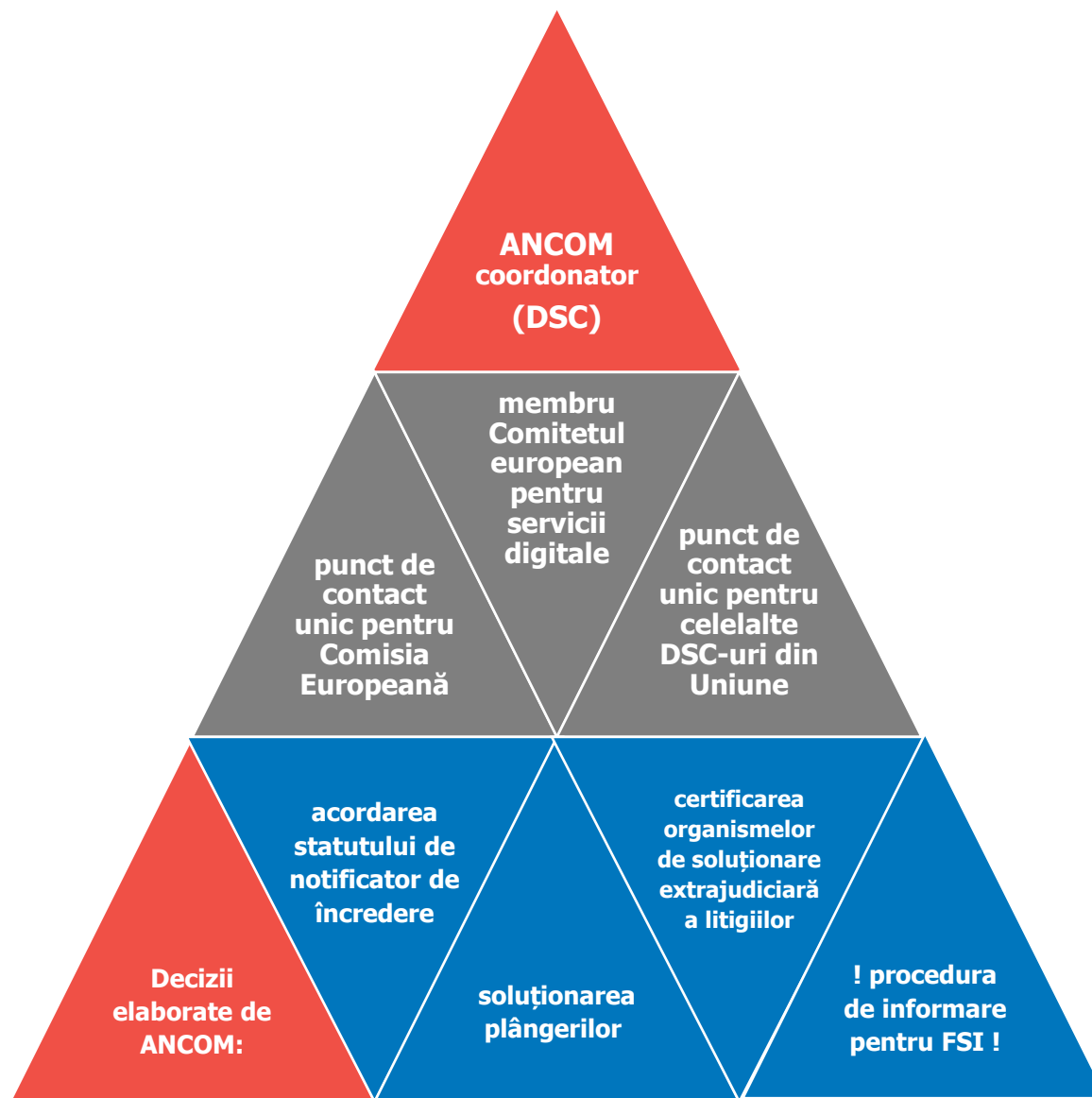
# Aplicarea DSA în România - atribuții ANCOM -

**03 martie 2025**

## TIMELINE – de la Regulament la Legea privind serviciile digitale



## Legea privind serviciile digitale: principale atribuții



## Regulamentul privind serviciile digitale: ce aduce nou?

**termeni și condiții  
transparente pentru utilizarea  
platformelor online**

**o mai bună cunoaștere a  
adevăraților vânzători ai  
produselor pe care le cumpără  
utilizatorii**

**noi măsuri de protecție pentru  
minori în mediul online**

**destinatarii serviciilor sunt  
informați și pot contesta  
eliminarea conținutului lor de  
către furnizorii de platforme  
online**

**interdicții privind comunicările  
cu caracter publicitar de pe  
platformele online, bazate pe  
crearea de profiluri, atunci  
când destinatarul serviciului  
este minor sau când sunt  
utilizate date personale  
sensibile**

**mecanisme rapide de răspuns  
în situații de criză, cu măsuri  
suplimentare de gestionare a  
riscurilor în cazul crizelor de  
sănătate publică și de  
securitate**

# Atribuții ANCOM de verificare a obligațiilor FSI & platformelor online

## Obligații FSI:

- Publică și actualizează informațiile cu privire la **de desemnarea unui punct de contact** pentru **autorități și destinatarii serviciului**, precum și a unui **reprezentant legal**
- notifică datele de contact ale reprezentantului legal
- publică condițiile generale de utilizare
- **publică anual** un raport cu privire la moderările pe care le-au efectuat în perioada relevantă
- **instituie** mecanisme de notificare a conținutului ilegal și un **mod de prelucrare** a notificărilor
- **elaborează o** expunere de motive clară și specifică pentru restricțiile impuse

## Obligații suplimentare ale FSI de găzduire și ale platformelor online

- **instituie** mecanisme de notificare a conținutului ilegal și un **mod de prelucrare** a notificărilor
- **elaborează o** expunere de motive clară și specifică pentru restricțiile impuse

## Obligații suplimentare aplicabile furnizorilor de platforme online

- **modul de funcționare** a sistemului de soluționare a plângerilor
- **emiterea prealabilă a unui avertisment**
- **decizie** cu privire la suspendare și la circumstanțele relevante
- **publică**, în condițiile generale de utilizare, politica de utilizare abuzivă

## Obligații suplimentare aplicabile furnizorilor de platforme online

- **publică** raportul privind litigiile
- **publică** numărul mediu lunar de destinatari activi
- **acordă acces la** modul în care sunt **proiectate** interfețele online

## Tipuri de conținut ilegal (exemple)

În cazul în care conținutul constituie/vizează	Poate fi ilegal în temeiul...
O amenințare a unei persoane cu săvârșirea unei infracțiuni sau a unei fapte păgubitoare îndreptate împotriva sa ori a altei persoane	Art.206 din Codul penal
Parte a unei campanii de hărțuire (cum ar fi cyberbullying)	Art. 208 din Codul penal
Incitarea la suicid	Art. 191 din Codul penal
Partajarea neconsensuală a imaginilor	Art. 226 din Codul penal
Traficul de arme	Art. 342 din Codul penal
Amenințarea unei persoane sau a unui grup de persoane, prin intermediul unui sistem informatic, cu săvârșirea unei infracțiuni pentru care maximul pedepsei prevăzute de lege este închisoarea de cel puțin 5 ani, pe motiv de rasă, culoare, ascendență sau origine națională ori etnică sau în considerarea religiei	Ordonanța de Urgență a Guvernului nr. 31/2002
Constituirea unei organizații cu caracter fascist, rasist ori xenofob, precum și aderarea sau sprijinirea, sub orice formă, a unui astfel de grup	Ordonanța de Urgență a Guvernului nr. 31/2002

*\*Tabelul nu reprezintă o listă exhaustivă și nu are valoare de consultanță juridică. Alte exemple de conținut posibil ilegal includ promovarea înșelăciunii sau a produselor nesigure sau ilegale, încălcarea drepturilor de autor, dezvăluirea ilegală a datelor cu caracter personal, produse ilegale etc.*

# Măsuri împotriva conținutului ilegal

## Soluții posibile:

1. Notificarea informației de către **destinatarul serviciului** – art. 16 din Regulament
2. Informarea din partea **notificatorului de încredere** – art. 22 din Regulament
3. Emiterea **ordinului de acțiune împotriva conținutului ilegal** – art. 7-8 din Legea nr. 50/2024 și art. 9 din Regulament.

\*opțiunile ar putea fi abordate independent una de alta

## **Pentru soluția de la pct. 1:**

- ✓ furnizorii de servicii de găzduire instituie mecanisme care să permită oricărei persoane să notifice informații pe care le consideră conținut ilegal;
- ✓ notificările trebuie să conțină: explicație/justificare, o indicație a localizării informației (URL), numele și adresa de e-mail ale persoanei care face notificarea și o declarație a persoanei care transmite notificarea [art. 16 (2) din Regulament].

## **Pentru soluția de la pct. 2:**

- ✓ furnizorii de platforme online iau măsuri pentru a trata cu prioritate notificările primite din partea notificatorului de încredere.

## **Pentru soluția de la pct. 3:**

- ✓ analiza pe fond este realizată de autoritatea relevantă ce deține competențele specifice unui sector sau domeniu de activitate;
- ✓ autoritatea relevantă emite ordinul de eliminare conform art. 7 din Legea nr. 50/2024.

## Măsuri împotriva conținutului ilegal

Legea nr. 50/2024 instituie posibilitatea autorităților sau instituțiilor publice ce dețin atribuții cu privire la supravegherea unui anumit domeniu sau sector de activitate de a emite ere a ordinele de eliminare (soluția nr. 3)

„conținut ilegal” înseamnă orice informație care, în sine sau prin raportare la o activitate, inclusiv vânzarea de produse sau furnizarea de servicii, nu este conformă cu dreptul Uniunii sau cu dreptul oricărui stat membru care este conform cu dreptul Uniunii, indiferent de obiectul sau natura exactă a dreptului respectiv (art. 3 lit. h din Regulament).



### Important:

- Cadrul național în vigoare trebuie să califice o anumită situație sau un anumit produs ca fiind ilegal.
- Cadrul național specific pe domeniu de activitate trebuie să conțină obligația de a acționa împotriva conținutului ilegal.

Un număr semnificativ dintre obligațiile prevăzute în Regulamentul privind serviciile digitale se referă la modul în care furnizorii de servicii intermediare tratează conținutul ilegal. Aceștia au obligații specifice cu privire la conținutul ilegal atunci când acesta le este notificat.

Principiul exonerării de răspundere (existent încă din Directiva privind comerțul electronic) nu se mai aplică dacă există o notificare referitoare la conținutul ilegal [art. 16 alin. (2) din Regulament].



## Atribuții ANCOM în privința conținutului ilegal

ANCOM nu preia atribuțiile autorităților publice în domeniile lor de activitate

Primește ordinele de a acționa împotriva conținutului ilegal emise de autoritățile judiciare sau administrative naționale relevante și le transmite DSC-urilor din celelalte state

Primește ordinele de a furniza informații emise de autoritățile judiciare sau administrative naționale relevante și le transmite DSC-urilor din celelalte state

DSC-ul (ANCOM) nu are competențe pentru verificarea ordinelor (formă sau fond) ce se emit de autoritățile relevante în domeniile lor de activitate

### Autoritățile administrative naționale relevante (AR)

- Este necesară identificarea tuturor autorităților administrative relevante
- Ar fi utilă identificarea domeniului de competență pentru fiecare AR
- DSC ar putea acorda acces AR la datele de contact ale FSI (obținute în urma notificării) pentru a facilita transmiterea ordinelor, în măsura în care activitatea FSI este cunoscută

**ANCOM, în calitate de DSC, verifică modul în care furnizorii de servicii intermediare respectă obligațiile ce le revin conform Regulamentului privind serviciile digitale, dar NU are rol de moderare a conținutului, nu poate să acționeze ca organism de apel împotriva deciziilor furnizorilor de servicii intermediare în legătură cu conținutul ilegal și nu poate să acționeze ca autoritate extrajudiciară în litigiile dintre diferite părți sau diferiți utilizatori cu privire la conținutul ilegal.**

## Activitatea ANCOM în implementarea Regulamentului DSA

ANCOM a acordat suport constant și consistent **autorităților relevante** încă de la momentul desemnării sale oficiale ca DSC și a rămas în contact permanent cu Comisia Europeană prin participarea fizică sau online la întâlniri

- Scrisoare ANCOM către **37 de instituții relevante** din România (spre știință MAE, SGG și Cancelariei Primului Ministru) – precizări menite a consolida aplicarea Regulamentului DSA și a Legii nr. 50/2024
- Scrisoare ANCOM către **27 de autorități relevante** (spre știință MAE, SGG și Cancelariei Primului Ministru) - reiterarea competențelor autorităților relevante de a acționa împotriva conținutului ilegal
- Organizarea sau participarea la 23 de întâlniri importante cu autorități relevante din România (**MCID, DNSC, CNA, MAI, AEP, CNCD, UNBR, PICCJ, INM, IGPR, MAE, ASF, Procurorul General al României**), precum și cu platformele sociale **TikTok, META, Twitter, Microsoft, Google** pentru a discuta aspecte esențiale legate de reglementarea serviciilor digitale
- 4 videoconferințe și 4 adrese sau scrisori oficiale transmise către marile platforme despre obligațiile ce le revin odată cu demararea procesului electoral, pentru a solicita tratarea solicitărilor AEP cu prioritate și urgență sau pentru a le indica prevederile relevante din Elections Guidelines
- 5 întâlniri cu societatea civilă precum **ExpertForum, Activewatch, Centrul pentru Jurnalism Independent, Funky Citizens, GRADO, Declic**
- Material informativ dedicat AR-urilor - dispozițiile Regulamentului privind serviciile digitale și ale Legii nr. 50/2024
- Campanie ANCOM de informare despre DSA pe rețelele sociale: transmiterea a 22 de comunicate de presă și distribuirea de postări pe Facebook (21 postări) și LinkedIn (16 postări)
- Seminar ANCOM dedicat reprezentanților mass media
- **Scrisori ANCOM** către **Autoritatea Națională pentru Protecția Drepturilor Copilului și Adopție** referitor la tratarea conținutului ilegal în mediul online, dar și la modalități de acțiune împotriva conținutului online vătămător, dar nu ilegal, de genul provocărilor periculoase diseminate pe platforma online foarte mare TikTok
- Alte întâlniri cu diverse autorități precum INM, Uniunea Națională a Barourilor din România, Asociația bibliotecilor publice ANBPR

# Regulamentul privind serviciile digitale: combaterea dezinformării online

Codul de bune practici privind dezinformarea\* (integrat drept cod de conduită în cadrul DSA la 13 februarie 2025) stabilește setul de reguli ce trebuie urmărite în vederea adoptării de măsuri menite să combată dezinformarea în mediul online

<https://disinfocode.eu/subscriptions-forms/>

Platformele online au o serie de obligații în considerarea unor articole din Regulamentul (UE) 2022/2065:

- art. 26 – Publicitatea pe platformele online;
- art. 27 – Transparența sistemelor de recomandare;
- art. 34 – Evaluarea riscurilor; **VLOP**
- art. 35 – Atenuarea riscurilor; **VLOP**
- art. 39 – Cerințe suplimentare în materie de transparență a publicității online; **VLOP**
- art. 40 – Accesul la date și controlul acestora; **VLOP**
- art. 41 – Funcția de conformitate; **VLOP**
- art. 42 – Obligații de raportare în materie de transparență; **VLOP**

Regulamentul de stabilire a unor norme armonizate privind inteligența artificială și de modificare a anumitor acte legislative ale uniunii (Artificial Intelligence Act – AIA)

- Publicat la mijlocul anului 2024
- Termene de implementare = începând cu august 2025

- [2022 Strengthened Code of Practice on Disinformation | Shaping Europe's digital future \(europa.eu\)](https://europa.eu)

# Combaterea dezinformării online

## Codul de bune practici privind dezinformarea din 2022:

### Change of CoP commitments 2022 – 2025 by topic:

CoP Section	2022*	2025*	% Change
Advertising	73	45	-38,36%
<b>Empowering the fact-checking community</b>	<b>73</b>	<b>26</b>	<b>-64,38%</b>
<b>Empowering the research community</b>	<b>82</b>	<b>39</b>	<b>-52,44%</b>
Empowering users	110	74	-32,73%
Integrity of Services	47	42	-10,64%
Monitoring of the Code	145	111	-23,45%
Permanent task-force	66	63	-4,55%
<b>Political Advertising</b>	<b>105</b>	<b>47</b>	<b>-55,24%</b>
Transparency Centre	154	139	-9,74%
Grand Total	855	586	-31,46%

Platforms reduced their commitments in the Code of Practice (CoP) by **31.46%**.

The most impacted measures were those supporting the **fact-checking community**, followed by measures on **political advertising** and on **empowering the research community**.

\*This represents the total number of measures subscribed to by all platforms combined. It is calculated by adding up the measures for each platform.

## Combaterea dezinformării online

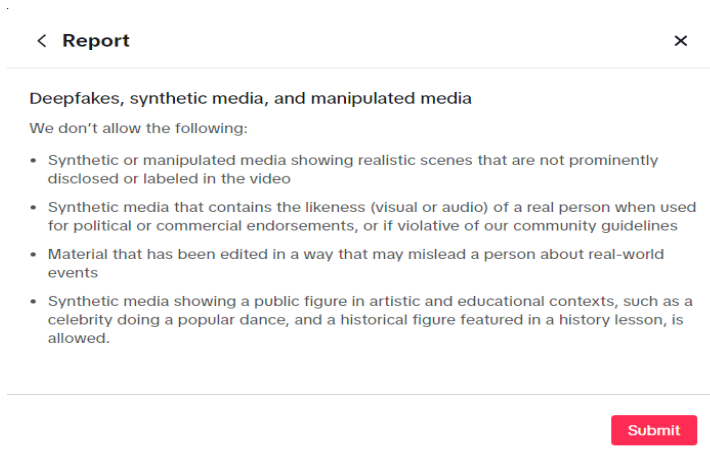
### Ghidul privind reducerea riscurilor sistemice pentru procesele electorale:

- destinat marilor platforme online
- elaborat în temeiul **art. 35** din Regulamentul privind serviciile digitale și aplicabil furnizorilor de platforme online foarte mari (**VLOP**) și de motoare de căutare online mari și foarte mari (**VLOSE**);
- are în vedere obligațiile stabilite prin **Regulamentul (UE) 2024/900** al Parlamentului European și al Consiliului din 13 martie 2024 privind transparența și vizarea unui public-țintă în publicitatea politică;
- conține norme pentru alegerile europene sau cele care au loc la nivel național;
- **VLOP + VLOSE** trebuie să prezinte pe platformele lor informații oficiale privind procesele electorale;
- încurajează colaborarea cu organismele media naționale pentru creșterea gradului de conștientizare și crearea de campanii referitoare la desfășurarea alegerilor;
- instituirea de măsuri privind furnizarea de informații de context pentru desfășurarea alegerilor;
- verificarea sistemelor de recomandare [recitalurile 70, 84, 88 și 94, precum și art. 34 alin. (2) din Regulament];
- etichetarea conținutului produs cu ajutorul sistemelor de IA și efectuarea de eforturi pentru ca informațiile generate de sistemele de IA să se bazeze pe surse fiabile în contextul electoral, cum ar fi sursele oficiale de informații de la autoritatea electorală;
- Comisia Europeană recomandă ca **VLOP + VLOSE** să facă schimb de informații în mod regulat și, dacă este necesar, în regim de urgență, și să aibă puncte de contact pentru autoritățile naționale și europene competente (coordonatorul serviciilor digitale și autoritatea competentă în materie electorală);
- Autoritatea electorală poate informa **VLOP + VLOSE** cu privire la procesul de vot în vederea integrării informațiilor în serviciile furnizate și poate transmite date cu privire la eventualele riscuri în jurul proceselor electorale.

# Combaterea dezinformării online

## Ghidul privind reducerea riscurilor sistemice pentru procesele electorale:

- recomandă **VLOP** și **VLOSE** aplicarea în avans a **Regulamentului (UE) 2024/900** al Parlamentului European și al Consiliului din 13 martie 2024 privind transparența și vizarea unui public-țintă în publicitatea politică;
- recomandă **VLOP** și **VLOSE** aplicarea în avans a **Regulamentului AI** (etichetarea conținutului generat de sistemele AI, marcarea adecvată sau instituirea de politici pentru eliminare);
  - se recomandă inclusiv instituirea posibilității pentru utilizatori de a semnala un conținut ca fiind deepfake;
  - exemplu: TikTok
- recomandă **VLOP** și **VLOSE** cunoașterea sistemului care gestionează alegerile (e.g. AEP & BEC, perioada de desfășurare a campaniilor);
- **este recomandată instituirea de puncte de contact între VLOP/VLOSE și autoritățile naționale;**
- în perioada alegerilor VLOP/VLOSE trebuie să colaboreze cu organizații independente de verificare (fact-checking) și să instituie mecanisme interne de răspuns.



## Combaterea dezinformării online

### Foreign Information Manipulation and Interference (FIMI)

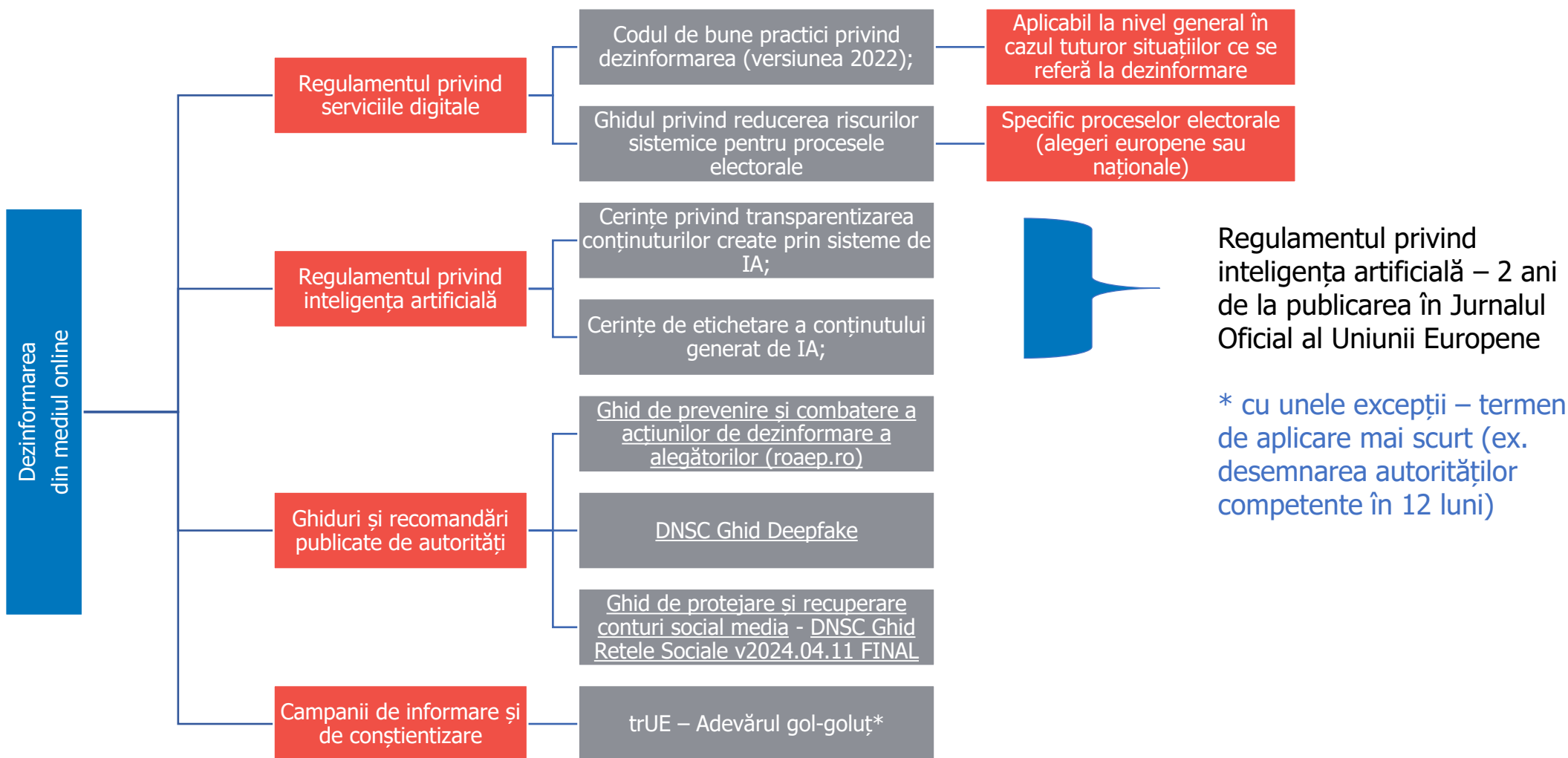
- Proiect al Serviciului European de Acțiune Externă ([https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference\\_en](https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en))
- Al doilea raport conține un toolkit ce poate ajuta autoritățile naționale cu atribuții în domeniu să combată FIMI ([https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats\\_en](https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en));
- Ghidul practic pentru efectuarea investigațiilor cu sursă deschisă (noiembrie 2024), material disponibil la [https://www.eeas.europa.eu/eeas/how-detect-analyse-identity-based-disinformationfimi-practical-guide-conduct-open-source\\_en](https://www.eeas.europa.eu/eeas/how-detect-analyse-identity-based-disinformationfimi-practical-guide-conduct-open-source_en))
- Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory.



- [2022 Strengthened Code of Practice on Disinformation | Shaping Europe's digital future \(europa.eu\)](https://european-council.europa.eu/media/e3001420/1622224/1622224_en.pdf)



# Combaterea dezinformării online



\* [https://romania.representation.ec.europa.eu/stiri-evenimente-si-resurse-pentru-presa/true-adevarul-gol-golul\\_ro](https://romania.representation.ec.europa.eu/stiri-evenimente-si-resurse-pentru-presa/true-adevarul-gol-golul_ro)

## Activități pentru combaterea dezinformării

**Decembrie 2024** – ANCOM inițiază discuții cu reprezentanții MAI, MAE, CNA, MAPN, DNSC în cadrul unei întâlniri de lucru privind derularea unei campanii de conștientizare și educare a publicului cu privire la dezinformare

**Ianuarie 2025** – ANCOM a discutat cu reprezentanții MAI despre posibile scenarii de implementare a acestei campanii

**Decembrie – ianuarie** – ANCOM a derulat deja o mini-campanie de informare pe rețelele proprii de social media cu privire la dezinformare

<https://www.facebook.com/ancom.ro/>

## Ce urmează?

Srijin pentru autoritățile relevante, contact permanent cu Comisia Europeană, cu reprezentanții societății civile și utilizatori

Organizarea unei serii de evenimente, întâlniri și mese rotunde cu:

- **Autorități relevante în domeniul electoral** pentru clarificarea rolurilor în contextul alegerilor: AEP, CNA, MAI, MAE, DNSC, CNCD;
- **Potențiali candidați** la funcția de președinte al statului (actori politici);
- **Organizații non-guvernamentale** pentru dezvoltarea cooperării în contextul DSA;
- Întâlnire **exercițiu** cu **AEP, CNA, MAI, MAE, CE, VLOPs și organizații neguvernamentale** pentru testarea capacităților participanților în context de alegeri;
- **Creatori digitali**, CNA, AEP, MAI/MAE pentru familiarizarea cu rolurile autorităților publice.

Campanie TV, radio și online pentru informarea publicului cu privire la serviciile digitale

Împreună cu MAI - desfășurarea unei campanii de informare cu privire la dezinformare și manipulare

**Vă mulțumesc!**

