CAPACITATEA UNIUNII EUROPENE DE A ABORDA DEZINFORMAREA, MANIPULAREA INFORMAȚIILOR ȘI INTERFERENȚELE STRĂINE

THE EUROPEAN UNION'S CAPACITY TO ADDRESS DISINFORMATION, INFORMATION MANIPULATION, AND FOREIGN INTERFERENCE

Carmelita GAȚAPUC
Universitatea de Stat din Moldova
e-mail: *carmelitagatpuc8@gmail.com*

CZU 323.266:316.776.23

Rezumat. Articolul examinează în profunzime modul în care Uniunea Europeană (UE) dezvoltă și implementează politici, mecanisme și instrumente pentru prevenirea, detectarea și combaterea dezinformării, manipulării informațiilor și interferențelor străine (FIMI). Analiza se bazează pe cadrul legislativ (inclusiv Digital Services Act), mecanisme operaționale precum Sistemul de Alertă Rapidă (RAS), instrumente de autoreglementare și coreglementare (Codul consolidat de bune practici privind dezinformarea) și infrastructuri specializate (EUvsDisinfo, rapoartele FIMI). Studiul evidențiază rolul educației media, al cooperării transnaționale și al sancțiunilor diplomatice în consolidarea rezilienței democratice europene. Sunt abordate provocările generate de evoluțiile tehnologice, în special de inteligența artificială generativă, care amplifică riscurile de manipulare informațională. Concluzia subliniază că protejarea spațiului informațional european necesită o abordare adaptivă, integrată și colaborativă, care să mențină echilibrul între libertatea de exprimare și securitatea democratică. Articolul este elaborat în cadrul implementării proiectului Jean Monnet Chair „EU's role in the emerging international system” (EUREIS), nr. 101126798.

Cuvinte cheie: *dezinformare, manipulare informațională, interferențe străine, reziliență democratică, Digital Services Act.*

JEL: D83, L86, K23

Abstract. This article provides an in-depth analysis of how the European Union (EU) develops and implements policies, mechanisms, and tools to prevent, detect, and counter disinformation, information manipulation, and foreign information manipulation and interference (FIMI). The study draws on the legislative framework (including the Digital Services Act), operational mechanisms such as the Rapid Alert System (RAS), self-regulation and co-regulation instruments (the strengthened Code of Practice on Disinformation), and specialized infrastructures (EUvsDisinfo, FIMI reports). It highlights the role of media literacy, transnational cooperation, and diplomatic sanctions in enhancing the EU's democratic resilience. The paper also addresses the challenges posed by technological advances, particularly generative artificial intelligence, which intensifies the risks of information manipulation. The

conclusion emphasizes that safeguarding the EU’s information space requires an adaptive, integrated, and collaborative approach that balances freedom of expression with democratic security. The article has been prepared within the framework of the implementation of the Jean Monnet Chair project “EU’s Role in the Emerging International System” (EUREIS), No. 101126798.

Keywords: *disinformation, information manipulation, foreign interference, democratic resilience, Digital Services Act.*

JEL: D83, L86, K23

Introducere. Într-o eră a vitezei informaționale, în care milioane de date circulă neîngrădite în spațiul digital, provocările generate de fenomenul dezinformării s-au transformat într-o preocupare centrală pentru state, instituții internaționale și societăți democratice. Uniunea Europeană (UE), ca spațiu al valorilor democratice și al statului de drept, se confruntă în mod constant cu acest pericol subtil și invaziv. Dezinformarea nu este un fenomen recent, însă amploarea și profunzimea cu care afectează structura democratică și coeziunea socială sunt fără precedent. Din acest motiv, tema abordării dezinformării, manipulării informaționale și interferenței străine nu este doar de actualitate, ci una de o stringență majoră, care necesită acțiuni coordonate, reglementări stricte și conștientizare publică la toate nivelurile. Conform opiniei profesorului universitar Svetlana Cebotari, dezinformarea este fabricarea, distorsionarea sau manipularea conștientă a informațiilor, cu scopul de a înșela publicul și a produce un efect concret.[1]

Dezinformarea, spre deosebire de simpla eroare informativă sau ignoranță, este un fenomen cu intenționalitate clară. Ea presupune fabricarea, distorsionarea sau manipularea conștientă a unor informații, cu scopul de a înșela publicul și a produce un efect concret: inducerea în eroare, polarizarea opiniei publice, slăbirea încrederii în instituții sau destabilizarea unor regimuri democratice. Se face adesea prin amestecarea adevărului cu minciuna, prin utilizarea de surse false, prin apelul la emoții și frici colective, sau prin repetarea obsesivă a unor narațiuni care răspund unor interese externe. Astfel, dezinformarea devine o armă hibridă, un mijloc de luptă în războaiele informaționale contemporane, desfășurate adesea în afara cadrului clasic militar, dar cu potențial distructiv comparabil. Din acest motiv, în terminologia modernă de securitate, dezinformarea este clasificată ca o amenințare la adresa securității naționale și a ordinii constituționale.

Gradul de investigare a problemei la momentul actual, **scopul cercetării.** Studiile recente, rapoartele oficiale ale Serviciului European de Acțiune Externă (SEAE) și investigațiile serviciilor specializate, precum VIGINUM, au documentat atât amploarea, cât și complexitatea mecanismelor utilizate în campaniile de manipulare informațională. Cazuri precum rețeaua „Portal Kombat” au relevat modul în

care infrastructurile digitale pot fi utilizate pentru a redistribui masiv conținut manipulator, cu impact direct asupra pluralismului, democrației și libertății de informare. Concomitent, evoluțiile tehnologice recente, în special în domeniul inteligenței artificiale generative, au multiplicat exponențial riscurile, facilitând producerea de materiale *deepfake* și automatizarea campaniilor de influență, cu efecte potențial destabilizatoare asupra proceselor electorale, așa cum s-a observat în contextul alegerilor europarlamentare din 2024. Acestea includ rețele transfrontaliere de site-uri coordonate, optimizarea conținutului pentru motoare de căutare, integrarea tehnologiilor AI generative și utilizarea tacticilor de micro-țintire pentru influențarea opiniilor publice. Fenomenul este recunoscut ca amenințare strategică la adresa securității naționale, coeziunii sociale și integrității proceselor democratice, fiind integrat în strategiile UE de contracarare a amenințărilor hibride. Instrumente precum Digital Services Act, Sistemul de Alertă Rapidă și Codul de bune practici privind dezinformarea sunt deja operaționalizate și monitorizate, generând rezultate concrete, însă analiza academică indică necesitatea consolidării continue a cadrului normativ și a capacităților operaționale.

Scopul cercetării este de a examina în profunzime modul în care UE dezvoltă și implementează politici, mecanisme și instrumente pentru prevenirea, detectarea și combaterea dezinformării, manipulării informaționale și interferențelor străine. Studiul își propune să evalueze eficiența reglementărilor adoptate, capacitatea de reacție a instituțiilor europene și gradul de adaptare la noile riscuri generate de tehnologiile emergente, în special inteligența artificială generativă. Totodată, cercetarea urmărește identificarea provocărilor persistente, precum echilibrul între libertatea de exprimare și protecția spațiului informațional, precum și formularea de recomandări pentru creșterea rezilienței digitale a UE. În acest sens, analiza va integra perspective instituționale, juridice și tehnologice, corelate cu studii de caz relevante, pentru a oferi o înțelegere comprehensivă a fenomenului și a răspunsurilor strategice europene.

Materiale utilizate și metode aplicate. Studiul de față se bazează pe o analiză comprehensivă a cadrului legislativ, instituțional și operațional dezvoltat de UE, pentru combaterea fenomenului dezinformării și a interferențelor informaționale străine (FIMI). Materialul documentar a fost constituit din surse oficiale ale UE, inclusiv Regulamentul (UE) 2022/2065 privind serviciile digitale (Digital Services Act – DSA), rapoartele anuale elaborate de SEAE în domeniul FIMI, precum și documente strategice conexe, cum ar fi Codul consolidat de bune practici privind dezinformarea și Planul de acțiune pentru democrația europeană. Acestea au fost completate cu investigații tehnice și rapoarte publicate de entități specializate, precum VIGINUM (serviciul tehnic francez dedicat combaterii ingerințelor digitale), inclusiv studiul de caz asupra rețelei „Portal Kombat”, și de platforma EUvsDisinfo, recunoscută

la nivel european pentru activitatea de documentare și analiză a campaniilor de manipulare pro-Kremlin. Au fost consultate, de asemenea, *surse open-source*, articole științifice și analize media, cu scopul de a identifica atât dimensiunea fenomenului dezinformării, cât și impactul noilor tehnologii – în special al inteligenței artificiale generative – asupra propagării acestuia. Studiul a integrat și date furnizate de organisme internaționale partenere ale UE, precum NATO și G7, în special în ceea ce privește mecanismele de coordonare și răspuns comun la campaniile informaționale ostile.

Metodologia aplicată a avut un caracter multidimensional. *În primul rând*, s-a recurs la *analiza calitativă a documentelor*, pentru a evidenția prevederile cheie, angajamentele asumate și mecanismele instituționale relevante. *În al doilea rând*, s-a utilizat *analiza de conținut* a materialelor de dezinformare documentate de *EUvsDisinfo* și în rapoartele FIMI, pentru identificarea tiparelor narative și a tehnicilor de manipulare. *În al treilea rând*, au fost analizate elemente tehnice ale campaniilor digitale, prin preluarea rezultatelor investigațiilor OSINT (*Open Source Intelligence*) efectuate de actori specializați, vizând infrastructura digitală (IP-uri comune, cod HTML, faviconuri identice), rețelele de site-uri coordonate și optimizarea acestora pentru motoarele de căutare. Abordarea a inclus analiza comparativă, prin raportarea măsurilor adoptate de UE la bunele practici internaționale în domeniul combaterii dezinformării, precum și o componentă evaluativă, menită să aprecieze eficacitatea instrumentelor europene în raport cu provocările emergente, cum sunt campaniile automatizate sau conținuturile *deepfake*. Această structură metodologică a permis nu doar identificarea vulnerabilităților actuale ale spațiului informațional european, ci și formularea unor direcții strategice pentru consolidarea rezilienței democratice în era digitală.

Rezultatele obținute în baza analizelor științifice efectuate. Identificarea rețelelor de dezinformare: Investigarea rețelei „Portal Kombat» a evidențiat peste 190 de site-uri aparent independente, dar care aparțin unei rețele coordonate de propagandă pro-Kremlin. Acestea redistribuie conținut preluat din surse rusești, afectând valori fundamentale ale UE precum pluralismul și democrația. Implementarea instrumentelor UE: *Digital Services Act* (DSA) a introdus reglementări stricte pentru platformele online, inclusiv obligația de a eticheta conținutul generat de AI și de a asigura transparența algoritmilor. Sistemul de Alertă Rapidă (RAS) a fost activat cu succes în timpul alegerilor europarlamentare din 2019 și pandemiei COVID-19.

Educație și conștientizare: Inițiative, precum *EUvsDisinfo,* au documentat peste 15.000 de cazuri de dezinformare, contribuind la creșterea alfabetizării mediatice în UE. Totuși, provocările rămân uriașe. Cum putem proteja libertatea de exprimare fără a decupla controlul asupra conținutului dăunător? Cum adaptăm reglementările

la viteza fulgerătoare a tehnologiei? Și, mai ales, cum construim o imunitate colectivă împotriva dezinformării într-o societate tot mai fragmentată? Răspunsul pare să fie o combinație de educație media (prin programe precum EUvsDisinfo), transparență (obligând platformele să dezvăluie algoritmii), și cooperare transnațională (extinzând rețelele de *fact-checking*).

Care sunt riscurile dezinformării? Dezinformarea atacă pilonii esențiali ai unui stat democratic – transparența, participarea, pluralismul și legitimitatea instituțiilor. Atunci când cetățenii nu mai pot distinge între real și fals, între adevăr și manipulare, capacitatea lor de a lua decizii informate este serios compromisă. Mesajele de dezinformare sunt adesea construite pentru a diviza, pentru a exploata tensiuni identitare, culturale, religioase sau economice. Ele creează două realități paralele în care fiecare tabără se radicalizează împotriva celeilalte. Unul din scopurile dezinformării este decredibilizarea surselor oficiale și stimularea neîncrederii în presă. Într-un climat de suspiciune generalizată, autoritățile își pierd capacitatea de a gestiona crize sau de a mobiliza populația în momente critice. Tehnologiile, în special inteligența artificială, au dus la apariția unor instrumente extrem de periculoase, precum *deepfakes* – clipuri audio/video false dar convingătoare. Acestea pot fi folosite pentru a crea scandaluri false, a induce panică sau a sabota lideri politici și procese democratice. Un exemplu recent este rețeau „Portal Kombat", identificată și documentată în perioada septembrie–decembrie 2023 de către VIGINUM, serviciul tehnic specializat al Franței în combaterea ingerințelor digitale străine. Deși investigația este inițiată de o instituție națională franceză, impactul său este unul profund european, având în vedere că rețeaua vizează în mod direct mai multe state membre ale Uniunii Europene care susțin Ucraina în contextul războiului (precum Franța, Germania, Polonia sau Spania), prin intermediul unor site-uri precum *pravda-fr[.]com*, *pravda-pl[.]com* etc.[3]

Din punct de vedere metodologic, investigația VIGINUM s-a bazat pe surse *open-source* și o analiză tehnică detaliată, care a inclus examinarea infrastructurii digitale, identificarea IP-urilor comune, a codului HTML similar, a faviconurilor identice și, nu în ultimul rând, analiza conținutului publicat. Astfel, au fost descoperite peste 190 de site-uri aparent independente, dar care aparțin, în realitate, unei rețele coordonate de propagandă pro-Kremlin. Aceste portaluri nu produc conținut original, ci redistribuie materiale preluate masiv din surse rusești: agenții de presă, canale de Telegram sau site-uri oficiale locale.

Importanța acestui caz constă în demonstrarea modului în care pot fi afectate în mod direct valorile fundamentale ale UE, precum pluralismul, democrația, libertatea de informare, coeziunea statelor membre și securitatea digitală. În plus, faptul că respectivele conținuturi sunt optimizate pentru a apărea în rezultatele motoarelor de căutare (Google) le conferă o periculozitate sporită, mai ales în contextul alegerilor

europene, al crizelor geopolitice sau al proceselor decizionale comune din cadrul UE și NATO. Prin urmare, este evident că Uniunea Europeană devine, în mod implicit, o țintă strategică a acestei rețele. Acest lucru subliniază necesitatea continuării și consolidării sprijinului pentru astfel de investigații, precum și importanța implementării unor politici de reglementare eficiente, cum este cazul Digital Services Act, care vine să responsabilizeze platformele online în lupta împotriva manipulării informaționale.

Un exemplu concret al vulnerabilităților actuale ale UE în fața fenomenului dezinformării este contextul alegerilor europarlamentare din 2024. Aproximativ 360 de milioane de cetățeni din cele 27 de state membre sunt chemați la vot pentru desemnarea celor 720 de membri ai Parlamentului European, într-un moment geopolitic tensionat și profund marcat de insecuritate informațională. Experții avertizează în continuare, că inteligența artificială generativă a devenit un amplificator major al riscurilor de dezinformare. În prezent nu mai este nevoie de „*ferme de troli*" care să redacteze manual mesaje propagandistice, deoarece orice individ cu intenții malițioase poate crea, cu ajutorul unui software AI, imagini, videoclipuri sau înregistrări audio, care simulează realitatea, inducând în eroare alegătorii.

În preajma alegerilor europene, autoritățile și cercetătorii au constatat o creștere alarmantă a volumului și diversității conținutului dezinformativ, în special a aceluia cu tentă anti-UE, anti-NATO și anti-Ucraina. Cazurile de dezinformare documentate în state membre ale UE sunt relevante și îngrijorătoare. În Spania, un site fals care imita o autoritate locală a difuzat un articol despre un presupus atac terorist iminent, exact înaintea alegerilor naționale. În Polonia, o amenințare falsă cu bombă a fost mediatizată intens prin canale asociate cu interferența rusă. În Slovacia, înregistrări audio generate prin AI, care prezentau în mod fals un candidat discutând despre fraudarea votului, s-au răspândit masiv înainte de alegerile parlamentare. De asemenea, agenția de presă națională a Poloniei a fost victima unui atac cibernetic, fiind publicat un comunicat fals atribuit prim-ministrului, cu implicații grave de securitate. [4] Toate aceste exemple demonstrează că obiectivul acestor campanii nu este doar manipularea alegerilor în sine, ci și erodarea încrederii cetățenilor în mecanismele democratice, în autorități și în presă. Scopul este divizarea societății, accentuarea polarizării și crearea unei percepții de instabilitate și haos instituțional.

În fața intensificării fenomenului de dezinformare, UE a dezvoltat un cadru complex de acțiune strategică și instituțională, menit să protejeze procesele democratice, coeziunea internă și securitatea informațională a statelor membre. Un pilon central al acestui efort îl constituie abordarea FIMI – *Foreign Information Manipulation and Interference* (Manipularea și Interferența Informațiilor Străine), coordonată în principal de Serviciul European de Acțiune Externă.[5]

Abordarea FIMI are ca obiectiv protejarea Politicii Externe și de Securitate Comună (PESC) a Uniunii Europene, precum și a integrității proceselor democratice și a rezilienței cetățenilor UE. Lansată inițial ca răspuns la campaniile rusești de dezinformare din 2015, această inițiativă a evoluat într-o strategie solidă, cu aplicabilitate globală și instrumente operaționale concrete. Prin combaterea FIMI, SEAE urmărește să prevină manipularea informațiilor cu caracter strategic, să expună actorii statali și nestatali implicați, să consolideze reziliența democratică a UE, și să promoveze un spațiu informațional sigur, pluralist și transparent.

SEAE acționează pe baza unui cadru de patru piloni strategici, fiecare cu funcții distincte:

Prin sistemul de alertă rapidă (Rapid Alert System – RAS), UE colectează și distribuie informații despre campanii de dezinformare în derulare, facilitând cooperarea între statele membre și instituții. SEAE dezvoltă și publică rapoarte anuale FIMI, oferind analize detaliate despre actorii, tacticile și narativele manipulative folosite (ex. Rusia, China).

Prin inițiative de educație media, sprijinirea mass-mediei independente, proiecte pentru societatea civilă și rețele de *fact-checking*, UE urmărește să reducă vulnerabilitățile populației în fața propagandei. Tot aici se încadrează FIMI ISAC, centrul de schimb și analiză a informațiilor, creat pentru a susține cooperarea între actori instituționali și non-guvernamentali.

UE adoptă și implementează instrumente legislative ale *Digital Services Act*, obligând platformele online mari să limiteze răspândirea dezinformării și să eticheteze conținutul fals sau generat de AI (ex. *deepfake*-uri). De asemenea, sunt impuse sancțiuni diplomatice actorilor statali implicați, precum în cazul Rusiei.

SEAE colaborează cu parteneri internaționali (NATO, G7) prin Mecanismul de răspuns rapid (RRM), coordonând răspunsuri comune la interferențele informaționale și susținând sancțiuni. De asemenea, promovează excluderea narativelor manipulative din spațiul public global, prin acțiuni de atribuire politică și expunere publică a autorilor campaniilor FIMI. UE prin intermediul SEAE a demonstrat în ultimii ani că abordarea fenomenului FIMI nu rămâne doar la nivel declarativ, ci se concretizează în rezultate tangibile, strategii coerente și instrumente care contribuie efectiv la protejarea spațiului informațional european.[6]

Lansată în 2015 ca răspuns la campaniile de manipulare informațională orchestrate de Federația Rusă, *inițiativa EUvsDisinfo* s-a impus rapid ca unul dintre cele mai importante instrumente ale Uniunii Europene în domeniul combaterii dezinformării. Până în anul 2024, platforma a identificat și documentat peste 15.000 de cazuri de dezinformare pro-Kremlin, afectând nu doar statele membre ale UE, ci și țări din vecinătate precum Republica Moldova, Georgia sau Ucraina. Conținutul produs este

publicat în 13 limbi și ajunge anual la milioane de cetățeni, contribuind semnificativ la creșterea alfabetizării mediatice în spațiul european. Pe lângă funcția sa de monitorizare, EUvsDisinfo oferă analize tematice și resurse educaționale pentru jurnaliști, *fact-checkeri* și organizații civice, devenind un model de bună practică recunoscut la nivel internațional. Această inițiativă demonstrează capacitatea Uniunii Europene de a construi infrastructuri digitale specializate, menite nu doar să expună campaniile de manipulare, ci și să furnizeze publicului larg instrumente concrete pentru apărarea împotriva acestora. În completare, o contribuție deosebit de valoroasă este reprezentată de seria celor trei rapoarte *FIMI* (2022, 2023, 2024), elaborate de experții Serviciului European de Acțiune Externă (SEAE). Aceste documente sistematizează mii de incidente de manipulare și interferență informațională străină – de exemplu, raportul din 2023 a analizat aproximativ 750 de cazuri – acoperind campanii ce au vizat procese electorale, instituții europene, teme identitare și conflicte culturale.

Rapoartele introduc modele analitice comune, precum cadrul *ABCDE* (Actor, Behaviour, Content, Degree, Effect) și *taxonomiile TTP* (Tactics, Techniques, Procedures), care s-au dovedit extrem de utile pentru detectarea timpurie a campaniilor de manipulare. În plus, acestea au contribuit la armonizarea metodelor de analiză între statele membre ale UE, partenerii NATO și G7, fiind deja utilizate în numeroase intervenții diplomatice coordonate. Astfel, aceste rapoarte nu constituie doar instrumente tehnice de analiză, ci și un exemplu de transparență instituțională, prin care Uniunea Europeană își afirmă rolul de lider global în documentarea și contracararea interferențelor informaționale străine.

Sistemul de Alertă Rapidă (*Rapid Alert System* – RAS), creat în 2019, reprezintă unul dintre instrumentele cheie ale Uniunii Europene pentru detectarea și contracararea timpurie a campaniilor de dezinformare. De la implementarea sa, acest mecanism a fost testat și consolidat în contexte reale, demonstrându-și eficiența în situații critice. Prima activare majoră a avut loc în timpul alegerilor europarlamentare din 2019, când RAS a jucat un rol esențial în identificarea rapidă a narațiunilor false care circulau pe rețelele sociale, permițând o reacție coordonată între statele membre.

În perioada pandemiei de COVID-19, sistemul și-a confirmat utilitatea prin semnalarea și contracararea campaniilor de dezinformare legate de vaccinuri și de teoriile conspirației referitoare la așa-numita „dictatură sanitară". În 2024, RAS a fost modernizat prin integrarea unor componente de inteligență artificială, capabile să detecteze cu o viteză sporită campaniile automate, materialele deepfake și manipulările algoritmice, reducând semnificativ timpul de reacție în fața atacurilor informaționale concertate.

Complementar acestui mecanism, SEAE a dezvoltat și susține un portofoliu extins de proiecte dedicate consolidării capacităților societății civile și mass-mediei.

Printre acestea se numără programe de formare în domeniul *Open Source Intelligence* (OSINT), adresate jurnaliștilor, activiștilor și cercetătorilor; elaborarea de ghiduri pentru detectarea dezinformării bazate pe identitate (IBD), menite să contracareze polarizarea socială și discriminarea împotriva minorităților, femeilor și comunităților LGBTIQ+; precum și sprijin financiar și logistic pentru rețelele de *fact-checking* locale și regionale, precum EUfactcheck și EDMO. Prin aceste măsuri, UE nu se limitează la sancționarea dezinformării, ci investește în crearea unor sisteme democratice reziliente, în care cetățenii sunt formați să identifice manipularea informațională și să reacționeze în mod responsabil, contribuind astfel la protejarea integrității spațiului public european. Toate aceste realizări confirmă faptul că UE a depășit faza reactivă și s-a angajat într-o abordare proactivă, multidimensională și colaborativă în fața FIMI. De la infrastructură digitală (EUvsDisinfo), la intervenție rapidă (RAS), analiză standardizată (rapoartele FIMI), educație media și reglementare legislativă (DSA), UE creează un ecosistem coerent de apărare democratică.

Într-un context global instabil, în care frontierele digitale sunt tot mai fragile, consolidarea acestor mecanisme nu este doar o opțiune politică, ci o necesitate existențială pentru viitorul proiectului european. În condițiile de proliferare a dezinformării și al creșterii influenței actorilor străini în spațiul digital european, Uniunea Europeană a recunoscut necesitatea unui cadru legislativ ferm, capabil să reglementeze responsabilitățile platformelor online și să protejeze cetățenii împotriva manipulării informaționale. Astfel, a fost conceput *Digital Services Act* (DSA), un regulament ambițios care marchează un moment de cotitură în guvernanța digitală europeană, cu implicații directe asupra modului în care conținutul circulă pe internet și asupra capacității instituțiilor de a interveni împotriva fenomenelor precum dezinformarea, incitarea la ură, interferențele străine sau conținutul manipulator generat de inteligență artificială.[7]

Adoptat în 2022 și implementat progresiv începând cu anul 2023, DSA stabilește un set de reguli clare și obligatorii pentru toate serviciile digitale care facilitează interacțiuni între utilizatori și conținut online. Deși se aplică întregului ecosistem digital – de la furnizori de *hosting* și motoare de căutare până la rețele sociale și *marketplace*-uri – regulamentul are prevederi deosebit de stricte pentru așa-numitele „*platforme foarte mari*" (VLOP – Very Large Online Platforms), definite prin numărul de utilizatori activi. Platforme precum Facebook, Instagram, TikTok, X (fostul Twitter), YouTube, Amazon și Google Search intră sub această reglementare specială, având obligații sporite privind evaluarea riscurilor, transparența algoritmică, moderarea conținutului și cooperarea cu autoritățile europene.

DSA se fundamentează pe principiul „diligenței responsabile" (*due diligence*), conform căruia platformele digitale nu mai pot funcționa într-un regim de autoregle-

mentare voluntară, ci trebuie să adopte măsuri proactive pentru prevenirea riscurilor sistemice, inclusiv cele generate de campaniile de dezinformare sau interferență străină. Printre cele mai importante inovații aduse de regulament se numără obligația platformelor de a realiza evaluări periodice ale riscurilor pe care le generează în societate. Aceste riscuri pot include răspândirea deliberată a informațiilor false, utilizarea conturilor false în scopuri politice, promovarea unor narațiuni toxice prin algoritmi sau amplificarea conținuturilor care polarizează și fragmentează societatea. De asemenea, DSA impune o transparență fără precedent asupra algoritmilor de recomandare, cerând platformelor să explice modul în care funcționează aceste sisteme și să ofere utilizatorilor opțiunea de a dezactiva personalizarea bazată pe profilare. Astfel, cetățenii europeni obțin un control mai mare asupra fluxului informațional care le este prezentat, iar deciziile algoritmice nu mai rămân ascunse în cutii negre inaccesibile publicului.

Un alt element marcabil este asigurarea accesului la date pentru cercetători autorizați. Platformele trebuie să permită specialiștilor independenți să studieze efectele politicilor lor de moderare și de distribuție a conținutului, să analizeze campaniile de dezinformare și să evalueze impactul asupra opiniei publice și a proceselor democratice. Această măsură contribuie direct la consolidarea cercetării academice și a jurnalismului de investigație, oferind societății instrumente de autocorecție și adaptare la noile amenințări. În același timp, DSA răspunde provocărilor tot mai mari generate de inteligența artificială. În contextul în care conținuturile *deepfake* devin tot mai realiste și dificil de identificat, regulamentul prevede obligativitatea etichetării materialelor generate artificial care pot induce în eroare publicul, mai ales în perioade electorale. Este o măsură crucială pentru menținerea integrității spațiului democratic, mai ales în fața riscului ca manipulările audio-video să afecteze direct imaginea unor candidați sau încrederea în procesul electoral.

Un alt aspect important reglementat de DSA este introducerea unor mecanisme eficiente de reclamație și corectare a deciziilor de moderare. Utilizatorii care consideră că le-au fost eliminate nedrept conținuturile sau că au fost vizați de acțiuni arbitrare ale platformelor au acum posibilitatea de a contesta decizia și de a cere o reevaluare echitabilă. În paralel, autoritățile naționale și Comisia Europeană pot interveni direct pentru a impune măsuri corective și, în cazuri grave, pot aplica sancțiuni financiare semnificative – de până la 6% din cifra de afaceri globală a platformei în culpă.

Impactul DSA a început deja să se facă simțit. În 2024, Comisia Europeană a activat mai multe mecanisme prevăzute de regulament. De exemplu, a solicitat informații detaliate de la Microsoft în legătură cu chatbot-ul Bing Copilot, analizând riscurile legate de manipularea automată a informației politice. De asemenea, Meta a

fost investigată pentru lipsa de acțiune în fața campaniilor de dezinformare politică, iar TikTok a fost vizată pentru insuficiența măsurilor de protecție a minorilor și pentru lipsa de transparență în raport cu conținuturile sponsorizate.

Regulamentul funcționează și în sinergie cu alte inițiative europene, cum ar fi Codul de bune practici privind dezinformarea – revizuit în 2022 – sau Planul de Acțiune pentru Democrația Europeană. Totodată, DSA este completat de Legea privind Inteligența Artificială (AI Act), care urmează să intre în vigoare în 2025 și care va introduce standarde obligatorii privind utilizarea sistemelor AI cu impact social major, inclusiv obligativitatea etichetării conținuturilor generate de inteligență artificială.

În ansamblu, *Digital Services Act* reprezintă un pas decisiv către o reglementare responsabilă și modernă a spațiului digital european, care stabilește un nou echilibru între libertatea de exprimare și responsabilitatea digitală, între inovație și protejarea democrației. DSA nu are ca scop cenzura sau controlul ideologic al internetului, ci introduce un cadru de funcționare corect și transparent pentru toți actorii implicați – de la giganții tehnologici până la utilizatorii obișnuiți. El recunoaște că în era digitală, regulile trebuie adaptate nu doar pentru a permite dezvoltarea tehnologică, ci și pentru a apăra valorile fundamentale ale UE: democrația, statul de drept, pluralismul și protecția cetățenilor. Astfel, într-un peisaj marcat de instabilitate geopolitică, crize suprapuse și un război informațional în plină desfășurare, DSA devine unul dintre cele mai importante instrumente de apărare a integrității spațiului public european. Prin responsabilizarea platformelor, creșterea transparenței și consolidarea rezilienței digitale, UE își asumă un rol de lider în lupta pentru un internet sigur, echitabil și democratic – o bătălie esențială pentru viitorul ordinii liberale globale.

În completarea cadrului legislativ oferit de Digital Services Act, UE a dezvoltat și un instrument flexibil, adaptabil și colaborativ: Codul de bune practici privind dezinformarea, un set de angajamente voluntare, dar strategice, asumate de platformele digitale, industria publicității și alți actori relevanți din ecosistemul online. Inițiat în anul 2018, Codul s-a născut din nevoia de a răspunde rapid și coordonat la pericolul dezinformării, fără a aștepta finalizarea unor procese legislative de lungă durată. A fost conceput ca un mecanism de autoreglementare, dar cu o importanță tot mai mare în peisajul european al guvernanței digitale, mai ales în contextul intensificării campaniilor de manipulare informațională.[8]

Prima versiune a Codului a fost semnată de 16 actori majori – inclusiv platforme precum Facebook, Google, Twitter, Mozilla și Microsoft – și a inclus 21 de angajamente menite să sporească transparența publicității politice, să limiteze monetizarea dezinformării, să consolideze integritatea serviciilor digitale și să ofere sprijin cercetătorilor și *fact-checkerilor*. Codul a introdus o abordare inovatoare prin care

industria digitală își asuma, în mod formal, o serie de responsabilități în prevenirea și combaterea dezinformării. Deși voluntar, Codul a fost primul pas semnificativ către recunoașterea rolului esențial pe care îl joacă platformele online în conturarea opiniilor publice și în susținerea unui spațiu informațional sănătos.

Crizele succesive care au urmat – în special pandemia COVID-19 și războiul declanșat de Rusia împotriva Ucrainei – au demonstrat că autoreglementarea nu este suficientă. Campaniile de dezinformare medicală privind vaccinurile, teoriile conspirației care puneau în pericol sănătatea publică, dar și propaganda agresivă pro-Kremlin, distribuită masiv în mediul digital, au scos la iveală limitele Codului în forma sa inițială. Astfel, în 2021, în cadrul Planului de acțiune pentru democrația europeană, Comisia Europeană a formulat orientări clare pentru consolidarea Codului, cerând o extindere semnificativă a angajamentelor și a responsabilităților asumate de semnatari.[9]

Rezultatul acestor consultări a fost lansarea, în iunie 2022, a Codului de bune practici consolidat, care marchează o tranziție de la autoreglementare la un model de coreglementare, în strânsă legătură cu cerințele DSA pentru platformele online foarte mari. Numărul semnatarilor aproape s-a dublat, ajungând la 34, iar noul cadru cuprinde 44 de angajamente și 127 de măsuri specifice, mult mai bine definite, monitorizabile și aplicabile în practică. Printre cele mai importante inovații se numără măsuri ferme de demonetizare a dezinformării, pentru a bloca sursele de venit ale celor care promovează conținut manipulator. Totodată, Codul consolidat introduce cerințe mai clare privind transparența publicității politice și tematice, esențiale într-un context electoral din ce în ce mai vulnerabil la influențe externe. A fost extinsă capacitatea utilizatorilor de a detecta și semnala conținut înșelător, au fost dezvoltate instrumente pentru creșterea acoperirii verificării veridicității informațiilor în toate limbile UE, iar cercetătorii au primit acces mai amplu la datele relevante ale platformelor, un pas crucial pentru înțelegerea fenomenelor de viralizare a falsurilor.

Un element notabil al noilor arhitecturi instituționale este *Centrul de transparență*, o platformă online unde experții pot consulta date despre politicile și rezultatele implementării Codului de către fiecare semnatar (mecanisme interne de monitorizare). În paralel, a fost creat un grup operativ permanent, însărcinat cu actualizarea periodică a Codului și adaptarea sa la noile forme de manipulare emergente – cum ar fi conținuturile generate prin inteligență artificială sau tacticile coordonate de *micro-targeting*.[10]

Implementarea Codului a produs deja efecte vizibile. În timpul pandemiei, platformele au fost obligate să transmită lunar rapoarte Comisiei Europene, detaliind măsurile luate pentru a promova informațiile oficiale, pentru a combate afirmațiile false și pentru a preveni răspândirea de conținut dăunător. Aceste schimburi au con-

tribuit la o mai bună înțelegere a dinamicii platformelor și la o cooperare crescută între autorități și industrie. Mai mult, Codul a devenit o referință internațională pentru guvernele și organizațiile care caută să responsabilizeze mediul digital fără a recurge la cenzură sau supracontrol. Într-un sondaj realizat la nivelul Uniunii Europene, 83% dintre cetățeni consideră că dezinformarea amenință democrația, iar 51% afirmă că au fost expuși la informații false online. Tinerii europeni, în proporție de peste 60%, declară că întâlnesc știri false de mai multe ori pe săptămână. În acest context, un instrument precum Codul de bune practici nu mai este opțional, ci o necesitate pentru menținerea unei societăți informate, reziliente și capabile să distingă între fapte și manipulări.[11] Codul nu acționează izolat. El face parte dintr-un ecosistem instituțional și normativ mai larg, care include Planul de Acțiune pentru Democrația Europeană, DSA, rapoartele FIMI, sistemul de alertă rapidă și rețelele precum EDMO sau EUvsDisinfo. Toate aceste instrumente funcționează în complementaritate, consolidând apărarea Europei împotriva unei amenințări care evoluează constant.

Într-o lume în care informația este atât armă, cât și vulnerabilitate, UE a demonstrat că poate răspunde la amenințările hibride ale secolului XXI cu o combinație de fermitate și inovație. Dezinformarea, odată considerată doar un zgomot de fond al spațiului digital, s-a transformat într-un instrument sofisticat de destabilizare, capabil să erodeze democrația, să polarizeze societățile și să subvertească procesele electorale. Totuși, așa cum evidențiază acest raport, UE nu a rămas pasivă. Prin mecanisme precum Sistemul de Alertă Rapidă (RAS), Digital Services Act (DSA), sau Codul de bune practici, ea a construit un ecosistem de apărare multidimensional – unul care nu doar expune manipularea, ci și educă cetățenii, responsabilizează platformele și sancționează actorii răuvoitori.

Cheia succesului europene a fost abordarea proactivă. Nu este suficient să identificăm campaniile de dezinformare; trebuie să anticipăm tacticile lor. Aici intervin rapoartele FIMI și colaborarea cu NATO sau G7, care transformă datele în acțiune. Exemplul Portal Kombat dovedește că UE poate dezmembra rețele întregi de propagandă, dar și că lupta este un maraton, nu un sprint. Inteligența artificială, deși un amplificator al riscurilor, poate deveni și un aliat – prin detectarea *deepfake*-urilor sau analiza algoritmică a tendințelor manipulatoare [3].

Concluzii. Analiza prezentată confirmă faptul că fenomenul dezinformării, amplificat de progresele tehnologice și de dinamica geopolitică actuală, reprezintă o amenințare strategică la adresa securității informaționale, a coeziunii sociale și a stabilității democratice a UE. Studiile de caz, precum rețeaua „Portal Kombat”, demonstrează modul în care infrastructuri digitale coordonate pot exploata vulnerabilitățile spațiului informațional european, vizând atât opinia publică, cât

și procesele politice și instituționale fundamentale. UE a răspuns acestei provocări printr-o abordare integrată și multidimensională, combinând instrumente legislative (Digital Services Act), mecanisme operaționale (Sistemul de Alertă Rapidă – RAS), cadre de autoreglementare și coreglementare (Codul consolidat de bune practici privind dezinformarea) și infrastructuri specializate de monitorizare și analiză (EUvsDisinfo, rapoartele FIMI). Această arhitectură instituțională nu doar expune campaniile de manipulare, ci și consolidează reziliența democratică prin educație media, cooperare transnațională și sancționarea actorilor implicați în interferențe informaționale străine.

Totuși, complexitatea și adaptabilitatea tacticilor de dezinformare, în special prin utilizarea inteligenței artificiale generative, impun o permanentă actualizare a cadrului normativ, a capabilităților tehnice și a competențelor instituționale. Provocarea majoră rămâne menținerea echilibrului între protejarea libertății de exprimare și garantarea integrității spațiului public digital, într-un context în care viteza de propagare a informațiilor false depășește adesea capacitatea de reacție a autorităților. Drept urmare, apărarea spațiului informațional european nu poate fi tratată ca o intervenție punctuală, ci ca un proces continuu, adaptiv și colaborativ, fundamentat pe inovație, transparență și responsabilitate. Consolidarea rezilienței democratice în fața manipulării informaționale nu este doar o prioritate politică, ci o condiție esențială pentru viabilitatea pe termen lung a proiectului european, pentru protecția cetățenilor săi și pentru menținerea unei ordini internaționale bazate pe norme și valori comune.

Referințe bibliografice

1. Svetlana Cebotari. Identificări Conceptual-Teoretice Ale Fenomenului „Dezinformare”. Conferinţă ştiinţifică naţională. 2024 - p.208. Disponibil:https://ibn.idsi.md/sites/default/files/imag_file/207-215_7.pdf
2. Viorica Zaharia. Dezinformarea în arsenalul acțiunilor anti-UE. Repere istorice și conceptuale. Conferinţă ştiinţifică naţională. 2024 – p.155. Disponibil:https://ibn.idsi.md/sites/default/files/imag_file/151-159_15.pdf
3. Portal Kombat. Raport Tehnic. 2024. Disponibil:https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf
4. Lorne Cook Și Kelvin Chan. AI could supercharge disinformation and disrupt EU elections, experts warn. In: Revista ApNews. Disponibil: https://apnews.com/article/eu-european-union-election-disinformation-43-b7e4017825d9d382859894b7625e7a

5. EUvsDisinfo: how to debunk over 6,500 disinformation cases in four years? Disponibil:https://www.eeas.europa.eu/eeas/euvsdisinfo-how-debunk-over-6500-disinformation-cases-four-years_en?utm_source=chatgpt.com
6. How to Detect and Analyse Identity-Based Disinformation/FIMI a Practical Guide to Conduct Open Source Investigations. Disponibil:https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-DataTeam-Osint-Guidelines-04-Digital.pdf
7. Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale). Disponibil:https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32022R2065
8. Consolidarea Codului de bune practici privind dezinformarea. Disponibil:https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/strengthened-eu-code-practice-disinformation_ro
9. Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor. Orientări ale Comisiei Europene privind consolidarea Codului de bune practici privind dezinformarea. Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52021DC0262&from=EN
10. 2022 Strengthened Code of Practice on Disinformation. Disponibil:https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation
11. Cost of living and environment are the main concerns of young people in the EU. Disponibil:https://www.europarl.europa.eu/news/it/press-room/20250210IPR26795/cost-of-living-and-environment-are-the-main-concerns-of-young-people-in-the-eu?utm_source=chatgpt.com
12. Liliana BENIUC. La communication strategique de l'Union Europeenne comme instrument de renforcement de la resilience de la Republique de Moldava dans le contexte du conflit arme en Ukraine. In: ANADISS. Discours et communication strategique en situation de crise. Responsable de numero: Mariana Șovea et Angela Grădinaru. Juillet 2025. [online]. Disponibil: https://anadiss.usv.ro/wp-content/uploads/sites/74/2025/07/I.01.-Beniuc_Liliana_corectat-CI.pdf