

III. STATELE UNIUNII EUROPENE – ÎNTRE SUVERANITATEA COGNITIVĂ ȘI SUVERANITATEA DIGITALĂ

BOGDAN-GEORGE RĂDULESCU*

Introducere

Arhitectura conceptuală a strategiei europene de combatere a dezinformării este construită pe o abordare multidimensională. Ea combină instrumente de reglementare, instituționale și societale. Documentele fondatoare care susțin această strategie includ *Planul de acțiune împotriva dezinformării* din 2018, *Codul de bune practici al UE privind dezinformarea* (2018, consolidat în 2022), *Legea privind serviciile digitale* (DSA), *Planul de acțiune pentru democrația europeană* și orientări specifice privind responsabilitatea platformelor digitale, transparența în publicitatea politică și sprijinirea jurnalismului independent. Dintr-o perspectivă istorică, evoluția strategiei Uniunii Europene privind combaterea dezinformării trebuie înțeleasă în raport cu schimbările profunde ale mediului geopolitic și informațional de după 2014. Anexarea Crimeei de către Rusia și dezvăluirea întregului spectru de amenințări hibride asociate acestui moment au produs o ruptură conceptuală majoră în gândirea strategică europeană: informația a fost recunoscută nu doar ca instrument de comunicare, ci și ca vector operațional în logica războiului hibrid. În acest context, reacția Uniunii Europene a fost graduală, dar semnificativă.

* CS III dr. la Institutul de Științe Politice și Relații Internaționale „Ion I. C. Brătianu” al Academiei Române.

În 2015, Uniunea Europeană a adoptat *Planul de acțiune pentru comunicare strategică*¹ și a înființat *grupul operativ East StratCom*² în cadrul Serviciului European de Acțiune Externă (SEAE)³. Acestea au fost primele încercări instituționale de a dezvolta capacități interne de monitorizare sistematică a narațiunilor ostile, de a crește nivelul de conștientizare publică și de a formula răspunsuri adaptate amenințărilor emergente.

Aceste măsuri timpurii au fost consolidate prin *Planul de acțiune din 2018 privind dezinformarea*⁴, care a oficializat un nou cadru de cooperare între statele membre, platformele digitale și actorii media. Accentul s-a mutat treptat de la dimensiunea strict tehnică a identificării conținutului manipulator la o abordare integrată, care include dezvoltarea capacității de reacție rapidă, îmbunătățirea conștientizării situaționale și consolidarea rezilienței societale în ansamblu.

¹ Planul de acțiune al UE pentru comunicare strategică, adoptat în iunie 2015, a fost elaborat ca răspuns la creșterea campaniilor de dezinformare din vecinătatea estică, în special cele atribuite Rusiei. Planul a înființat Grupul operativ East StratCom în cadrul Serviciului European de Acțiune Externă (SEAE) pentru a coordona comunicarea strategică și a combate dezinformarea. Principalele sale obiective sunt: (1) comunicarea și promovarea eficientă a politicilor și valorilor UE față de vecinătatea estică; (2) consolidarea mediului mediatic, inclusiv sprijinirea mass-media independente și a libertății mass-media; și (3) creșterea gradului de conștientizare a publicului și îmbunătățirea capacității UE de a anticipa și de a răspunde activităților de dezinformare. Planul pune accent pe construirea de rețele între comunicatori, pe consolidarea capacităților jurnaliștilor și pe promovarea alfabetizării mediatică și a implicării societății civile, formând o bază esențială pentru abordarea UE privind reziliența informațională și mesajele externe.

² Grupul operativ East StratCom, înființat în 2015 în cadrul Serviciului European de Acțiune Externă (SEAE), este prima structură europeană dedicată contracarării dezinformării provenite în special din Federația Rusă. Mandatul său cuprinde monitorizarea narațiunilor ostile, analiza interferențelor informaționale, comunicarea strategică în vecinătatea estică și publicarea săptămânală a buletinului *Disinformation Review*. East StratCom a devenit astfel elementul central al capacității UE de a identifica timpuriu campaniile de influență malignă și de a dezvolta răspunsuri coordonate la nivel instituțional.

³ Serviciul European de Acțiune Externă (SEAE) este structura diplomatică a Uniunii Europene, creată prin Tratatul de la Lisabona, care sprijină Înalțul Reprezentant și coordonează politica externă și de securitate a UE. SEAE gestionează delegațiile UE din lume, facilitează cooperarea între statele membre și acționează ca instrument central al diplomației și acțiunii externe europene.

⁴ Planul de acțiune din 2018 privind dezinformarea – adoptat de Comisia Europeană la 5 decembrie 2018 – a reprezentat un pas decisiv în consolidarea răspunsului european la ingerințele informaționale. Documentul a stabilit patru piloni principali: (1) creșterea capacității instituțiilor europene de a detecta, analiza și contracara campaniile de dezinformare, inclusiv prin extinderea structurilor specializate precum East StratCom; (2) instituirea unui mecanism de alertă timpurie pentru schimbul rapid de informații între statele membre; (3) intensificarea cooperării cu platformele online în vederea reducerii diseminării conținutului manipulator; și (4) consolidarea rezilienței societale prin alfabetizare media, sprijinirea jurnalismului de calitate și transparențizarea ecosistemului informațional. Documentul a fost elaborat în contextul riscului sporit de interferență externă înaintea alegerilor europene din 2019 și a marcat trecerea de la o abordare reactivă la una coordonată și structurată a Uniunii Europene în domeniul securității informaționale.

Pe măsură ce se apropiau alegerile europene din 2019 – moment critic din punctul de vedere al vulnerabilității informaționale –, aceste inițiative s-au intensificat. Răspunsul Uniunii Europene s-a reconfigurat într-o direcție mai explicit securitară, cu accent pe cooperarea interinstituțională, coordonarea operațională și recunoașterea oficială a dezinformării drept o amenințare sistemică la adresa funcționării democratice.

În acest fel, Uniunea Europeană a început să instituționalizeze o paradigmă nouă, în care protejarea spațiului informațional devine un element central al arhitecturii de securitate europeană.

Strategia actuală integrează mecanisme juridice obligatorii: *Legea privind serviciile digitale (DSA)*⁵, *Legea privind inteligența artificială (AI Act)*⁶, *European Media Freedom Act (EMFA)*⁷, adaptarea continuă

⁵ Legea privind serviciile digitale (Digital Services Act-DSA) este un regulament UE de referință adoptat în 2022 și pe deplin aplicabil din 2024, care stabilește un nou cadru juridic pentru supravegherea, responsabilitatea și transparența platformelor online, a serviciilor digitale și a rețelelor sociale din întreaga Uniune Europeană. DSA impune obligații obligatorii platformelor online foarte mari (cum ar fi Meta, Google, Twitter, TikTok), obligându-le să abordeze conținutul ilegal, să protejeze drepturile utilizatorilor, să limiteze riscurile sistemice (inclusiv dezinformarea) și să furnizeze rapoarte transparente privind practicile și algoritmii de moderare. Aceasta marchează o schimbare de paradigmă în guvernarea digitală a UE prin consolidarea protecției consumatorilor, sprijinirea jurnalismului de investigație și permiterea supravegherii publice, făcând din UE pionierul mondial în reglementarea cuprinzătoare a platformelor digitale (Vezi: Maria Luisa Chiarella, Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment, *Athens Journal of Law*, Volume 9, Issue 1, January 2023, pp. 33-58).

⁶ Legea privind inteligența artificială (Legea IA) este un act legislativ inovator al Uniunii Europene, adoptat în 2025 pentru a reglementa dezvoltarea, implementarea și utilizarea sistemelor de inteligență artificială în cadrul UE. Aceasta stabilește un cadru bazat pe risc, care clasifică aplicațiile IA de la risc minim la „risc ridicat” (cum ar fi identificarea biometrică, gestionarea infrastructurilor critice sau luarea deciziilor algoritmice în domeniul sănătății și justiției). Legea impune cerințe stricte privind transparența, responsabilitatea, supravegherea umană, robustețea și guvernarea datelor, în special pentru sistemele cu risc ridicat, și interzice anumite practici precum scorarea socială sau supravegherea biometrică de la distanță în timp real în spațiile publice. Legea IA este recunoscută pe scară largă ca prima reglementare cuprinzătoare din lume a tehnologiei IA, vizând atât protejarea drepturilor fundamentale, cât și promovarea inovației, abordând în același timp preocupările exprimate de industrie cu privire la competitivitate și conformitate.

⁷ Legea europeană privind libertatea mass-media (*European Media Freedom Act – EMFA*), adoptată în 2024 și care intră în vigoare în 2025, este un regulament cuprinzător al UE, conceput pentru a proteja pluralismul, independența și transparența mass-media în întreaga Uniune Europeană. EMFA stabilește protecții solide pentru libertatea editorială, interzice interferența nejustificată a statului, impune o proprietate transparentă asupra mass-media și asigură o alocare echitabilă a publicității publice. Aceasta oferă garanții juridice pentru jurnaliști și denunțatori, introduce garanții împotriva supravegherii și capturării mass-media și obligă platformele online foarte mari să respecte conținutul mass-media și autonomia editorială. EMFA marchează un progres istoric în politica europeană de informare, consolidând discursul democratic deschis și dreptul la informații publice fiabile ca elemente centrale ale rezilienței democratice a UE.

a politicilor și inovarea instituțională, în special *Observatorul European al Media Digitală* (EDMO)⁸, care încurajează cercetarea, alfabetizarea media și rețelele de verificatori de fapte. Acest observator a fost creat ca o rețea paneuropeană pentru cercetare, verificarea faptelor și consolidarea capacităților împotriva dezinformării, sprijinind implementarea politicilor și implicarea societății civile.

Progresul este marcat de o trecere de la angajamente voluntare la standarde aplicabile, o concepție extinsă a amenințărilor informaționale și o colaborare transfrontalieră mai profundă. Toate aceste eforturi au culminat cu integrarea contracarării dezinformării ca element central al rezilienței democratice și al autonomiei strategice a UE.

Dezinformarea – amenințare existențială pentru UE

Uniunea Europeană a trecut de la tratarea dezinformării ca fenomen comunicațional negativ la înțelegerea sa ca risc sistemic la adresa ordinii democratice. Dezinformarea nu mai este percepută ca o simplă problemă de „conținut fals“, ci ca o formă de *agresiune cognitivă*⁹. Ea afectează autonomia decizională și capacitatea de discernământ colectiv în interiorul statelor membre ale Uniunii Europene. Prin urmare, discuția despre combaterea dezinformării nu se poate limita la politici media sau campanii educaționale, ci atinge esența suveranității statului democratic: dreptul statului de a-și proteja infrastructura cibernetică și,

⁸ Observatorul European al Media Digitală (European Digital Media Observatory – EDMO) este o structură independentă, lansată în 2020 și finanțată de Comisia Europeană, care funcționează ca un hub paneuropean pentru cercetători academici, organizații de fact-checking și experți în educație media implicați în combaterea dezinformării online. EDMO coordonează o rețea de huburi naționale și transnaționale (inclusiv pentru Bulgaria și România), care desfășoară activități de monitorizare și analiză a ecosistemului informațional digital, verificare a faptelor, dezvoltare de programe de educație media și sprijin pentru autoritățile publice în evaluarea politicilor platformelor online și a implementării Codului de bune practici privind dezinformarea.

⁹ În studiile de securitate recente despre războiul cognitiv, noțiunea de „agresiunea cognitivă“ este abordată într-un sens mai normativ pentru a descrie acțiuni ostile deliberate care vizează degradarea sau manipularea proceselor cognitive ale indivizilor și societăților (de exemplu, prin operațiuni informaționale sistematice, manipulare psihologică sau instrumente de război informațional), mai degrabă decât simpla influențare a ceea ce gândesc oamenii. Agresiunea cognitivă este o agresiune intenționată, planificată și orientată spre un scop, utilizată ca mijloc calculat pentru a obține un anumit beneficiu (de exemplu, putere, avantaj strategic), mai degrabă decât o reacție impulsivă determinată de o emoție acută (vezi: Ireland, J. L., & Adams, C. (2015). „Implicit cognitive aggression among young male prisoners: Association with dispositional and current aggression“, *International Journal of Law and Psychiatry*, 41, 52-59).

totodată, integritatea proceselor cognitive publice. În plan filosofico-politic, se conturează noțiunea de *suveranitate cognitivă*¹⁰, înrudită cu ideea kantiană de „autonomie a rațiunii publice“ și cu principiul habermasian al deliberării libere. Suveranitatea cognitivă definește capacitatea unei comunități de a genera judecăți autonome, nealterate de interferențe algoritmice, propagandistice sau neuropsihologice.

Conceptul de *suveranitate cognitivă*, introdus de Ulrich Beck în 1986 în lucrarea „Risikogesellschaft“ (tr. rom. „Societatea riscului“), a apărut ca rezultat al unei analize sociologice a modului în care modernitatea avansată produce și distribuie riscul în forme noi și complexe. Beck conceptualizează tranziția de la „societatea industrială“ la „societatea riscului“ ca fiind una în care incertitudinile fabricate – cum ar fi pericolele de mediu, accidentele tehnologice și crizele sistemice – produc atât o fragmentare a structurilor sociale, cât și o intensificare a reflexivității individuale. În centrul acestui cadru se află ideea că indivizii trebuie să dezvolte o capacitate sporită de suveranitate cognitivă: abilitatea autonomă de a înțelege, evalua și negocia riscurile în medii din ce în ce mai imprevizibile. Pentru Beck cunoștințele științifice autoritare și managementul instituțional nu mai pot garanta securitatea. În schimb, indivizii sunt obligați să adopte o poziție activă și reflexivă față de necunoscutele care pătrund în viața de zi cu zi.

Acest concept de suveranitate cognitivă se extinde dincolo de simpla autonomie cognitivă. În viziunea lui Beck, indivizii – în loc să se supună pur și simplu directivelor statului sau ale experților – trebuie să se implice critic și responsabil în gestionarea informațiilor, a incertitudinii și a dilemelor etice. Astfel, suveranitatea cognitivă este indispensabilă pentru dezvoltarea competențelor necesare pentru a naviga prin

¹⁰ Conceptul de „suveranitate cognitivă“ este atribuit în literatura academică sociologului german Ulrich Beck, care a inventat pentru prima dată termenul în lucrarea sa fundamentală „Risikogesellschaft“ (Societatea Riscului) în 1986. Beck a folosit termenul pentru a articula nevoia umană fundamentală de a înțelege și modela propria cunoaștere și mediul înconjurător, încadrând-o ca o problemă centrală în transformările sociale determinate de risc, tehnologie și informație în societatea contemporană. Cercetătorii ulteriori au extins conceptul, în special în dezbaterile despre tehnologia digitală, neuroetica și inteligența artificială, unde suveranitatea cognitivă semnifică acum apărarea gândirii autonome și a integrității mentale în era digitală (vezi: Ulrich Beck, *Risk society: Towards a new modernity*, Sage Publications, London, 1992; Lee A. Bygrave, Machine Learning, „Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions“, în Marcello Ienca, Effy Vayena, and Oliver W. Lembecke (Eds.), *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights*, Cambridge University Press, 2022; Robert Atkinson, „Cognitive Sovereignty and Neurocomputational Harm in Predictive Digital Platforms“, *Ethics and Information Technology*, vol. 27, no. 4, 2025).

provocările modernității – un imperativ epistemologic și moral pentru indivizii care se confruntă cu globalizarea, imprevizibilitatea și politizarea riscului.

Dezinformarea, așa cum este propagată prin campanii externe coordonate – în special războiul informațional hibrid al Rusiei împotriva statelor Uniunii Europene – reprezintă o amenințare directă la adresa suveranității cognitive. Campaniile sistematice de dezinformare subminează capacitatea indivizilor de gândire autonomă și critică. Strategia Rusiei valorifică operațiunile psihologice, platformele digitale și ingineria socială pentru a distorsiona percepțiile, a amplifica polarizarea și a manipula atât emoțiile colective, cât și cadrele interpretative din cadrul societăților vizate. Această erodare a suveranității cognitive se manifestă prin capacitatea diminuată a cetățenilor de a evalua independent realitatea și de a distinge faptele de narațiuni inventate sau de minciuni mediatice. Diminuarea capacității cognitive a cetățenilor europeni de a face o netă diferență între realitatea faptelor și interpretarea lor intenționat distorsionată are ca efect slăbirea încrederii în instituțiile democratice și împiedică participarea democratică rațională. Prin urmare, protejarea suveranității cognitive în Uniunea Europeană necesită măsuri sistematice de apărare care să sporească reziliența și conștientizarea publicului. Primul pas ar fi ca statele membre să integreze evaluările amenințărilor cognitive în politica de securitate; apoi, să investească în educație și instrumente tehnologice pentru a contracara tacticile de dezinformare din ce în ce mai sofisticate utilizate de actorii ostili.

Este demn de remarcat că, începând cu 2014, la nivelul Uniunii Europene, dezinformarea nu mai este percepută ca un eveniment accidental sau episodic, cu impact limitat asupra anumitor segmente ale populației sau anumitor instituții comunitare. Dimpotrivă, liderii de la Bruxelles au început să recunoască caracterul sistemic al fenomenului, înțeles ca o strategie deliberată de subminare a coeziunii interne, a legitimității instituțiilor și a procesului decizional european. Această schimbare de percepție a culminat cu articularea, în discursul politic oficial, a dezinformării ca o *amenințare existențială* la adresa valorilor și securității întregului bloc comunitar. În acest context, instituțiile europene au inițiat un proces de securitzare colectivă a spațiului informațional, care s-a concretizat prin politici de guvernare digitală, reglementare a platformelor și contra-propagandă instituționalizată.

*Rolul Școlii de la Copenhaga în analiza
strategiei UE de combatere a dezinformării*

Definirea dezinformării ca o *amenințare existențială* la adresa valorilor și securității Uniunii Europene în ansamblul său a fost posibilă printr-un recurs al celor care configurează politicile publice comunitare la două teorii-cadru din teoria relațiilor internaționale privind asigurarea securității statelor. Prima a fost *teoria securitizării* elaborată de Școala de la Copenhaga (Buzan, Wæver, de Wilde)¹¹. Această teorie oferă cadrul conceptual prin care poate fi înțeleasă transformarea discursivă despre dezinformare dintr-o simplă observație asupra unui fenomen care ține de patologia comunicării (fake news, dezinformare) într-o amenințare existențială la adresa securității europene.

În formularea sa originară, teoria Școlii de la Copenhaga postulează că o problemă devine una de securitate nu prin natura ei obiectivă, ci prin actul discursiv al unor actori de securizare (elite politice și instituționale). Acestea reușesc să convingă o audiență asupra urgenței și gravității amenințării. Această perspectivă – adesea criticată drept „elitistă” – presupune o relație asimetrică, „de sus în jos”, între elitele statale și public. Mai precis: această teorie nu explică *ce este* securitatea în sine, ci cum un actor politic (în acest caz, Uniunea Europeană) reușește să transforme o problemă oarecare într-o problemă de securitate. Această transformare justifică și măsuri excepționale, dincolo de regulile normale ale politicii.

A doua teorie care a fundamentat demersurile normative ale Uniunii Europene privind combaterea dezinformării la nivel comunitar a fost cea a Școlii de Securitate de la Paris (Thierry Balzacq, Didier Bigo,

¹¹ Școala de la Copenhaga, fondată de Barry Buzan, Ole Wæver și Jaap de Wilde, este o abordare teoretică majoră în studiile de securitate, cunoscută în principal pentru dezvoltarea conceptului de securitizare. Aceasta susține că problemele de securitate nu sunt date, ci sunt puse în aplicare discursiv, în special prin „acte de vorbire” care prezintă subiectele ca amenințări existențiale care necesită măsuri excepționale și le ridică deasupra politicii normale. Lucrările centrale largesc, de asemenea, agenda de securitate pentru a include sectoare dincolo de cel militar – cum ar fi securitatea societală, de mediu, economică și politică –, subliniind interacțiunea dintre constructele sociale și relațiile internaționale (vezi: Barry Buzan, *People, States and Fear: The National Security Problem in International Relations*, Harvester Wheatsheaf, 1983; Barry Buzan, Ole Wæver, Jaap de Wilde, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, 1998; Ole Wæver, „Securitization and Desecuritization”, în Ronnie D. Lipschutz (Ed.), *On Security*, Columbia University Press, 1995; Barry Buzan, Ole Wæver, *Regions and Powers: The Structure of International Security*, Cambridge University Press, 2003).

Jef Huysmans, Michael Williams)¹², care, la nivel academic, în domeniul relațiilor internaționale, a reprezentat o dezvoltare critică față de teoria Școlii de la Copenhaga și, în esență, o completare a ei.

În teoria Școlii de la Paris accentul cade pe cum se traduce definirea clară a amenințării existențiale pentru securitatea statului/statelor în practicile instituționale, în aplicarea pragmatică a dispozitivelor de control, a tehnologiilor de securitate și a raporturilor de putere prin care măsurile de securitate sunt implementate. Dacă Școala de la Copenhaga postula că securitatea se „produce” prin discursul unui actor politic care enunță o amenințare, teoreticienii Școlii de la Paris observă că nu doar discursul elitei politice securitizează, ci și practicile, normele, infrastructurile, tehnologiile, algoritmi, bazele de date. De exemplu: sistemele de supraveghere sau rețelele de monitorizare online produc efectiv securitate dincolo de nivelul retoric al indicării amenințării existențiale. Teoria Școlii de la Paris a ajutat la legitimarea felului în care această securitizare s-a materializat prin mecanisme de guvernare digitală, infrastructuri de detecție automată, audituri algoritmice, structuri interministeriale, verificatori de fapte, centre de reziliență – adică aparate de guvernare a veridicității informaționale

În cazul Uniunii Europene, această schemă este extinsă prin concepțiile de „securitizare colectivă” și „interacțiune recursivă”, care descriu modul în care instituțiile UE și statele membre construiesc discursul de securitate. *Securitizarea colectivă*, în sensul formulat de James Sperling și Mark Webber (2019)¹³, desemnează procesul prin care un grup de actori

¹² Școala de Studii de Securitate de la Paris – reprezentată de teoreticieni precum Thierry Balzacq, Didier Bigo, Jef Huysmans și Michael C. Williams – se concentrează pe fundamentele sociologice și constructiviste ale securității. Această abordare evidențiază practicile cotidiene ale profesioniștilor din domeniul securității, gestionarea (in)securității și producerea de securitate ca parte normalizată, rutinizată a guvernării. Școala de la Paris critică noțiunile tradiționale și cele ale Școlii de la Copenhaga despre securitizare, subliniind importanța rețelelor de securitate transnaționale, a guvernamentalității și a interacțiunii dintre politica de securitate internă și externă. (vezi: Thierry Balzacq, *Securitization Theory: How Security Problems Emerge and Dissolve*, Routledge, 2010; Jef Huysmans, *The Politics of Insecurity: Fear, Migration and Asylum in the EU*, Routledge, 2006; Didier Bigo and Elspeth Guild (Eds.), *Controlling Frontiers: Free Movement Into and Within Europe*, Routledge, 2005).

¹³ Vezi: James Sperling, Mark Webber, „The European Union: Security Governance and Collective Securitisation”, in Sonia Lucarelli, James Sperling, Mark Webber (Eds.), *Collective Securitisation and Security Governance in the European Union*, Abingdon, Routledge, 2019; James Sperling, Mark Webber, „NATO and the Ukraine Crisis: Collective Securitisation”, *European Journal of International Security*, 2017; Mark Webber, James Sperling, „The collective securitization of climate change: Implications for EU governance”, *Review of International Studies*, 2025.

politici – de pildă statele membre ale UE sau NATO – identifică, formulează și gestionează în mod comun amenințările la adresa securității.

Acest lucru se realizează printr-un discurs coordonat și prin acțiuni politice convergente, nu prin răspunsuri unilaterale ale statelor. Abordarea se distanțează astfel de modelele clasice de securitzare, centrate pe exclusivitatea competențelor unui pe stat, și pune accentul pe mecanismele de mobilizare instituționalizată prin care organizațiile internaționale elaborează narațiuni comune despre risc și generează rezultate orientate spre protecție și stabilitate.

Un element central al acestui model este interacțiunea recursivă: un schimb continuu și dinamic între actorul securitizant (de exemplu, o organizație internațională) și publicul său – fie statele membre, fie publicul larg. În această logică, securitzarea nu este produsul unui act unilateral de discurs, ci rezultatul unei negocieri intersubiective constante, prin care atât organizația, cât și audiența contribuie la definirea și validarea amenințării.

Sperling și Webber subliniază că securitzarea colectivă este caracterizată de negocieri multiple pe niveluri diferite, de proceduri legislative complexe și de dialoguri recurente între actorii implicați. Toate acestea contribuie la instituționalizarea unor noi politici de securitate în contexte de guvernare transnațională, unde procesul decizional este împărțit, stratificat și profund interdependent.

Pornind de la acest cadru teoretic, strategia Uniunii Europene de combatere a dezinformării – concretizată prin *East StratCom Task Force*¹⁴, *Planul de acțiune împotriva dezinformării* (2018)¹⁵ și *Digital Services Act* (2022) – reprezintă un proces de securitzare supranațională a informației.

¹⁴ *East StratCom Task Force* este o echipă operativă înființată în 2015 de către Serviciul European pentru Acțiune Externă, dedicată identificării, analizării și contracarării campaniilor de dezinformare coordonate, în principal în spațiul estic al Uniunii Europene. Aceasta monitorizează și contracarează dezinformarea promovată în special de actori străini, precum Federația Rusă, având un rol esențial în consolidarea rezilienței informaționale și în protejarea suveranității cognitive a statelor membre ale UE prin instrumente precum platforma EUvsDisinfo. *East StratCom Task Force* reprezintă un pilon al strategiei UE în lupta împotriva războiului hibrid și a manipulării informaționale (Vezi: Alessia D'Andrea & all, „Policy Review: Countering Disinformation in the Digital Age – Policies and Initiatives to Safeguard Democracy in Europe“, *Information Polity*, Volume 30, Issue 1, 2025, Pages 82-91, <https://doi.org/10.1177/15701255251318900>).

¹⁵ *Planul de acțiune împotriva dezinformării* (2018) al Uniunii Europene reprezintă o strategie cuprinzătoare care vizează consolidarea rezilienței democrațiilor europene prin prevenirea, detectarea și combaterea diseminării deliberate a știrilor false și a manipulării informației. Planul include măsuri de autoreglementare a platformelor digitale, susținerea mass-mediei independente

Aceasta redefinesc sfera publică europeană, legitimând măsuri excepționale (precum interzicerea posturilor *Russia Today* și *Sputnik*)¹⁶ și marcând o cotitură geopolitică în guvernanta informațională, unde discursul securitar devine instrumentul central al protejării ordinii liberale europene.

Recunoașterea de către Uniunea Europeană a faptului că *dezinformarea este parte a războiului hibrid* a însemnat o evoluție a cadrului normativ comunitar. Factorul geopolitic catalizator al acestei evoluții l-a reprezentat anexarea ilegală a Peninsulei Crimeea de către Federația Rusă în 2014 și conștientizarea că asupra statelor membre ale spațiului comunitar a fost declanșat un război hibrid de proporții din partea regimului lui Vladimir Putin. Ulterior, până la războiul de agresiune împotriva Ucrainei în februarie 2022, Uniunea Europeană a fost ținta unor campanii de dezinformare ale Federației Ruse pe timpul pandemiei de COVID-19 din 2020. Cu ocazia crizei în domeniul sănătății publice generată de pandemia de COVID-19, autoritățile de la Bruxelles au constatat că dezinformarea rusească a început să devină sistemică și să ridice problema unei amenințări existențiale. În Uniunea Europeană, dezinformarea online cu privire la măsurile preventive și campaniile de vaccinare împotriva COVID-19 a subminat încrederea cetățenilor din statele membre în răspunsul guvernamental la această chestiune de sănătate publică și a provocat daune în lumea reală. Un studiu efectuat între ianuarie și februarie 2021 în state membre importante ale Uniunii Europene (Franța, Germania, Italia și Spania) de către *Global Disinformation Index* (GDI), organizație britanică nonprofit care și-a propus să identifice, să blocheze finanțarea și să obțină desființarea

și promovarea alfabetizării media, marcând o abordare coordonată între statele membre și instituțiile UE pentru protejarea spațiului democratic și a încrederii publice (Vezi: Ethan Shattock, „Self-regulation 2.0: A critical reflection of the European fight against disinformation“, *Misinformation Review*, 2(3), pp. 1-8, Harvard Kennedy School, 2021, <https://doi.org/10.37016/mr-2020-73>).

¹⁶ Uniunea Europeană a interzis oficial difuzarea și diseminarea de conținut de către canalele media rusești *Russia Today* (RT) și *Sputnik*, inclusiv toate versiunile lingvistice și filialele, în martie 2022, ca răspuns la agresiunea rusă împotriva Ucrainei și la campaniile coordonate de dezinformare care vizau UE. Temeiul juridic pentru această interdicție constă în Regulamentul (UE) 2022/350 al Consiliului de modificare a Regulamentului (UE) nr. 833/2014 și în Decizia (PESC) 2022/351 a Consiliului de modificare a Deciziei 2014/512/PESC. Aceste documente justifică măsurile ca fiind necesare pentru promovarea ordinii publice și a securității UE prin stoparea propagandei și a „campaniilor internaționale sistematice de manipulare și denaturare a faptelor din partea mass-media“, cu referire la articolul 29 din Tratatul UE și articolul 215 din Tratatul de Funcționare al UE. Sancțiunile rămân în vigoare până la încetarea agresiunii și dezinformării ruse împotriva Uniunii și a statelor sale membre.

acelor site-uri care răspândesc știri false și duc campanii de dezinformare, a scos în evidență faptul șocant că majoritatea companiilor de tehnologie publicitară nu au avut politici specifice privind conținutul de dezinformare privind COVID-19 și că acestea continuă să finanțeze site-uri de știri marcate public ca furnizori de dezinformare. Logica comercială și mecanismele ei publicitare au creat, de o manieră impersonală, indirectă și involuntară, platforme de susținere și supraviețuire financiară pentru acele site-uri care organizează campanii de diseminare de fake news și care, astfel, pun grav sub semnul întrebării noțiunea însăși de obiectivitate în informarea de masă.

Lovite de scăderea profiturilor lor pe timpul pandemiei de COVID-19, companiile au abandonat exigența etică în domeniul businessului online. Nevoia lor vitală de a recupera pierderile economice cauzate de pandemie au determinat anumite firme multinaționale, prezente pe teritoriul Uniunii Europene, să renunțe la orice criteriu care ține de etica afacerilor, exact într-un moment când segmente masive de populație, de categorii sociale, averse consumatoare de informații online, au fost bulversate psihologic și informațional din cauza incertitudinilor existențiale induse de pandemie. Aceste segmente sociale au fost confruntate cu campanii sistematice de dezinformare și cu retorica populismului algoritmic pe tema infectării cu noul coronavirus (SARS CoV-2).

O analiză realizată de *The Global Disinformation Index* (GDI)¹⁷ indica faptul că *piața internațională a advertisingului online* nu mai ținea cont de criterii de moralitate sau de sănătate publică. Ea folosea site-urile care distribuiau fake news din domeniul medical în chip amoral pentru promovarea produselor comerciale sau a serviciilor unor companii cu notorietate. Organizația *The Global Disinformation Index*, care a colaborat cu guvernele stelor membre ale Uniunii Europene, cu mediile de afaceri și cu societatea civilă pe baza principiilor neutralității, independenței și transparenței, a atras atenția în studiul ei că de cele mai multe ori publicitatea pentru brandurile create de mari companii au finanțat unele dintre cele mai cunoscute site-uri pentru răspândirea dezinformării în Uniunea Europeană. Analiza GDI arată că peste 76 de milioane de dolari alocați de industria de marketing pentru publicitatea în favoarea unor mărci devenite celebre (*Amazon Prime*, *Burger*

¹⁷ Global Disinformation Index, *Ad-funded COVID-19 conspiracy sites: A look at the EU*, 23 February 2021, <https://www.disinformationindex.org/blog/2021-2-23-ad-funded-covid-19-conspiracy-sites-a-look-at-the-eu/>.

King, Mercedes-Benz, Samsung, Spotify și Volvo) ajungeau să finanțeze site-uri toxice create ca să disemineze constant fake news și ca să susțină campanii agresive de dezinformare.

Google este cea mai importantă platformă de reclame online pentru aceste mărci. În același timp, tot Google plătea pentru spații publicitare online puse la dispoziție pe paginile lor de către aproape 60% dintre site-urile de dezinformare. Pentru acest serviciu, Google le oferă 62% din veniturile estimate din advertising online (48 milioane dolari anual). Poziția dominantă a companiei Google în Uniunea Europeană – la capitolul cumpărării de spațiu de reclamă online – indică ce rol negativ a avut acesta în asigurarea oxigenului financiar pentru site-urile de dezinformare la nivel global. Oferindu-le acestor site-uri șansa autofinanțării prin cumpărarea de la ele a spațiilor de reclamă, Google a devenit, în mod involuntar și nefast, principalul „sponsor“ al unor campanii de dezinformare orchestrate de grupuri de interese statale sau nonstatale.

Potrivit studiului *The Global Disinformation Index*, împreună cu Google, alte patru companii reprezintă în totalitate 97% din veniturile din reclame plătite site-urilor de dezinformare din UE: *Criteo, OpenX, Taboola* și *Xandr*. Totodată, studiul efectuat de GDI a arătat că reclamele de la mărci binecunoscute precum *Amazon Prime, American Express* și *Microsoft* au continuat să finanțeze, fără să vrea, acest conținut în principalele state membre ale Uniunii Europene. Această realitate cinică a demonstrat „absența unei politici publicitare la nivel de industrie, care să elimine dezinformarea COVID-19”¹⁸. GDI a publicat topul companiilor care au plătit, direct și indirect, site-uri rusești care au monetizat prin distribuirea de conținuturi editoriale false cu intenția clară de dezinformare.

Sugestiile lansate de GDI pentru statele membre din Uniunea Europeană se refereau la implementarea de acorduri, reglementări și coduri cu industria publicitară, astfel încât să se stipuleze clar că serviciile publicitare nu vor fi furnizate acelor site-uri al căror conținut încalcă termenii și condițiile companiilor care oferă astfel de servicii. Un astfel de protocol nu înseamnă că se încalcă libertatea de exprimare sau dreptul la opinie.

În timp ce libertatea de exprimare este protejată, acțiunea de a profita, cinic și din interes politic/geopolitic, de această libertate pentru

¹⁸ *Idem*.

a disemina intens fake news, narațiuni mincinoase și dezinformări strategice nu trebuie să fie acceptată sau protejată prin lege.

Comisia Europeană a depus eforturi în acest sens pentru a pune capăt stimulentei financiare pentru site-uri care diseminează conținuturi false și dezinformare (reclame online, plată electronică, comerț electronic și alte platforme de monetizare). Aceste măsuri s-au concretizat prin adoptarea *Actului Uniunii Europene privind serviciile digitale* (lb. engl. *European Union Digital Services Act*) și *Planului de acțiune al Uniunii Europene pentru democrație* (lb. engl. *European Union Democracy Action Plan*)¹⁹. De asemenea, blocul comunitar a actualizat între timp și *Codul de practică al Uniunii Europene privind dezinformarea* (lb. engl. *EU Code of Practice on Disinformation*)²⁰. Toate aceste documente cruciale privind implementarea unei comunicări online în spațiul comunitar au fost elaborate cu scopul de a crește gradul de conștientizare, de rezistență socială, de mobilizare a sectorului privat și a instituțiilor europene pentru a detecta mai repede și pentru a analiza în timp util procesele de dezinformare folosite ca arme împotriva democrației și a statului de drept.

Fenomenul „*monetizării continue a dezinformării*“, prin plasarea de reclamă pe site-uri angajate în diseminarea de știri false despre pandemia de COVID-19, este unul considerat extrem de îngrijorător de către Comisia Europeană. În *Codul de practică al Uniunii Europene privind dezinformarea din 2021*, oficialii de la Bruxelles constatau nemulțumiți că, „*în pofida unor acțiuni de limitare a monetizării*

¹⁹ Planul de Acțiune al Uniunii Europene pentru Democrație (European Union Democracy Action Plan) este o inițiativă strategică care urmărește consolidarea democrației și promovarea statului de drept prin susținerea participării cetățenilor, transparenței și rezilienței instituțiilor democratice în fața amenințărilor interne și externe. Acest plan cuprinde măsuri pentru combaterea dezinformării, sprijinirea societății civile și întărirea sistemelor electorale în statele membre, reflectând angajamentul UE de a proteja și dezvolta valorile democratice fundamentale într-un context geopolitic complex (Vezi: Charles Brasseur, Vera Pachta and Chiara Grigolo, „The EU’s External Democracy Action in a New Geopolitical Reality. Recommendations Report“, *International Idea*, 2023, <https://doi.org/10.31752/idea.2023.1>).

²⁰ Codul de bune practici al UE privind dezinformarea este un cadru de autoreglementare cu participarea mai multor părți interesate – lansat în 2018 și revizuit semnificativ în 2022 – care își propune să limiteze răspândirea și amplificarea dezinformării online prin angajamente axate pe demonetizare, integritatea serviciilor, capacitatea utilizatorilor, transparența publicității politice și a problemelor specifice și cooperarea în timpul alegerilor. Integrat în cadrul Legii privind serviciile digitale (DSA) în februarie 2025, Codul este recunoscut ca un cod de conduită voluntar, care impune semnatarilor (inclusiv platformelor majore, furnizorilor de publicitate și societății civile) să implementeze peste 40 de angajamente și să raporteze progresele înregistrate prin intermediul unor măsuri structurate de monitorizare și transparență, respectând în același timp drepturile fundamentale și valorile democratice ale UE.

dezinformării”, problema intoxicării ecosistemului informațional online cu fake news persistă.

Printre măsurile recomandate de Comisia Europeană pentru a stopa dezinformarea pe tema pandemiei, câteva sunt pertinente și pot fi implementate de autoritățile fiecărui stat membru al Uniunii Europene în legislații naționale sau, cel puțin, într-un set de măsuri punctuale în asemenea cazuri de criză „infodemică”: 1/ „retrogradarea și eliminarea conținuturilor care includ informații false și/sau înșelătoare”, pentru că acestea „ar putea provoca vătămări fizice sau să afecteze politicile de sănătate publică”; 2/ interzicerea activităților publicitare „care exploatează criza de sănătate”; 3/ eforturile statelor membre de a furniza „informații exacte despre vaccinuri”; 4/ difuzarea pe scară largă de rapoarte care analizează „comportamentul manipulativ” al unor distribuitori de mesaje false și „fluxurile de publicitate legate de dezinformarea COVID-19” de pe „site-urile web ale terților”²¹.

Adoptarea strategiei împotriva dezinformării – proces decizional lent

Procesul decizional lent pe care l-au parcurs liderii statelor membre ale Uniunii Europene până la acceptarea realității că dezinformarea reprezintă o amenințare existențială a fost cauzat de precauțiile în legătură cu protejarea libertății de exprimare. Această lentoare a procesului decizional reflectă tensiunea profundă dintre cultura juridico-normativă a Uniunii – întemeiată pe libertatea de exprimare, pluralismul mediatic și autonomia individuală – și noile realități geopolitice ale spațiului informațional global. În momentul în care informația este conceptualizată ca vector de atac și nu doar ca instrument de comunicare, fundamentele unei democrații liberale sunt puse la încercare.

În tradiția liberală europeană, pluralismul mediatic a fost considerat fundamentul libertății de exprimare și al sănătății democrației. *Articolul 11 din Carta Drepturilor Fundamentale a Uniunii Europene* consacră explicit principiul potrivit căruia „libertatea și pluralismul mijloacelor de informare în masă trebuie respectate”. În această paradigmă, statul avea o funcție de garant, asigurând cadrul juridic care

²¹ Vira Jourová, Thierry Breton, „Code of Practice on disinformation”, *European Commission*, 1st October 2021, <https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation>.

proteja competiția de idei, fără a interveni direct în conținutul comunicării. Această ordine normativă a fost însă profund perturbată de apariția platformelor digitale, care au dizolvat distincția clasică dintre emițător și receptor.

Modelul informațional unidirecțional – în care presa profesională difuza conținut către un public pasiv – a fost înlocuit de un model interactiv, „de tip rețea“, în care orice individ devine, simultan, generator și consumator de informație. Această democratizare aparentă a comunicării a adus o explozie haotică a opiniilor, dar și o devalorizare a criteriilor epistemice – adevărul, verificarea, autoritatea sursei. În absența unui cadru de reglementare corespunzător, spațiul digital s-a transformat într-o arenă a excesului comunicațional, unde coexistă libertatea de expresie, discursul urii, manipularea emoțională și propaganda coordonată. Ceea ce în modernitate era o piață a ideilor, în era platformelor a devenit o piață a atenției, dominată de logica algoritmică și de capitalizarea afectelor.

Libertatea de exprimare, așa cum este definită în articolul 10 al Convenției Europene a Drepturilor Omului (CEDO), este în esență un drept negativ: ea presupune o obligație de *nonintervenție* din partea statului. Această viziune liberală a libertății ca absență a constrângerii explică reticenta structurală a statelor democratice de a acționa direct împotriva dezinformării – acțiune care riscă să fie imediat percepută ca cenzură. Această tensiune constituie o capcană a democrațiilor liberale: pentru a proteja libertatea discursului, ele ezită să intervină chiar și atunci când spațiul public este invadat de conținuturi manipulative sau ostile. Aici se vede diferența fundamentală dintre regimurile autoritare – care își apără ordinea prin controlul total al comunicării – și democrațiile care trebuie să protejeze adevărul fără a interzice libertatea.

Mai mult, istoria constituțională a Europei, marcată de abuzurile cenzurii de stat (în special în cazul statelor membre care au trecut prin experiența comunistă), a generat o memorie colectivă a suspiciunii față de autoritatea publică. Statul este perceput adesea ca potențial opresiv, iar sectorul privat, inclusiv platformele digitale, ca spațiu de libertate și inovație.

Această inversare simbolică – în care statul devine „dușmanul libertății“, iar corporația devine „garantul exprimării“ – a fost exploatată strategic de marii actori tehnologici, care invocă libertatea de exprimare pentru a evita responsabilitatea. Cazul Facebook este emblematic: în timp ce Mark Zuckerberg invocă Primul Amendament al Constituției americane pentru a susține că „oamenii, nu companiile, ar

trebui să decidă ce este credibil²², aceeași companie angajase deja zeci de mii de verificatori de narațiuni online. În realitate, apelul la libertatea absolută de exprimare a individului a servit drept mecanism de evitare a reglementării și, implicit, de protejare a statu-quo-ului manipulării informaționale.

În plus, lentoarea adoptării unor măsuri de securitate care să contribuie la apărarea mediului informațional european de campanii sistematice de dezinformare din partea unor actori statali s-a produs și din cauza „absenței unei definiții convenite și a unei înțelegeri comune a problemei atât în rândul practicienilor, cât și al cercetătorilor. În timp ce cercetătorii din domeniul mass-media și al comunicării au avertizat asupra subminării liberei circulații a informației și a sferei publice, cercetătorii din discipline precum relațiile internaționale, studiile de securitate și studiile strategice tindeau să definească problema în termeni de război informațional sau război hibrid/război neliniar și aplicau un vocabular militarizat, referindu-se, de exemplu, la utilizarea informației ca armă²³.

Toate aceste ezitări inițiale la factorii de decizie ai Uniunii Europene, observate în documentele și dezbaterile europene de după 2014, au o explicație teoretică solidă: liberalismul politic care stă la baza construcției europene se bazează pe presupunerea că libertatea informației este, în sine, o garanție a raționalității publice. În schimb, introducerea noțiunii de *militarizare a informației* sau *folosirea informației ca armă* subminează această paradigmă. Sub presiunea factorului geopolitic, Uniunea Europeană s-a văzut nevoită să forțeze trecerea de la o concepție normativă a comunicării la una strategică și securitară. Dezinformarea nu mai este percepută doar ca o disfuncție a pieței informaționale, ci ca o formă deliberată de *agresiune cognitivă* îndreptată împotriva procesului democratic însuși. Această tranziție conceptuală – de la libertate la protecție – explică dilema morală și politică în care se află Uniunea: cum poți apăra libertatea fără a o restrânge?

²² Declarația lui Mark Zuckerberg conform căreia „oamenii, nu companiile, ar trebui să decidă ce este credibil” a fost formulată în mai multe intervenții publice între 2018 și 2020, în contextul dezbaterilor privind moderarea conținutului și libertatea de exprimare pe platformele digitale. În aceeași perioadă, Facebook a extins substanțial capacitatea internă și externă de moderare, angajând zeci de mii de verificatori ai conținutului. Vezi Mark Zuckerberg, *A Blueprint for Content Governance and Enforcement* (Facebook Newsroom, November 15, 2019).

²³ Charlotte Wagnsson, „What is at stake in the information sphere? Anxieties about malign information influence among ordinary Swedes”, *European Security*, Vol. 29, Issue 4, 2020, pp. 397-415, <https://doi.org/10.1080/09662839.2020.1771695>.

Pentru a-și proteja ordinea democratică, Uniunea Europeană a trecut prin dilema decizională dacă trebuie să intervină activ sau nu în spațiul informațional. Orice intervenție prea energică risca să contravină principiului libertății de exprimare. Această contradicție structurală definește paradoxul securității europene: nevoia de apărare a rațiunii publice prin mijloace care, în mod potențial, o pot vicia. În limbajul Școlii de la Copenhaga, Uniunea Europeană s-a confruntat cu o situație în care discursul securitar s-a extins asupra unei sfere normative esențiale, dar fără a dispune încă de legitimitatea deplină a publicului.

De aceea, un alt pas important în definitivarea unei strategii europene de combatere a dezinformării l-a constituit *implicarea activă a cetățenilor*. Uniunea a recunoscut că succesul oricărei politici de reziliență informațională depinde de capacitatea indivizilor de a înțelege, evalua și reacționa critic la conținuturile digitale. În acest sens, cetățenii sunt percepuți în același timp ca principalele ținte ale dezinformării și ca primii apărători ai democrației. Această dublă poziție impune consolidarea competențelor cognitive și civice necesare pentru a identifica informațiile false, pentru a evita propagarea lor și pentru a contribui la menținerea unui spațiu public bazat pe fapte și rațiune.

Pentru atingerea acestor obiective, Uniunea Europeană a dezvoltat un ansamblu de inițiative de alfabetizare mediatică și educație digitală, menite să sprijine formarea unei cetățenii informate, critice și participative. Aceste programe promovează capacitatea de analiză a surselor, recunoașterea manipulărilor emoționale și discernerea conținuturilor produse cu intenție înșelătoare. În paralel, proiecte europene de cercetare și inovare, precum *AI4Debunk*²⁴, finanțate de Comisia Europeană, urmăresc să pună la dispoziția cetățenilor instrumente de verificare a faptelor și resurse educaționale care să faciliteze o navigare conștientă în mediul digital. Obiectivul acestor inițiative este acela de a întări reziliența democratică printr-un proces de învățare colectivă și de responsabilizare civică. Rolul cetățeanului în combaterea dezinformării nu este unul pasiv, de beneficiar al protecției instituționale, ci activ, de participant direct la construirea unei culturi publice a adevărului.

²⁴ Proiectul european *AI4Debunk* reprezintă o inițiativă inovatoare care utilizează inteligența artificială pentru a combate dezinformarea prin dezvoltarea de tehnologii avansate ce detectează, clasifică și demontează știrile false. Scopul proiectului este crearea unor instrumente automate și accesibile pentru verificarea rapidă a faptelor și contracararea răspândirii informațiilor false în mediul digital, contribuind astfel la întărirea rezilienței informaționale în societățile democratice.

Consolidarea acestui rol marchează trecerea de la o abordare reactivă, centrată pe controlul conținutului, la una preventivă și participativă, bazată pe autonomia cognitivă a individului și pe consolidarea capitalului epistemic al societății democratice.

*Dezinformarea – efecte nocive
asupra proceselor politice interne*

Strategia Uniunii Europene de combatere a dezinformării a fost formulată în termenii unei probleme de securitate externă. Documentele strategice de la nivelul Consiliului și Comisiei Europene, începând cu *Action Plan Against Disinformation* (2018), definesc dezinformarea ca un instrument utilizat de actori statali și nonstatali din afara spațiului UE. O asemenea definiție reflectă percepția instituțională conform căreia principalele amenințări cognitive provin dinspre actori statali sau parastatali ostili – în special Federația Rusă și, în anumite dimensiuni, Republica Populară Chineză. Această încadrare securitară a transferat dezinformarea din sfera competiției politice interne către registrul mai larg al războiului informațional și al instrumentelor de influență strategică. Narațiunile ostile care au scopul de a produce confuzie socială și politică sunt conceptualizate ca vectori ai unui război cognitiv transnațional, un tip de agresiune hibridă ce depășește granițele clasice ale conflictului. Astfel, etichetarea acestei amenințări drept *externă* reflectă o logică geopolitică a intențiilor subversive, dar nu a impactului lor intern. Cu toate acestea, natura fenomenului obligă și la recunoașterea unei evidente dimensiuni de *securitate internă*. Dezinformarea nu acționează la nivelul frontierelor, ci al ecosistemului informațional domestic: mesajele toxice pătrund direct în spațiul digital la care sunt conectați cetățenii europeni, fake news circulă pe platforme sociale, influențează opinii, polarizează comunități și fragilizează încrederea publică în instituții. Efectul este profund endogen, afectând coeziunea socială, integritatea proceselor democratice și reziliența psihologică a corpului politic. Tocmai aici se vede tensiunea paradigmatică a actualelor politici europene: deși amenințarea este produsă de actori externi, terenul pe care acționează este în întregime intern. Din acest motiv, orice strategie eficientă trebuie să integreze simultan logica securității externe cu aceea a securității interne. Ea presupune o abordare care recunoaște caracterul hibrid al războiului informațional contemporan.

În analizele elaborate de instituțiile Uniunii Europene dezinformarea rusă și interferențele în procesele democratice au fost tratate drept o amenințare hibridă cu efecte transfrontaliere, orientată să erodeze coeziunea socială, să distorsioneze deliberarea publică și să încetinească sau să blocheze capacitatea decizională a statelor membre. În această cheie, „amenințările hibride“ desemnează seturi sincronizate de acțiuni civile și militare – de la campanii de dezinformare și operațiuni cibernetice până la infiltrarea de agenți de influență, presiuni asupra mass-media independente și achiziția de infrastructuri critice – dificil de descurajat, atribuit și sancționat din cauza ambiguității și caracterului lor clandestin.

Un raport elaborat de Serviciul European de Acțiune Externă (SEAE) în 2024 indică faptul că: „De la publicarea primului Raport al SEAE privind amenințările de manipulare și interferență informațională străină (FIMI), în februarie 2023, actorii externi au continuat încercările intenționate, strategice și coordonate de a manipula faptele, de a crea confuzie și de a semăna dezbinare, teamă și ură. Cel mai evident exemplu este Rusia, care încearcă să-și justifice războiul de agresiune împotriva Ucrainei”²⁵. Potrivit investigațiilor făcute de serviciile specializate ale Serviciului European de Acțiune Externă, pe durata agresiunii rusești asupra Ucrainei peste 4.000 de canale au fost active de 9.800 de ori în 750 de incidente investigate. Canalele erau site-uri web sau profiluri de socializare, grupuri și pagini. Platformele cel mai des implicate au fost *Telegram* și *X* (fostul Twitter). Din punct de vedere operațional, evaluările europene arată că actorii ruși exploatează deliberat libertățile care definesc democrațiile europene (libertatea de exprimare, a presei și deschiderea piețelor) pentru a activa clivaje preexistente și a introduce forme de manipulare care împing dezacordurile legitime de opinii către polarizare și neîncredere generalizată. Trecerea de la canale oficiale (Russia Today, Sputnik) la ecosisteme de proxy și parteneri ai Rusiei, completată de ferme de troli, boți și conținut generat/alterat tehnologic, a mărit atât puterea rusească de penetrare în mentalul colectiv al statelor membre ale UE, cât și costurile detectării *post factum* de către instituțiile europene a acestor tipuri de operațiuni de coordonate de Kremlin.

²⁵ The European External Action Service (EEAS), 2nd EEAS Report on Foreign Information Manipulation and Interference Threats. A Framework for Networked Defence, January 23th, 2024, 2nd EEAS Report on Foreign Information Manipulation and Interference Threats | EEAS.

Pe linia exemplificărilor empirice, UE și statele membre au semnalat interferențe și tentative de manipulare în mai multe scrutine europene recente. În Franța, alegerile prezidențiale din 2017 au fost ținta unor scurgeri coordonate („MacronLeaks“), atacuri cibernetice și campanii de dezinformare, neutralizate parțial prin reacție rapidă instituțională și cooperare public-privat. În spațiul UE, alegerile pentru Parlamentul European din 2019 au determinat adoptarea și consolidarea unui set de măsuri de protecție (planul de acțiune contra dezinformării, cooperare în rețea, alerte timpurii), pe fondul riscului de interferență străină. În Slovacia, ciclul electoral 2023–2024 a fost marcat de utilizarea în campanie a conținutului audio/video falsificat (deepfake) și a rețelelor de dezinformare, semnalate în mod repetat de structuri europene specializate. Pentru diverse cicluri electorale în statele membre în 2024 (locale, naționale, europene), instituțiile UE au avertizat asupra operațiunilor rusești de influențare (inclusiv rețele media-proxy de tip „Voice of Europe“), ceea ce a condus la rezoluții ale Parlamentului European și la investigații serioase. Primele documente europene de după 2015 indică o percepție clară a fenomenului ca fiind o amenințare venită din afara Uniunii, mai ales dinspre Federația Rusă.

Consiliul European, în concluziile sale din martie 2015 – la un an după anexarea Crimeei –, a menționat explicit „necesitatea de a combate campaniile de dezinformare ale Rusiei“ și a solicitat pregătirea unui plan de acțiune pentru comunicarea strategică. Această încadrare inițială a dezinformării în logica războiului hibrid a avut consecințe structurale asupra arhitecturii instituționale europene. Definind amenințarea ca fiind externă, Uniunea a plasat răspunderea în sfera politicii externe și de securitate comună, sub egida Serviciului European de Acțiune Externă. În logica teoriei securitizării, aceasta marchează momentul discursiv al „declanșării excepționalității“: o problemă socială (dezinformarea) este convertită într-o chestiune de apărare, gestionată de instituțiile cu competență în crize.

Momentul deciziei la nivel comunitar a survenit când autoritățile de la Bruxelles au constatat că, în mod sistematic, „caracterul netransparent al social media a fost exploatat în mod repetat și de «fermele de troli» sprijinite de Rusia, inclusiv notoria «Internet Research Agency». Aceste organizații susținute de Kremlin au derulat campanii extinse cu troli și boți și au creat mii de conturi false, nu doar pe rețelele sociale, ci și pe platforme de discuții, forumuri media online și servicii de streaming

video, urmărind polarizarea dezbatelor și promovarea narațiunilor anti-occidentale²⁶.

Această decizie a permis Uniunii să-și dezvolte capacitatea de reacție strategică la campaniile de influență externe, legitimizând instrumente precum *East StratCom Task Force* și platforma *EUvsDisinfo*²⁷.

Internet Research Agency (Agenția de Cercetare pe Internet) este o „fermă de trol” rusească cu sediul în Sankt Petersburg, care operează ca o entitate aliniată Kremlinului, producând și diseminând sistematic dezinformare și propagandă prin intermediul unor conturi false de pe principalele platforme de socializare. Identificată de investigațiile americane și europene ca parte a setului mai larg de instrumente al Federației Ruse pentru războiul hibrid, Internet Research Agency s-a angajat în campanii online coordonate care vizează alegerile, dezbatările de sănătate publică și problemele de politică externă, inclusiv operațiuni susținute împotriva statelor membre și instituțiilor UE.

În contextul strategiei UE de combatere a dezinformării rusești, Internet Research Agency este frecvent citată²⁸ ca un exemplu paradigmatic de manipulare și interferență organizată în procesele electorale și politice din interiorul spațiului comunitar.

²⁶ Sandra Kalniete & Tomass Pildegoviēs, „Strengthening the EU’s resilience to hybrid threats“, *European View*, Vol. 20, Issue 1, pp. 23-33, 2021, DOI: 10.1177/17816858211004648 journals.sagepub.com/home/euv.

²⁷ Platforma *EUvsDisinfo* este o inițiativă a Uniunii Europene dedicată identificării și analizei dezinformării coordonate și sponsorizate de Kremlin. *EUvsDisinfo* dezvăluie cu regularitate mecanismele acestor dezinformări care vizează destabilizarea coeziunii sociale și a democrației în statele membre. Mandatul *EUvsDisinfo* constă demontarea acestor dezinformări prin verificări ale experților în comunicare și prin publicarea investigațiilor lor, contribuind la creșterea rezilienței informaționale a statelor membre și la protejarea suveranității cognitive europene într-un context de amenințări hibride complexe (Vezi: Bruns, A., & Burgess, J. (2022), „Truth in Fake News: How Disinformation Laws Are Reframing the Concepts of Truth and Accuracy on Digital Platforms“, *Information, Communication & Society*, 25(10), 1350-1366. <https://doi.org/10.1080/1369118X.2022.2107635>; Shao, C., Ciampaglia, G. L., & Menczer, F. (2024), „EUvsDisinfo: A Dataset for Multilingual Detection of Pro-Kremlin Disinformation“, *News Articles*. arXiv, <https://arxiv.org/abs/2408.00000>).

²⁸ Referințe: Yochai Benkler, Robert Faris, and Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, Oxford University Press, 2018; Darren L. Linvill, Patrick L. Warren, „Troll Factories: How Russian Influence Operations Work and Their Impact on Social Media Discourse“, *Political Communication*, 37(2), 2020; United States Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Volume 2: Russia’s Use of Social Media, U.S. Government Publishing Office, 2019; European External Action Service (EEAS), *Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)*, EEAS Policy Framework, 2024; Alina Polyakova, Spencer Phipps Boyer, *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, Brookings Institution, 2018.

Între 2015 și 2018, abordarea europeană a dezinformării a rămas preponderent geopolitică, orientată către contracararea „destabilizării externe” și abia ulterior a început să includă dimensiunile societale și educaționale. Raportul Comisiei Europene din 2018, urmat de *Codul de bune practici privind dezinformarea*, marchează momentul în care Uniunea începe să își reformuleze paradigma: de la apărare externă la reziliență internă. Din perspectiva teoriei Școlii de la Paris, acest moment reprezintă tranziția de la securitizarea discursivă la guvernarea cognitivă. Nu mai este vorba doar despre etichetarea unei amenințări, ci despre instituționalizarea unui ansamblu de practici, norme și tehnologii care gestionează fluxul informațional. Programele de media literacy, reglementările algoritmice ale *Digital Services Act*, inițiativele *FIMI Toolbox* sau *European Democracy Action Plan* exemplifică această materializare a securității cognitive în infrastructuri normative și tehnice.

Uniunea Europeană poate valorifica în mod strategic experiența statelor membre „de frontieră”, în special a statelor baltice, care s-au confruntat constant cu întregul repertoriu de interferențe și cu strategiile agresive de dezinformare ale Rusiei. În Letonia și Estonia, publicurile vorbitoare de rusă au fost vizate printr-o arhitectură media-tică multicanal – rețele sociale, televiziuni și ziare controlate de statul rus, precum și rețele de agenți de influență – proiectată să producă efecte cumulative. Nucleul narativ recurent are două axe: (1) delegitimarea statelor baltice ca „state eșuate”, naționaliste și „fasciste”, presupus aflate în declin după aderarea la UE și NATO; (2) portretizarea UE, NATO și SUA drept forțe care folosesc spațiul baltic ca rampă pentru o agresiune iminentă împotriva Rusiei. Acest cadru narativ este dublat de o strategie de rescriere a istoriei și falsificare a memoriei colective, prin care Moscova revendică un pretins „drept de control” geopolitic și de „tutelă politică” asupra unor vecini precum statele baltice, Ucraina, Belarus, Georgia sau Republica Moldova. Răspunsul baltic s-a construit pe o abordare la nivelul întregii societăți, conectând instituțiile publice, sectorul privat, mediul academic și organizațiile civice, generând politici publice incluzive și adaptive la preocupările reale ale populației. Elementele-cheie includ consolidarea pluralismului informațional, programe de educație civică orientate spre gândire critică, mecanisme agile de anticipare și neutralizare preventivă a narațiunilor false, precum și susținerea fermă a unei presei independente capabile să

verifice și să demonteze rapid afirmațiile înșelătoare. Lecția strategică pentru UE este clară: reziliența societală nu derivă doar din instrumente punitive sau tehnice, ci din capacitatea de a integra actori multipli într-un ecosistem informațional robust, transparent și responsabil, în care narațiunile manipulative își pierd tracțiunea înainte de a produce fisuri sociale profunde.

O serie de evenimente politice și tehnologice au determinat factorii de decizie din Uniunea Europeană să analizeze consecințele sociale și politice ale campaniilor de dezinformare. Analizele specialiștilor în comunicare au pus în evidență a unor fenomene precum cel legat de rolul *Cambridge Analytica* în alegerile prezidențiale americane din 2016 și în desfășurarea referendumului pentru Brexit. Campania de dezinformare din peisajul politic britanic în timpul votului pentru Brexit a determinat ieșirea Regatului Unit din Uniunea Europeană. Acest fapt, cu efecte destabilizatoare în interiorul spațiului comunitar, a demonstrat că, prin utilizarea unor algoritmi opaci, cetățenii unui stat pot fi manipulați și că o gamă de operațiuni hibride informaționale pot foarte ușor să afecteze grav integritatea proceselor democratice. Comisia Europeană și Parlamentul European descopereau că puterea marilor platforme digitale a crescut periculos, ajungând să vizeze scopuri politice. Algoritmii acestor platforme, orientați nu doar spre un profit strict comercial, ci și politic, indicau ce conținut este publicat, partajat și proliferat în spațiul digital, fără „transparență suficientă, fără verificare adecvată a faptelor și fără responsabilitate față de societăți și audiențe”²⁹.

Libertatea comunicării trebuie dublată de securitate cognitivă

Procesul lent și aparent greoi al elaborării unei strategii europene de combatere a dezinformării nu trebuie privit doar ca un deficit de reacție și de decizie politică. Elaborarea unei asemenea strategii a fost o consecință a unui proces de echilibrare între valori etice și demersuri politice. Europa a fost forțată să-și redefinească propria identitate liberală într-un context în care *protecția democrației* presupune o formă activă

²⁹ European Centre of Excellence and the Media Pool, *Countering Disinformation: News Media and Legal Resilience workshop*, April 2019, <https://www.hybridcoe.fi/publications/hybrid-coe-paper-1-countering-disinformation-news-media-and-legal-resilience/>.

de intervenție în ecosistemul informațional. A accepta că informația poate fi instrumentalizată ca armă de către actori statali care vor să distrugă structura valorică a democrației liberale înseamnă, implicit, a admite că libertatea comunicării trebuie însoțită de o infrastructură de securitate cognitivă.

Începând cu pandemia de COVID-19 (2020), când fenomenul *infodemiei* a devenit o problemă de sănătate publică și de încredere socială, UE a recunoscut explicit necesitatea unei guvernante integrate a dezinformării. Astfel, logica „contracării narative” s-a transformat într-o politică de protejare a ecosistemului informațional, în care dimensiunile tehnice (infrastructură), juridice (reglementare) și educaționale (reziliență societală) converg într-un cadru coerent. Ceea ce se profilează, în ultimă instanță, este nașterea unei doctrine europene a *suveranității cognitive* – o extensie conceptuală a *suveranității digitale*. Dacă prima se exercită prin securitate tehnologică, a doua prin reziliență informațională democratică. Uniunea Europeană a trecut astfel de la o politică reactivă la o strategie comunitară coerentă, menită să protejeze însăși condiția epistemică a democrației. Potrivit declarației comune oficiale a statelor membre din 28 iunie 2018: „Consiliul European invită Înalțul Reprezentant și Comisia să prezinte, în cooperare cu statele membre și în conformitate cu concluziile Consiliului European din martie 2015, un plan de acțiune până în decembrie 2018, care să conțină propuneri specifice pentru un răspuns coordonat al Uniunii Europene la provocarea reprezentată de dezinformare, inclusiv mandate adecvate și resurse suficiente pentru echipele de comunicare strategică relevante ale Serviciului European de Acțiune Externă (EEAS)”³⁰.

Mult timp, politicile europene privind combaterea dezinformării fuseseră concepute limitativ în logica reglementării mass-media – axate pe etică jurnalistică, pluralism informațional și sprijin pentru presa independentă. Aceste măsuri, deși esențiale, s-au dovedit insuficiente în fața dezinformării algoritmice și a campaniilor coordonate derulate de actori statali sau rețele transnaționale. Într-un mediu digital dominat de platforme care funcționează ca *amplificatoare emoționale*, problema nu mai este doar cea a conținutului fals, ci a interferenței structurale în formarea percepțiilor și opiniilor.

³⁰ European Council Conclusions, 28 June 2018, <https://www.consilium.europa.eu/en/press/press-releases/2018/06/29/20180628-euco-conclusions-final/>.

De aceea, combaterea dezinformării trebuie reconceptualizată în termenii securității cognitive. Aceasta presupune trecerea de la o abordare reactivă (corectarea informațiilor false) la una sistemică și preventivă, care vizează protejarea integrității procesului de gândire publică. În acest cadru, instrumente precum DSA (prin evaluarea riscurilor sistemice și auditarea algoritmică), AI Act (prin reglementarea conținutului sintetic și a deepfake-urilor) și Foreign Information Manipulation and Interference³¹ (FIMI) Toolbox (prin coordonarea răspunsului diplomatic la ingerințe străine) devin elemente constitutive ale unei politici de apărare cognitivă.

În termeni de guvernanță, securitatea cognitivă extinde paradigma europeană de „securitate umană” către protecția libertății mentale – adică a condiției de a gândi, evalua și decide autonom. Ea transformă cetățeanul digital din simplu receptor de informații în subiect al rațiunii democratice, iar statul din simplu reglementator media într-un garant al ecologiei cognitive. Această mutație conceptuală este esențială: fără securitate cognitivă, securitatea cibernetică rămâne o formă fără fond. Un sistem digital impecabil din punct de vedere tehnic poate fi subminat prin controlul percepțiilor și manipularea narațiunilor. În epoca războiului informațional, mintea devine infrastructura strategică a democrației, iar protejarea ei trebuie tratată ca o prioritate de securitate națională și europeană.

Modele de combatere a dezinformării

Deși Uniunea Europeană a dezvoltat, începând cu 2015, un cadru strategic coerent pentru combaterea dezinformării și protejarea spațiului informațional, modul în care aceste orientări comune sunt transpuse în politici publice variază considerabil între statele membre.

³¹ Definițiile oficiale ale conceptului *Foreign Information Manipulation and Interference* (FIMI) în actele Uniunii Europene includ descrieri ale unor acțiuni deliberate, concertate, menite să influențeze opiniile publice și procesele democratice ale statelor membre prin manipularea sau interferența cu fluxul informațiilor. Comisia Europeană definește FIMI ca „*activități ostile externe care includ dezinformare, manipulare a opiniei publice și interferență în procesele politice pentru a submina suveranitatea digitală, stabilitatea democratică și coeziunea socială a Uniunii Europene*.” Acest concept subliniază natura transfrontalieră și strategică a acestor atacuri informaționale, reprezentând o provocare de securitate hibridă ce necesită cadre instituționale coordonate și tehnologii avansate pentru detectare și contracarare. Aceste definiții regăsite în documentele strategice și legislația UE, cum ar fi Strategia pentru o Uniune Europeană a Securității și documentele privind combaterea amenințărilor hibride, fundamentează înțelegerea și abordarea juridică a FIMI în spațiul european.

Această diversitate nu reflectă o lipsă de coordonare, ci un aspect structural al proiectului european: statele își adaptează arhitecturile de reziliență cognitivă în funcție de propriile tradiții instituționale, memorie istorică, percepții de securitate și experiențe directe cu operațiuni informaționale ostile. Astfel, strategia europeană devine un cadru de referință, nu un model uniform, lăsând spațiu pentru experimente naționale și configurații locale de protecție informațională.

În practică, convergența europeană în domeniul combaterii dezinformării funcționează pe două niveluri. La nivel vertical, instituțiile UE definesc standardele, instrumentele și mecanismele de cooperare – de la Planul de acțiune pentru comunicare strategică și *East StratCom Task Force* la reglementările privind platformele digitale (ex. Actul privind serviciile digitale – DSA). La nivel orizontal, statele membre internalizează aceste orientări, creând modele proprii de „suveranitate cognitivă“. Aici intervin diferențele: unele state prioritizează educația media și alfabetizarea digitală ca formă de imunitate socială; altele optează pentru structuri instituționalizate de supraveghere și reacție rapidă; iar altele dezvoltă mecanisme orientate spre contraîngerință și atribuire a actorilor străini.

Această pluralitate nu este accidentală, ci rezultatul unui context geopolitic și socio-cultural eterogen. Statele baltice și nordice – marcate de proximitatea Rusiei și de tradiții solide de educație civică – adoptă o abordare societală, în care protecția cognitivă este o extensie a culturii democratice. Țările central-europene, aflate la intersecția presiunilor geopolitice și a vulnerabilităților instituționale, preferă mecanisme de apărare centralizate, cu funcții operative clare. Franța, în schimb, conceptualizează dezinformarea ca problemă de suveranitate națională, integrând-o în arhitectura sa de securitate strategică. Prin urmare, politicile europene nu produc un model unic de reziliență cognitivă, ci generează o hartă complexă de soluții naționale, reflectând atât unitatea idealurilor europene, cât și diversitatea modalităților de a le proteja.

În interiorul Uniunii Europene, eforturile de combatere a dezinformării au evoluat într-un mozaic complex de politici naționale, fiecare reflectând specificități istorice, tradiții instituționale și raportări diferite la amenințările informaționale provenite din exterior. Această diversitate a produs trei modele strategice distincte, care pot fi interpretate ca tipologii ale suveranității cognitive europene: *modelul nordic-baltic*, fundamentat pe reziliență societală și educație civică; *modelul central-european*, centrat pe apărare instituționalizată și structură adminis-

trativă coerentă; și *modelul francez*, orientat spre contraîngerință informațională și afirmarea unei autonomii strategice în spațiul digital. Împreună, aceste modele nu descriu doar trei răspunsuri politice, ci trei filosofii ale protecției spațiului cognitiv într-o epocă în care informația devine parte integrantă a arhitecturii securității naționale.

Modelul nordic-baltic reprezintă paradigma în care suveranitatea cognitivă este concepută mai degrabă ca o calitate emergentă a culturii democratice decât ca un produs instituțional centralizat. Finlanda, considerată în mod constant un studiu de referință, a transformat alfabetizarea media într-un pilon structural al educației publice, tratând dezinformarea nu ca o îngerință externă punctuală, ci ca o formă de igienă democratică ce trebuie cultivată încă din școală. Integrarea educației media în curricula națională încă din 2016 a creat un ecosistem cognitiv în care gândirea critică, verificarea surselor și capacitatea de a recunoaște manipulări emoționale fac parte din „norma” participării civice. Această infrastructură educațională a fost completată de o arhitectură de încredere instituțională, în care transparența, comunicarea guvernamentală proactivă și colaborarea dintre stat, radiodifuzorul public și ONG-uri generează o reziliență cognitivă difuză, dar profund eficientă. Estonia, confruntată istoric cu operațiunile informaționale ale Federației Ruse, a adăugat acestei baze civice o componentă defensivă integrată în Ministerul Apărării, articulând un model hibrid în care monitorizarea narațiunilor ostile și consolidarea educației digitale sunt părți ale aceluiasi proiect societal. Lecția implicită a acestui model este că suveranitatea cognitivă nu se construiește prin reacție, ci prin împuternicirea cetățenilor și cultivarea discernământului într-un mediu informațional saturat.

Modelul central-european, ilustrat cel mai clar de Cehia și Polonia, adoptă o filosofie diferită: suveranitatea cognitivă este văzută ca o extensie a securității naționale, un domeniu ce reclamă vigilență, infrastructuri administrative clare și reacții instituționale rapide. Crearea *Centrului împotriva Terorismului și Amenințărilor Hibride* (CTHH) în Cehia a reprezentat prima încercare sistematică din UE de a dezvolta o capacitate guvernamentală dedicată monitorizării campaniilor de influență și coordonării răspunsului statului. Acest model presupune centralizare, expertiză tehnică și responsabilizare publică – o abordare care reflectă poziționarea Europei Centrale la intersecția presiunilor geopolitice, în special din partea Rusiei. Polonia, prin Strategia de

Reziliență și Securitate a Informațiilor din 2023, merge chiar mai departe, plasând dezinformarea în registrul apărării teritoriale extinse, ca parte a protecției „frontierelor mentale” ale națiunii. În ciuda riscului inerent de politizare sau birocratizare, modelul central-european oferă o coerență operațională importantă: capacitatea de răspuns este organizată, scalabilă și ancorată în structuri instituționale stabile, ceea ce permite statelor să reacționeze rapid la campanii de interferență externă.

Modelul francez propune o a treia paradigmă: *combaterea dezinformării este concepută ca o problemă de suveranitate informațională*, un domeniu în care statul își protejează activ spațiul digital împotriva ingerințelor străine. Înființarea, în 2021, a structurii VIGINUM³² marchează instituționalizarea unei doctrine în care detecția, atribuirea și documentarea campaniilor externe de manipulare devin funcții strategice. Spre deosebire de modelul nordic, centrat pe societate, sau de cel central-european, orientat spre gestionarea internă a riscului, modelul francez introduce o dimensiune geopolitică explicită: apărarea cognitivă presupune nu doar monitorizare, ci și capacitatea de a răspunde diplomatic, tehnologic și normativ actorilor care încearcă să destabilizeze spațiul informațional național. Integrarea eforturilor de securitate cognitivă cu politicile de *autonomie strategică digitală* – de la proiectele de *cloud souverain*³³ la reglementarea platformelor prin DSA – transformă Franța într-un vector al unei noi viziuni europene: aceea că securitatea informațională și suveranitatea tehnologică sunt inseparabile într-o lume dominată de competiția pentru controlul fluxurilor narrative distribuite online.

³² VIGINUM (Serviciul de vigilență și protecție împotriva interferențelor digitale străine) este serviciul guvernamental francez creat în 2021 sub autoritatea primului-ministru (în cadrul Secretariatului General al Apărării și Securității Naționale) pentru a detecta, analiza și documenta interferențele digitale străine care vizează spațiul informațional francez. Acesta funcționează ca o unitate specializată de combatere a dezinformării și monitorizare, axată pe campanii de manipulare externă în comunicarea publică online (alegeri, crize majore, dezbateri strategice), cu misiuni principale de detectare tehnică (analiza platformelor și rețelelor), atribuirea operațiunilor de influență străină și producerea de rapoarte și alerte publice care informează autoritățile franceze, partenerii și publicul larg.

³³ Cloud suveran (eng. „sovereign cloud”) se referă la infrastructura și serviciile cloud operate sub jurisdicție și control legal european, asigurând că toate datele, sarcinile de lucru și operațiunile sunt supuse exclusiv legislației UE și rămân protejate de accesul entităților din afara UE. Acest concept își propune să garanteze rezidența datelor, confidențialitatea, securitatea și conformitatea pentru operațiunile sensibile din sectorul public și din industria critică. Printre caracteristicile cheie se numără stocarea și prelucrarea locală a datelor, gestionarea și asistența la nivelul UE și măsuri de protecție a datelor de legile străine (din afara UE), permițând astfel autonomia strategică pentru guvernele și întreprinderile europene în ecosistemul cloud.

Împreună, cele trei modele reflectă maturizarea conceptului de suveranitate cognitivă la nivel european. Diversitatea lor nu este un semn de fragmentare, ci expresia unui pluralism operațional adaptat unor ecologii informaționale diferite. Uniunea Europeană trece astfel de la o paradigmă mediacentrică, focalizată pe combaterea punctuală a știrilor false, la o paradigmă sistemică, în care reziliența cognitivă este înțeleasă ca o condiție structurală pentru menținerea unui spațiu public democratic și a unei ordini politice stabile.

Cazul României

România nu are încă o strategie națională unică și coerentă împotriva dezinformării, comparabilă cu modelele mai instituționalizate din state precum Franța, dar dezinformarea este recunoscută în mod explicit ca o amenințare la adresa securității în documentele strategice de bază. Strategia Națională de Apărare 2020–2024³⁴ încadrează operațiunile informaționale ostile și campaniile de dezinformare drept riscuri la adresa securității naționale și solicită capacități de identificare și contracarare a „mișcărilor de dezinformare susținute de actori statali sau nestatali ostili“, inclusiv printr-o comunicare strategică îmbunătățită și o alfabetizare funcțională.

Într-un sens mai larg, analizele ONG-urilor europene notează că autoritățile române „până acum nu au reușit să combată eficient dezinformarea“³⁵, indicând o discrepanță între recunoașterea amenințărilor în documentele strategice și absența unui organism de coordonare dedicat, cu resurse suficiente, sau a unei legislații actualizate, adaptate special manipulării și interferențelor informațiilor străine.

Cadrul normativ românesc referitor la dezinformare este alcătuit dintr-o serie de acte legislative și reglementări disparate, fiecare abordând parțial problema, fără a constitui însă o arhitectură coerentă de protecție informațională. În această categorie intră: articolul 404 din *Codul penal*, care incriminează comunicarea de informații false atunci când aceasta pune în pericol siguranța națională; *Legea 504/2002 privind audiovizualul*, împreună cu *Codul CNA*, actualizate în 2025;

³⁴ Romania Presidential Administration, „National Defence Strategy 2020-2024“, Bucharest 2020, https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf.

³⁵ Ciprian Cucu, Susanna Dragomir, Madalina Botan, *The disinformation landscape in Romania*, EU DisinfoLab, 3 November 2025, <https://www.disinfo.eu/publications/disinformation-landscape-in-romania/>.

Legea 50/2024, prin care România a implementat *Regulamentul (UE) 2022/2065 privind serviciile digitale (DSA)*; precum și *Ordonanța de Urgență nr. 1/2025*, adoptată în contextul anulării alegerilor din 2024, cu scopul declarat de a contracara interferențele informaționale.

Cu toate acestea, convergența acestor acte legislative rămâne în mare parte formală. *Articolul 404* nu a fost aplicat în practică până în prezent, ceea ce indică reticența autorităților de a utiliza instrumente penale într-un domeniu sensibil pentru libertatea de exprimare. La rândul său, *OUG 1/2025* a generat critici consistente din partea organizațiilor civice și a experților în drept digital, din cauza lipsei de transparență în elaborare și a riscului de a introduce restricții disproporționate asupra comunicării publice. Astfel, deși legislația existentă reflectă o preocupare crescândă pentru combaterea dezinformării, ansamblul rămâne fragmentat și lipsit de un cadru conceptual unitar, ceea ce limitează eficiența și legitimitatea intervențiilor statului în spațiul informațional.

În acest context, răspunsul României în timpul alegerilor prezidențiale din 2024 s-a bazat în mare măsură pe mecanisme de informații, electorale și de reglementare, mai degrabă decât pe o strategie antidezinformare solidă și bine articulată. Rapoartele de informații declasificate, publicate de președintele României, precum și litigiile constituționale legate de primul tur anulat al scrutinului prezidențial au evidențiat rolul unui stat străin – cunoscut pe scară largă ca fiind Rusia – în orchestrarea unor operațiuni coordonate de influențare pe rețelele sociale (boți TikTok, amplificare neautentică, finanțare sub acoperire a influencerilor) în favoarea unui candidat de extremă dreapta. Societatea civilă și observatorii internaționali descriu acest episod ca un „test de stres” pentru democrația românească, menționând că răspunsurile instituționale au fost reactive și fragmentate, fără nicio agenție unică mandată în mod clar să conducă detectarea, atribuirea și comunicarea publică cu privire la interferențele străine.

Interferența Rusiei în contextul electoral din România în 2024 s-a manifestat printr-un set coerent de mecanisme hibride, adaptate vulnerabilităților locale și calibrate în raport cu evoluțiile geopolitice regionale (războiul din Ucraina, tensiunile energetice, polarizarea politică internă). Pe plan informațional, rețelele mediatice pro-Kremlin – atât cele vizibile, cât și cele covertizate – au amplificat narațiuni asociate delegitimării procesului electoral, erodării încrederii în instituțiile democratice și promovării unei imagini disfuncționale a statului român. Acestea au inclus teme precum „România colonie”, „dictatura Bruxelles-ului”,

„războiul NATO cu Rusia“, „îminența mobilizării“, precum și mesaje antiucraniene destinate să fractureze consensul prooccidental. În paralel, s-au activat operațiuni digitale de amplificare artificială a conținutului polarizant: utilizarea de conturi false, troli și boți, rețele de microinfluențatori plătiți, precum și recurența platformelor Telegram și TikTok ca noduri de difuzare rapidă a narațiunilor destabilizatoare.

Pe dimensiunea cibernetică, România a înregistrat atacuri asupra unor infrastructuri instituționale și platforme publice, atribuite unor actori afiliați GRU sau grupărilor proxy (Killnet, NoName057(16)), care au urmărit mai degrabă perturbarea și intimidarea decât compromiterea directă a procesului de vot. Toate aceste acțiuni au fost însoțite de operațiuni de influență indirectă – sprijin mediatic și algoritmic acordat unor candidați radicali sau antisistem, infiltrarea discursurilor extremiste în spațiul online și exploatarea temelor socio-economice sensibile (inflație, migrație, sărăcie). În ansamblu, mecanismele rusești au urmărit să altereze percepția publică, să inducă neîncrederea în integritatea procesului electoral și să slăbească capacitatea României de a acționa concertat în plan euro-atlantic, folosind un arsenal hibrid ce combină propaganda, cyber-perturbarea și manipularea psihologică în mediul digital.

O mare parte din activitatea de monitorizare, analiză și combatere a dezinformării în România este desfășurată de o constelație de ONG-uri, organizații de cercetare media și rețele europene, mai degrabă decât de o autoritate națională centrală. Printre actorii cheie se numără Centrul Român pentru Politici Europene (CRPE), care publică rapoarte detaliate de monitorizare a narațiunilor anti-UE și pro-Kremlin. Grupuri de reflecție sau organisme de supraveghere precum Expert Forum și Veridica urmăresc rețelele de dezinformare și narațiunile conspirative legate de politicile UE, energie, migrație și reglementarea digitală. Aceste organizații funcționează adesea ca centre de avertizare timpurie și analiză, contribuind cu concluziile lor la dezbaterile la nivel UE privind riscurile sistemice în temeiul Legii privind serviciile digitale și privind implementarea Codului de bune practici al UE privind dezinformarea.

O dezvoltare structurală importantă este participarea României la Observatorul Bulgaro-Român al Media Digitală (BROD), un hub regional EDMO (Observatorul European al Media Digitală) cofinanțat de UE. BROD reunește verificatori de fapte, cercetători și parteneri tehnologici pentru a detecta și analiza campaniile de dezinformare

din Bulgaria și România, a oferi instrumente de verificare a faptelor în mai multe limbi și a dezvolta inițiative de alfabetizare media; rețeaua sa a jucat un rol vizibil în monitorizarea dezinformării în jurul alegerilor prezidențiale românești din 2024 și în legătură cu războiul din Ucraina și evoluțiile din Moldova. Evaluările internaționale subliniază faptul că, având în vedere lipsa unei autorități naționale centrale de combatere a dezinformării, aceste structuri legate de EDMO și parteneriatele societății civile sunt piloni *de facto* ai arhitecturii de reziliență a României.

Noua Strategie Națională de Apărare, adoptată în 2025 de România, recunoaște explicit că, în actualul context geopolitic legat de războiul din Ucraina și de riscurile implicate de operațiunile hibride, instrumentele de dezinformare, manipulare informațională și atacuri cibernetice generate de actori ostili – în special de Federația Rusă – constituie unele dintre cele mai grave amenințări la adresa securității naționale. Strategia identifică aceste amenințări nu doar ca incidente izolate, ci ca parte integrantă a unui „război hibrid” coordonat, menit să submineze coeziunea socială, încrederea în instituții, stabilitatea democratică și capacitatea României de acțiune strategică autonomă. Documentul menționează că „acțiunile din spectrul hibrid generate de actori ostili, manifestate în special prin dezinformare, *fake-news*, manipularea spațiului informațional, influențe maligne, însă și prin atacuri cibernetice, angrenarea zonei de intelligence și alte instrumente ale puterii rămân amenințări persistente, cu efecte cumulative pe termen lung. Agresiunile din zona informațională au ca scop modelarea și/sau influențarea percepției publice, în vederea subminării coeziunii sociale și a încrederii în instituțiile democratice, în UE și NATO”³⁶.

Strategia Națională de Apărare a Țării din 2025 inserează combaterea dezinformării și a manipulării informaționale în categoria vulnerabilităților interne – alături de corupție, slaba calitate a administrației publice și incoerența politicilor sectoriale – subliniind că integritatea spațiului informațional este la fel de importantă pentru securitatea unui stat precum securitatea militară sau economică. Această formulare semnalează o înțelegere strategică extinsă a securității, care recunoaște că statul trebuie să-și protejeze „frontierele cognitive” – adică capaci-

³⁶ Președinția României, „Strategia Națională de Apărare a Țării pentru perioada 2025-2030”, pg. 18, Punctul 48, <https://www.presidency.ro/ro/media/csat/strategia-nationala-de-aparare-a-tarii-pentru-perioada-2025-2030>.

tatea sa de a garanta un public informat, instituții credibile și control democratic – în fața amenințărilor informaționale externe. În consecință, strategia reafirmă rolul esențial al instituțiilor de stat – servicii de informații, autorități publice, organe de reglementare – nu doar în termeni de apărare convențională, dar și ca gardieni ai suveranității informaționale și ai rezilienței societale. Această abordare integrează securitatea informațională, protecția democratică și rezistența civică într-un cadru strategic coerent, reflectând transformarea paradigmei securitare europene la nivel național: nu mai e vorba doar despre arme și teritoriu, ci și despre memorie colectivă, discurs public și veridicitate informațională.

*Suveranitatea digitală:
între autonomie tehnologică și dependență globală*

Abordarea europeană a combaterii dezinformării nu poate fi înțeleasă în afara cadrului mai larg al transformărilor geopolitice și tehnologice care au reconfigurat relația dintre securitate și infrastructura digitală. Deși măsurile de contracarare a manipulării informaționale par, la prima vedere, încadrate în logica protecției spațiului public, ele indică de fapt emergența unei noi paradigme: securitatea cognitivă depinde tot mai mult de arhitectura tehnologică în care circulă informațiile. În acest sens, strategiile antidezinformare ale UE nu reprezintă doar un răspuns la agresiuni informaționale punctuale, ci și primul pas către o reflecție mai profundă asupra vulnerabilităților inerente democrațiilor din UE care se confruntă cu un ecosistem digital dominat structural de actori noneuropeni.

Această observație conduce inevitabil la ideea că protejarea spațiului cognitiv european presupune, în mod structural, protejarea spațiului tehnologic european. Dezinformarea, ingerințele străine și manipularea narativă sunt posibile pentru că există o ingeniozitate tehnologică a actorilor statali ostili. Dar aceste ingerințe sunt favorizate și pentru că UE operează într-o infrastructură digitală globalizată, în care fluxurile de date, algoritmii și platformele sunt controlate în mare parte în afara suveranității sale normative. Astfel, lupta împotriva dezinformării devine o fereastră către limitele strategice ale Europei: dependența de tehnologii externe, vulnerabilitatea la logici comerciale algoritmice și dificultatea de a impune standarde etice într-un mediu digital dominat de interese geopolitice divergente. În acest cadru, secu-

ritatea cognitivă se transformă într-o problemă de autonomie tehnologică, iar politica informațională devine inseparabilă de politica tehnologică.

În consecință, tranziția către tema suveranității digitale este nu doar logică. Este imperios necesară. Dacă strategia UE de combatere a dezinformării urmărește protejarea spațiului public și menținerea integrității democrației, suveranitatea digitală reprezintă infrastructura care face posibilă această protecție. Relația dintre ele nu este una de succesiune, ci una de interdependență: fără autonomie tehnologică, combaterea dezinformării rămâne o formă de reacție într-un mediu controlat de alții; iar fără reziliență cognitivă, suveranitatea digitală riscă să devină un proiect tehnic fără impact democratic. În această intersecție, capitolul dedicat suveranității digitale analizează tensiunea fundamentală în care se află UE: între aspirația la autonomie strategică și realitatea unei dependențe globale de infrastructuri, platforme și tehnologii care nu îi aparțin.

Combaterea eficientă a dezinformării și protejarea robustă a *suveranității cognitive* în Uniunea Europeană depind fundamental de urmărirea *suveranității digitale*. Suveranitatea digitală – definită drept capacitatea autonomă de a reglementa și guverna infrastructurile digitale, datele și tehnologiile în conformitate cu valorile și interesele europene – servește drept coloană vertebrală instituțională pentru apărarea capacității cetățenilor de a gândi, de a delibera și de a participa liber în cadrul proceselor democratice. În absența suveranității digitale, UE rămâne vulnerabilă la influența extrateritorială, la dependențele tehnologice și la fragmentarea reglementărilor, care nu numai că subminează acțiunile coordonate împotriva dezinformării, dar expun și procesele cognitive manipulării de către actori și platforme din afara UE.

Conceptul de *suveranitate digitală* s-a născut la intersecția dintre tehnologie, economie și politică, în momentul în care rețelele informatice au încetat să mai fie simple infrastructuri de comunicație și au devenit arhitecturi ale puterii. Formulată pentru prima dată la începutul anilor 2000 și teoretizată de Pierre Bellanger în 2011, termenul desemna capacitatea unui stat – și, prin extensie, a unei comunități politice – de a-și exercita controlul asupra propriei existențe colective în mediul digital, adică asupra modului în care tehnologiile, datele și algoritmiile modelează destinul său economic și cultural.

Interdependența dintre suveranitatea cognitivă și cea digitală devine deosebit de importantă în contextul strategiilor contemporane ale UE

de combatere a dezinformării. Fără un control european ferm asupra infrastructurii, platformelor și algoritmilor digitali, măsurile care vizează protejarea integrității informaționale și a încrederii publice sunt în mod inerent limitate.

Speculativ, pe măsură ce UE implementează inițiative legislative majore, cum ar fi Legea privind serviciile digitale, Legea privind piețele digitale și Legea privind inteligența artificială, fuziunea conceptuală dintre suveranitatea cognitivă și suveranitatea digitală apare ca o condiție prealabilă pentru o sferă publică rezistentă – una în care cetățenii sunt împuterniciți să navigheze în siguranță prin peisaje informaționale complexe, protejați de intervenții cognitive ostile. Suveranitatea digitală a UE evoluează astfel atât într-o precondiție, cât și într-un garant al suveranității cognitive, aliniind reglementarea tehnologică cu imperativul democratic de a proteja gândirea liberă și neinfluențată.

Declarația pentru suveranitatea digitală europeană (engl. *Declaration for European Digital Sovereignty*), semnată la Summitul UE de la Berlin din 18 noiembrie 2025, marchează o piatră de hotar în angajamentul Uniunii Europene față de autonomia strategică în domeniul digital. Susținută de reprezentanți ai tuturor celor 27 de state membre ale UE, declarația articulează o viziune colectivă pentru reducerea dependențelor tehnologice – în special față de actorii din afara UE –, consolidarea capacităților Europei în industriile digitale strategice și protejarea datelor sensibile de interferențele externe și de efectele reglementărilor extrateritoriale.

Documentul prezintă suveranitatea digitală ca fiind capacitatea autonomă a UE de a reglementa infrastructurile, platformele și tehnologiile digitale pe baza valorilor europene, a principiilor democratice și a intereselor de securitate, respingând în mod expres protecționismul în favoarea unei abordări deschise, dar reziliente, a parteneriatului internațional.

Printre principalele prevederi ale Declarației se numără angajamente de promovare a dezvoltării open source, investițiile în bunuri digitale comune și infrastructura publică (cum ar fi *Portofelul European de Identitate Digitală*³⁷ și soluțiile cloud de înaltă securitate) și de spo-

³⁷ Portofelul digital european de identitate (Portofelul EUDI) este o aplicație securizată și interoperabilă instituită prin Regulamentul (UE) 2024/1183 și actele de punere în aplicare aferente, care permite cetățenilor, rezidenților și întreprinderilor din UE să își dovedească identitatea online, să gestioneze datele cu caracter personal și să partajeze acreditări verificate la nivel trans-

rire a transparenței și competitivității în cadrul pieței interne printr-o simplificare a reglementărilor favorabilă inovării.

Franța și Germania, în calitate de principali susținători, au solicitat, de asemenea, amânarea anumitor prevederi ale Legii privind inteligența artificială privind sistemele cu risc ridicat pentru a facilita inovația, precum și alinierea reformelor GDPR cu cerințele europene mai ample în materie de securitate cibernetică. Declarația subliniază, de asemenea, dimensiunea umană a suveranității digitale, afirmând că autonomia tehnologică este inseparabilă de reziliența democratică, deschiderea societală și emanciparea cetățenilor europeni în lumea digitală.

Într-o lume dominată de gigantismul platformelor americane – Google, Apple, Facebook, Amazon –, dezbateră privind suveranitatea digitală a devenit rapid o chestiune de *supraviețuire strategică*. Transferul de valoare către aceste companii, asimetriile economice și dependența infrastructurală au început să submineze principiul însuși al suveranității naționale. De aceea, începând cu 2014, numeroase inițiative europene au încercat să formuleze răspunsuri politice și juridice la această colonizare digitală, pledând pentru un cadru normativ care să împace libertatea rețelei cu protecția interesului public.

Nevoia Uniunii Europene de a-și consolida suveranitatea digitală este determinată fundamental de ambiția de a proteja integritatea, competitivitatea și autonomia ecosistemului tehnologic al continentului într-un context global marcat de provocări fără precedent. Adoptarea unor reglementări precum *Regulamentul General privind Protecția Datelor* (GDPR)³⁸ sau *Actul privind Inteligența Artificială* reflectă nu

frontalier. Portofelul este conceput pentru a sprijini interacțiunile online și offline cu serviciile din sectorul public și privat, inclusiv cele bancare, educaționale și medicale, menținând în același timp controlul utilizatorului, confidențialitatea prin proiectare, divulgarea selectivă a atributelor și portabilitatea datelor. Statele membre sunt obligate să pună portofelele EUDI la dispoziția tuturor cetățenilor până în 2026, permițând semnăturile electronice calificate și sprijinind obiectivele de suveranitate digitală ale UE prin crearea unui cadru unificat și de încredere pentru identificarea și autentificarea personală.

³⁸ Regulamentul General privind Protecția Datelor (GDPR), oficial Regulamentul (UE) 2016/679, este cadrul cuprinzător al Uniunii Europene care reglementează colectarea, prelucrarea și transferul datelor cu caracter personal. Intrat în vigoare din 25 mai 2018, GDPR stabilește principii stricte de legalitate, echitate, transparență, minimizare a datelor, limitare a stocării, acuratețe, integritate, confidențialitate și responsabilitate pentru toate organizațiile – din interiorul sau din afara UE – care gestionează informațiile personale ale rezidenților UE. Acesta oferă persoanelor drepturi extinse, inclusiv acces, rectificare, ștergere („dreptul de a fi uitat”), obiecție, restricționare și portabilitate a datelor lor și impune respectarea confidențialității prin proiectare și implicit în sistemele și serviciile digitale. Regulamentul este aplicat prin sancțiuni semnificative pentru nerespectare (până la 20 de milioane de euro sau 4% din cifra de afaceri globală anuală), asigurând un standard ridicat de protecție a datelor și armonizare a reglementărilor în toate statele membre.

doar preocuparea pentru protecția datelor și pentru dezvoltarea etică a inteligenței artificiale, ci și dorința de a recalibra raportul de forțe în raport cu marile companii tehnologice globale, dintre care multe operează în afara jurisdicției directe a Europei. Deși oponenții – inclusiv giganți americani și europeni ai industriei – susțin că aceste reglementări ar putea frâna inovația și ar putea dezavantaja firmele europene, Uniunea Europeană le consideră instrumente necesare pentru apărarea intereselor sale strategice și reducerea dependenței de actori noneuropeni în domeniul infrastructurii digitale și al platformelor tehnologice.

Această reglementare este emblematică pentru strategia mai largă a UE de a construi o suveranitate digitală – capacitatea de a lua decizii independente privind infrastructura digitală, fluxurile de date și standardele tehnologice, protejând în același timp drepturile și valorile cetățenilor europeni. Un principiu central al acestei strategii este asigurarea faptului că entitățile europene păstrează un control substanțial asupra datelor personale, industriale și strategice, reducând astfel riscurile asociate presiunilor politice externe sau monopolizării pieței de către mari conglomerate tehnologice. Suveranitatea tehnologică – incluzând eforturi de consolidare a securității cibernetice, certificare a produselor digitale, dezvoltare de lanțuri de aprovizionare reziliente și susținere a soluțiilor europene de cloud și inteligență artificială – este privită ca o precondiție pentru un spațiu digital european autonom.

Dezbatările care înconjoară aceste reglementări de referință dezvăluie o tensiune structurală în cadrul politicii digitale europene: cum poate fi echilibrată nevoia de inovație și competiție cu imperatiile suveranității, protecției drepturilor și autonomiei strategice. Sub impactul perturbărilor geopolitice recente, UE acordă o prioritate tot mai mare independenței digitale, investind în reforme structurale și parteneriate public-private menite să stimuleze competitivitatea europeană pe termen lung. Astfel, suveranitatea digitală nu este doar un demers de reglementare, ci un proiect politic și economic destinat să modeleze viitorul tehnologic al Europei, să protejeze valorile societale ale acesteia și să îi consolideze capacitatea de a acționa decisiv într-o lume interdependentă, caracterizată de schimbări tehnologice rapide și riscuri geopolitice persistente.

Eforturile europene pentru apărarea *suveranității cognitive* (măsurile împotriva dezinformării) și a *suveranității digitale* nu se reduc la procesul de reglementare (ce norme elaborează Uniunea Europeană pentru susținerea unor asemenea eforturi). În strategiile de combatere

a dezinformării în spațiul comunitar și de susținere a suveranității digitale europene există principii de bază care fac referire la *etica utilizării datelor personale*, la cine deține, procesează și interpretează informația. În timp ce companiile promet politici de confidențialitate tot mai transparente, adevărata miză este *reconfigurarea raportului dintre stat, cetățean și mediul tehnologic*.

Asemenea teme de reflecție la nivel comunitar (cine deține, procesează și interpretează informația) marchează un punct de inflexiune politică în dezbaterea europeană despre suveranitatea digitală. Ele semnalează trecerea de la un cadru juridico-administrativ – preocupat de reguli, norme și protecții – la unul etic și politic. Miza lor reală este distribuția puterii cognitive în societate. Într-un sens profund, nu legislația în sine garantează libertatea digitală, ci principiul moral pe baza căruia se configurează mediul informațional online. Din punct de vedere moral, apare o întrebare crucială: cine are autoritatea de a decide ce anume devine vizibil, legitim, adevărat sau valoros în mediul online? Protejarea datelor nu mai este doar o chestiune de securitate sau de etică, ci una care ține de *antropologia politică*: redefinirea a ceea ce înseamnă libertate, încredere și intimitate personală într-un univers în care cetățeanul european devine simultan o sursă și un produs de date.

Această mutație se înscrie în logica trecerii de la suveranitatea teritorială la suveranitatea informațională. Este vorba despre trecerea de la controlul asupra spațiului fizic la controlul asupra spațiului cognitiv. În regimul clasic al statului-națiune, puterea se exercita prin monopolul legitim al forței și al domniei legii. În epoca digitală, puterea se exercită prin monopolul algoritmic – prin modul în care sunt structurate fluxurile de date și ierarhiile informaționale. Astfel, „cine deține, procesează și interpretează informația” devine echivalentul contemporan al întrebării: *cine guvernează?*

Această problemă nu mai este doar tehnică, ci ontologică și politică: datele nu sunt simple reprezentări ale realității, ci mecanisme care o constituie. De aceea, *etica datelor devine noua frontieră a democrației*. Atunci când interpretarea datelor este externalizată către entități private, transnaționale, opace – corporații care operează prin logici de maximizare a profitului –, se produce o mutare a centrului de suveranitate dinspre instituțiile reprezentative către algoritmi care nu pot fi trași la răspundere. Rezultatul este apariția unei tehnocrații invizibile, o formă de putere postpolitică ce redefineste raportul dintre cetățean și cunoaștere.

Aceasta conduce la *o criză a discernământului civic*, pentru că interpretarea informației nu mai aparține unei sfere publice transparente, ci unui sistem de selecție automatizată care preordonează percepția și decizia. Problema devine atunci una de moralitate publică: nu doar „cine are acces la date“, ci „cine are dreptul de a defini realitatea în baza lor“. Într-un asemenea context, reglementarea – oricât de strictă – nu mai e suficientă; ea poate cel mult limita abuzurile, dar nu restabilește autonomia cognitivă a cetățeanului.

Din această perspectivă, etica datelor se plasează la intersecția dintre filosofia politică a libertății și economia politică a informației. Ea cere nu doar norme juridice, ci și o redefinire a contractului social digital, în care accesul, transparența și responsabilitatea în interpretarea datelor devin drepturi civice fundamentale. Așadar, întrebarea „cine deține, procesează și interpretează informația“ nu mai privește doar protecția datelor personale, ci se extinde către însăși structura deliberativă a democrației. Într-o lume în care interpretarea este automatizată, etica devine singura formă de rezistență cognitivă.

Tensiunea dintre globalizare și autonomia digitală produce o nouă cartografie a puterii. Ea reprezintă una dintre cele mai profunde transformări politice ale epocii contemporane. În esență, nu mai asistăm doar la o redistribuire a resurselor economice, ci la *o reconfigurare a suveranității însăși* – o trecere de la controlul teritorial la controlul informațional. În această „geopolitică a datelor“³⁹, granițele nu se mai trasează pe hartă, ci în spațiul invizibil al infrastructurilor digitale și al fluxurilor de informație. Actorii centrali ai puterii nu mai sunt doar statele, ci și companiile globale și cetățenii interconectați, ale căror roluri se redefinesc în interiorul unui ecosistem complex, guvernat de logici algoritmice.

³⁹ „Geopolitica datelor“ desemnează modul în care controlul asupra datelor, fluxurilor de date și infrastructurilor digitale modelează relațiile de putere dintre state, regiuni și mari actori privați, transformând datele într-o resursă strategică comparabilă cu teritoriul, energia sau materiile prime critice. Se concentrează asupra modului în care regulile pentru transferurile transfrontaliere de date, localizarea datelor, reglementarea platformelor și standardele (pentru IA, cloud, 5G etc.) redistribuie puterea economică, militară și normativă la nivel global, de exemplu între SUA, UE și China (Vezi: Kieron O'Hara, Wendy Hall, *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*, Oxford University Press, 2021; Dov Greenbaum et al., „Data Geopolitics“, *Science*, 382(6675), 2023; Éric-André Martin, Julien Nocetti, Clément Tonon, „Europe: Subject or Object in the Geopolitics of Data?“, *Institut français des relations internationales* (Ifri), 2018).

Primul cerc al acestei noi topologii a puterii este *cetățeanul european*, adică individul aparținând unui stat membru al spațiului comunitar care trăiește, comunică și decide într-un mediu digital. Fiecare acțiune a acestuia în universul online devine dată, fiecare preferință a sa devine produs, iar fiecare interacțiune este stocată, analizată și valorificată economic. Într-o lume în care opacitatea tehnologică tinde să devină regulă, dreptul de proprietate asupra propriilor date devine o formă nouă de libertate civică. A ști cum sunt colectate și folosite datele personale echivalează, în secolul XXI, cu dreptul de a decide asupra propriei identități. În absența acestei transparențe, autonomia individuală este golită de conținut, iar cetățeanul se transformă într-o sursă de energie informațională pentru actori pe care nu îi poate controla.

Al doilea cerc îl reprezintă *companiile*, care au devenit principalii arhitecți ai economiei informaționale. Pentru ele, datele nu mai sunt simple resurse – sunt însuși capitalul structural din care derivă profitul, influența și legitimitatea. Totuși, în noul climat global, încrederea publică devine o resursă la fel de valoroasă ca și datele în sine. O companie care pierde încrederea consumatorilor își pierde implicit și accesul la fluxurile de informație care o hrănesc. Din această perspectivă, dilema fundamentală a capitalismului digital este cum să reconcilieze *rentabilitatea datelor* cu *responsabilitatea etică*.

Al treilea cerc este cel al *statelor membre* ale Uniunii Europene. Puterea lor tradițională de reglementare este erodată de transnaționalitatea infrastructurilor digitale. Confruntate cu hegemonia tehnologică americană și cu modelul de control cibernetic chinezesc, statele europene caută în cadrul Uniunii Europene o formă de *suveranitate colectivă*, bazată pe standarde juridice comune și pe capacitatea de negociere în fața giganților tehnologici. Astfel, UE devine un laborator geopolitic în care se testează posibilitatea unei „autonomii digitale democratice” – o formă de putere care să combine protecția drepturilor individuale cu competitivitatea tehnologică.

Împreună, aceste trei cercuri nu formează o ierarhie rigidă, ci un sistem interdependent: cetățeanul depinde de infrastructurile corporative, companiile depind de încrederea publică și de reglementarea statelor, iar statele depind de loialitatea și cooperarea cetățenilor într-un spațiu digital comun. În fond, noua cartografie a puterii nu mai delimitează teritorii, ci relații de interdependență cognitivă și morală, în care puterea nu se exercită doar prin forță sau bani, ci prin controlul sensului, al vizibilității și al fluxurilor informaționale. Astfel, con-

flictul dintre globalizare și autonomie digitală nu este doar o problemă economică, ci o luptă pentru *redefinirea libertății (concept politic și metafizic) în epoca algoritmică* – o libertate care nu mai înseamnă absența constrângerilor, ci capacitatea de a înțelege și de a decide în mod conștient în interiorul rețelelor care ne formează realitatea.

*Suveranitatea digitală a statelor membre:
protejarea autonomiei tehnologice și a spațiului democratic*

Deși suveranitatea digitală s-a impus în discursul european drept o soluție strategică pentru protejarea autonomiei tehnologice și a spațiului democratic, conceptul prezintă limite structurale care îi complică implementarea.

În primul rând, suveranitatea digitală riscă să preia în mod necritic vocabularul suveranității clasice, bazată pe control teritorial și monopol decizional, într-un domeniu – cel digital – în care arhitectura tehnologică nu respectă logica statelor-națiune. Infrastructurile digitale, rețelele de date și platformele sunt prin definiție transnaționale, operate de actori privați globali, iar fluxurile informaționale se sustrag cadrului juridic asociat modelului westfalian⁴⁰ al suveranității statale.

Puterea în era digitală, așa cum remarcă Anu Bradford⁴¹ și Joseph S. Nye⁴², este din ce în ce mai mult definită de structuri centrate pe rețea, mai degrabă decât de delimitări teritoriale. Această formă de putere se exercită prin crearea și controlul standardelor de interoperabilitate și al infrastructurilor digitale, permițând actorilor să stabilească regulile în spațiile tehnologice globale, indiferent de granițele tradiționale. În consecință, ambiția Uniunii Europene de a „recupera suveranitatea” în domeniile digitale transnaționale expune o tensiune inerentă între obiectivele sale politice și dinamica materială a guvernantei digitale, unde autoritatea este dispersată între platformele tehnice, lanțurile de aprovizionare globale și instituțiile de stabilire a standardelor.

Mai mult, conceptul de suveranitate digitală se caracterizează printr-o ambiguitate normativă considerabilă, ceea ce complică utilizarea sa în

⁴⁰ Termenul „suveranitate westfaliană” trimite la modelul de organizare statală consacrat de Pacea de la Westfalia (1648), care stabilește principiile autonomiei politice, neintervenției și egalității juridice între state – fundamentul sistemului internațional modern.

⁴¹ Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020.

⁴² Joseph S. Nye, *The Future of Power*, PublicAffairs Publishing House, New York, 2011.

construcția de politici publice. El încapsulează două traiectorii potențial divergente: pe de o parte, poate servi drept proiect pentru *emanipare democratică* – prioritizând angajamente liberale precum protecția datelor, guvernanta etică și constrângerea Big Tech; pe de altă parte, cercetători critici precum Laura DeNardis⁴³ avertizează că apelurile la suveranitate pot legitima, de asemenea, practici autoritare, inclusiv cenzura, supravegherea și *controlul centralizat al informațiilor*. Această dublă semnificație reflectă un context de reglementare în interiorul UE destul de problematic, întrucât retorica protejării autonomiei digitale ar putea fi adoptată și de diverse regimuri politice autoritare, atât în scopuri progresiste, cât și represive.

Uniunea Europeană se află, astfel, într-o poziție delicată. Trebuie să dezvolte mecanisme robuste de autonomie tehnologică fără a reproduce logica „suveranității digitale iliberale”⁴⁴ promovată de China și Rusia. Riscul este acela ca, în numele protecției cetățeanului, statul să dobândească o putere disproporționată asupra fluxurilor de date, generând un dezechilibru între securitate și libertate.

O a treia limită este legată de fezabilitatea tehnologică și economică a proiectului. Suveranitatea digitală presupune nu doar reglementare, ci și capacitatea de a produce infrastructuri „de înlocuire”: *cloud european*, lanțuri de aprovizionare independente, semiconductori, platforme digitale competitive, inteligență artificială proprie. După cum subliniază Dan Ciuriak⁴⁵ și Luciano Floridi⁴⁶, Europa operează într-un

⁴³ Laura DeNardis, *The Internet in Everything: Freedom and Security in a World with No Off Switch*, Yale University Press, 2020.

⁴⁴ Logica „suveranității digitale iliberale” promovată de China și Rusia se referă la un model de guvernanta a internetului centrat pe stat, în care autoritatea politică este exercitată prin mecanisme puternice de control tehnic și reglementare asupra infrastructurii digitale, a conținutului și a fluxurilor de date. În aceste sisteme, suveranitatea digitală este asociată în principal cu securitatea informațională, reglementarea conținutului și controlul național asupra spațiului cibernetic – adesea prezentate ca instrumente de apărare a intereselor naționale și de rezistență la influențe externe. Totuși, această abordare implică măsuri juridice și tehnologice de cenzură, supraveghere și reprimare a disidenței, susținând o normă de tip „suveranitate cibernetică” care înlocuiește guvernanta deschisă cu modele interguvernamentale și frontiere digitale consolidate. Această logică este codificată în acorduri bilaterale și multilaterale, precum și în strategii promovate prin organisme precum Organizația de Cooperare de la Shanghai, și este în general considerată o provocare la adresa principiilor liber-democratice privind deschiderea online, drepturile omului și interoperabilitatea globală.

⁴⁵ Dan Ciuriak, „From Gatekeeper to Gameplayer: Reclaiming Europe’s Strategic Relevance in the Data-Driven Age”, *Policy Paper no. 3*, IE University Centre for the Governance of Change, 2021.

⁴⁶ Luciano Floridi, „The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU”, *Philosophy & Technology*, vol. 35, no. 1, 2022.

context de decalaj tehnologic structural față de Statele Unite și China. Fără investiții masive, politici industriale coordonate și parteneriate strategice, suveranitatea digitală riscă să rămână un proiect normativ fără fundament tehnico-economic. Paradoxul este că, în încercarea de a-și reduce dependența, Uniunea Europeană poate ajunge să creeze noi dependențe – față de furnizori asiatici de hardware, față de platforme americane de cloud sau față de tehnologii open-source dezvoltate în exteriorul spațiului comunitar.

În fine, există o limită conceptuală mai profundă: suveranitatea digitală presupune ideea că autonomia poate fi reconstruită într-un sistem global hiperinterdependent. Dar, într-o economie a datelor și a standardelor, autonomia absolută este iluzorie; ceea ce pot urmări statele membre ale UE este o *autonomie funcțională*, negociată prin alianțe, standarde comune și interdependențe gestionate. În acest sens, Helga Nowotny⁴⁷ subliniază că Europa trebuie să regândească suveranitatea nu prin separarea de restul lumii, ci prin *capacitatea de a participa în mod suveran la guvernarea globală a tehnologiei*, modelând regulile, nu izolându-se de ele. În absența acestei viziuni, suveranitatea digitală riscă să devină un concept defensiv, reacționar, incapabil să influențeze ordinea tehnologică globală.

Suveranitatea digitală – de la nivelul Uniunii Europene și la cel al statelor membre

Relația dintre suveranitatea digitală la nivelul Uniunii Europene și suveranitatea digitală a statelor membre este una fundamental paradoxală: ele se revendică din aceeași nevoie – protejarea autonomiei într-un ecosistem tehnologic global dominat de actori extracomunitari –, dar se exprimă în registre diferite ale puterii. Această dinamică creează un câmp conceptual în care suveranitatea devine atât proiect european, cât și proiect național, dar niciodată în termeni simetrici. De fapt, ceea ce numim suveranitate digitală se divide în două dimensiuni complementare: suveranitatea tehnologică a Uniunii ca actor geopolitic și suveranitatea informațională a statelor ca actori constituționali.

La nivelul Uniunii Europene, suveranitatea digitală se configurează ca autonomie strategică externă: capacitatea de a stabili standarde glo-

⁴⁷ Helga Nowotny, *In AI We Trust: Power, Illusion and Control of Predictive Algorithms*, Polity Press, 2021.

bale, de a controla infrastructuri critice transnaționale (cloud european, spații de date, inteligență artificială) și de a reduce dependențele structurale față de tehnologiile americane și chineze.

Aici se înscriu inițiative precum *GDPR*, *AI Act*, *Chips Act*⁴⁸, *Data Governance Act*, *Digital Services Act* și proiectele de cloud federat (*Gaia-X*)⁴⁹. UE acționează ca un regulator geopolitic, încercând să impună o ordine digitală compatibilă cu valorile sale democratice și să recupereze puterea normativă într-o lume tehnologică dominată de alte centre civilizaționale. Suveranitatea digitală europeană este, așadar, un proiect extern, orientat către competiția pentru influență globală, controlul standardelor și protecția intereselor colective ale Uniunii.

În schimb, la nivelul statelor membre, suveranitatea digitală capătă un sens mult mai intern, centrat pe protecția ecosistemului informațional național, pe securitatea datelor publice și pe reziliența societății în fața operațiunilor psihologice și a manipulării digitale. Aici apar mecanisme precum: structuri de combatere a dezinformării (CTHH în Cehia⁵⁰,

⁴⁸ Legea europeană privind cipurile, adoptată în septembrie 2023, este un cadru de reglementare creat pentru a consolida ecosistemul semiconducătorilor, a spori poziția de lider tehnologic și a crește cota UE în producția globală de cipuri la 20% până în 2030. Cei trei piloni ai săi includ: (1) Inițiativa „Cipuri pentru Europa”, care sprijină cercetarea, proiectarea, liniile pilot și centrele de competență; (2) mecanisme de stimulare a investițiilor publice și private în unități de producție și turnătorii deschise în UE, acordând statutul de „primă de acest fel” și acces simplificat; și (3) un mecanism de coordonare a crizelor prin intermediul Consiliului European al Semiconducătorilor, care monitorizează oferta, prognozează cererea și implementează măsuri de urgență. Legea combină finanțarea UE, a statelor membre și a sectorului privat, abordează deficitul de competențe și prevede ajutoare de stat în anumite condiții, vizând asigurarea rezilienței lanțului de aprovizionare, reducerea dependenței de furnizorii externi și promovarea suveranității în microelectronică.

⁴⁹ *Gaia-X* este un proiect european de infrastructură cloud federată lansat în 2020 pentru a promova schimbul de date securizat, interoperabil și suveran în întreaga UE. În loc să ofere un singur cloud centralizat, *Gaia-X* stabilește un ecosistem transparent care leagă mai mulți furnizori de servicii cloud și utilizatori prin standarde deschise, cadre de conformitate și mecanisme federate de identitate și încredere. Obiectivele sale principale sunt de a consolida suveranitatea digitală europeană, de a asigura portabilitatea și confidențialitatea datelor conforme cu *GDPR* și de a permite „spații de date” sectoriale pentru inovare în domenii precum sănătatea, energia și mobilitatea. Inițiativa este condusă de Franța și Germania, implică actori publici și privați din întreaga Europă și urmărește să contracareze dominația străină a cloudului prin integrarea valorilor europene de transparență, reversibilitate și procesare securizată în serviciile cloud.

⁵⁰ CTHH – Centre Against Terrorism and Hybrid Threats (rom. Centrul împotriva Terorismului și Amenințărilor Hibrice) este unitatea specializată creată în 2016 în cadrul Ministerului de Interne al Republicii Ceha, cu misiunea de a monitoriza amenințările hibride, dezinformarea și ingerințele străine. Centrul realizează analize operative, coordonează răspunsurile instituționale și comunicarea publică și funcționează ca nod interministerial pentru gestionarea riscurilor informaționale.

STRATCOM în Estonia⁵¹), politici de protecție a infrastructurilor critice, strategii de securitate cibernetică, sisteme de alertă timpurie pentru ingerințe externe sau programe masive de alfabetizare media. Statele membre se ocupă astfel de frontiera cognitivă internă, în timp ce UE încearcă să reconstruiască frontiera tehnologică externă.

Această distribuție a responsabilităților generează o arhitectură hibridă și inovatoare: UE furnizează infrastructura de suveranitate, iar statele furnizează cultura de suveranitate. Bruxelles-ul negociază standarde globale, reglementează platformele și creează ecosisteme tehnologice comune, în timp ce capitalele europene se ocupă de traducerea acestor standarde în realitatea societală internă: educație, securitate, reziliență, infrastructuri administrative. Cu alte cuvinte, Uniunea construiește o „suveranitate tehnică”, iar statele construiesc o „suveranitate civică”.

Totuși, între cele două planuri există și o tensiune structurală. UE pretinde un rol de „suveran digital” în virtutea naturii transnaționale a tehnologiei moderne, dar statele rămân deținătorii legitimi ai suveranității politice și ai responsabilităților constituționale privind securitatea internă. De aici apar fricțiuni: unele state percep suveranitatea digitală europeană ca pe o transferare excesivă de competențe (de ex. în domeniul datelor industriale sau al cloudului), iar Bruxelles-ul percepe abordările strict naționale ca pe obstacole în construirea unui bloc tehnologic coerent, capabil să concureze global cu actori performanți precum Statele Unite sau China. Astfel, se conturează un paradox: suveranitatea digitală europeană nu poate exista fără suveranitatea digitală a statelor membre, iar suveranitatea digitală națională nu mai poate supraviețui fără infrastructura europeană comună.

În acest sens, suveranitatea digitală la nivel european și cea la nivel național trebuie înțelese ca două forme ale aceluiași univers politic. Uniunea Europeană oferă cadrul normativ, capacitatea de negociere globală și infrastructura strategică; statele ei membre oferă mecanismele de reziliență internă, cultura civică și legitimitatea democratică. Într-o lume în care puterea se exercită prin algoritmi, platforme și date, suveranitatea devine prin definiție distribuită, nu centralizată: nici UE

⁵¹ *STRATCOM Division / STRATCOM Task Force* din Estonia este structura integrată în cadrul Ministerului Apărării, responsabilă de monitorizarea campaniilor informaționale ostile, contracararea narațiunilor pro-Kremlin și consolidarea comunicării strategice a statului. Unitatea combină investigații de tip tehnologic cu evaluări de securitate și cu programe de reziliență societală. Este considerată una dintre cele mai avansate capacități de apărare cognitivă din Europa.

și nici statele membre nu pot pretinde monopolul asupra acestei noțiuni, ci doar coproducerea ei.

Prin urmare, relația dintre cele două niveluri nu este una de subordonare, ci una de coevoluție: suveranitatea digitală europeană se sprijină pe robustețea statelor membre, iar suveranitatea digitală națională se sprijină pe capacitatea Europei de a acționa ca bloc geopolitic într-o lume a competițiilor tehnologice sistemice. Această interdependență reconfigurează însăși natura suveranității în secolul XXI: ea nu mai este control exclusiv, ci capacitatea de a modela relații, a negocia standarde și a exercita influență în rețele care depășesc granițele tradiționale ale statului.

Concluzii

Europa se află în fața unei transformări a paradigmei de securitate, în care combaterea dezinformării și consolidarea suveranității digitale trebuie înțelese nu ca domenii sectoriale, ci ca două dimensiuni fundamentale ale unui proiect politic integrat: *refacerea autonomiei europene într-un ecosistem digital global* aflat în continuă accelerare. Războiul cognitiv, proliferarea operațiunilor informaționale ostile și dependențele sistemice față de infrastructuri tehnologice noneuropene au dezvăluit limitele modelului tradițional de securitate și ale instrumentelor normative ale Uniunii Europene. În fața acestor mutații, devine evident că Europa nu poate apăra democrația doar prin reglementări sau prin mecanisme reactive; are nevoie de o reconstrucție conceptuală a suveranității în epoca rețelelor, algoritmilor și interdependențelor tehnologice profunde.

Dacă dezinformarea afectează capacitatea colectivităților de a percepe și interpreta realitatea, suveranitatea digitală afectează capacitatea instituțiilor europene de a modela ecosistemul în care această percepție se formează. Cele două sfere – cognitivă și tehnologică – converg într-o frontieră conceptuală comună: aceea a *autonomiei europene de decizie și discernământ*. Studiul a evidențiat faptul că protecția spațiului informațional nu poate fi separată de protecția infrastructurii digitale care găzduiește acest spațiu, la fel cum arhitecturile tehnologice nu pot fi cu adevărat democratice în absența unor cetățeni dotați cu capacitate critică și imunitate cognitivă. În acest sens, securitatea informațională și suveranitatea digitală nu reprezintă două seturi independente de politici, ci două fețe ale aceluiași imperativ civilizațional:

capacitatea Europei de a rămâne un actor suveran într-o lume în care puterea se exercită tot mai mult prin controlul datelor, al infrastructurilor și al ecologiilor cognitive.

Totodată, observăm încă existența unor paradoxuri structurale: Europa caută autonomie într-o lume interdependentă; construiește suveranitate digitală în infrastructuri dominate de actori extracomunitari; susține un model normativ ambițios în absența unei baze tehnologice pe măsura acestei ambiții; și încearcă să protejeze drepturile fundamentale într-un ecosistem în care protecția datelor poate intra în tensiune cu dinamica inovării. Aceste paradoxuri nu anulează proiectul european, dar îi conferă o complexitate inevitabilă, obligându-l la o reconceptualizare continuă a propriilor obiective. Ele arată că suveranitatea europeană nu poate fi înțeleasă ca o revenire la modelul westfalic al controlului exclusiv, ci ca o formă de suveranitate relațională, adaptativă și colaborativă, articulată în interiorul ansamblului de interdependențe digitale, nu în afara lor.

În lumina acestor constatări, provocarea fundamentală pentru Uniunea Europeană nu este doar să reglementeze, să protejeze sau să reacționeze, ci să își redefinească rolul ca arhitect al ordinii digitale globale. Combaterea dezinformării și autonomia tehnologică sunt, în fapt, instrumente ale unei ambiții politice mai largi: aceea de a menține un spațiu european al raționalității, pluralismului și demnității umane într-o eră dominată de algoritmi, de supraveghere economică, de hegemonii digitale și competiție geopolitică acutizată. Suveranitatea, în această nouă paradigmă, devine capacitatea de a modela interdependențele, nu de a le refuza; capacitatea de a stabili standarde, nu doar de a le respecta; capacitatea de a proteja autonomia cognitivă a cetățeanului, nu doar de a securiza infrastructura tehnologică.

Prin urmare, viitorul Europei depinde de felul în care va reuși să articuleze aceste două dimensiuni – cognitivă și tehnologică – într-un proiect coerent, capabil să îmbine valorile democratice cu exigențele securității, pluralismul cu reziliența, interdependența globală cu autonomia strategică. Suveranitatea digitală și combaterea dezinformării nu sunt finalități în sine, ci mijloace prin care Europa încearcă să își păstreze capacitatea de a decide, de a judeca și de a acționa în propriile condiții. Iar în această încercare stă însăși continuitatea proiectului european ca spațiu de libertate, raționalitate și autodeterminare într-un secol marcat de turbulență tehnologică și competiții narative fără precedent.

BIBLIOGRAFIE

- Atkinson, R., „Cognitive Sovereignty and Neurocomputational Harm in Predictive Digital Platforms“, *Ethics and Information Technology*, vol. 27, nr. 66, 2025, pp. 1-19.
- Balzacq, T., *Securitization Theory: How Security Problems Emerge and Dissolve*, Abingdon, Oxfordshire, Routledge, 2010.
- Basch, C. E., G. C. Hillyer, Z. C. Meleo-Erwin și E. A. Zagnit, „YouTube Videos and Informed Decision-Making About COVID-19 Vaccination: Successive Sampling Study“, *JMIR Public Health and Surveillance*, vol. 7, nr. 5, 2021, pp. 1-8.
- Bayer, J., „Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States“, *European Parliament Think Tank*, Brussels, 2019.
- Beck, U., *Risk society: Towards a new modernity*, Sage Publications, London, 1992.
- Benkler, Y., R. Faris și H. Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, Oxford, Oxford University Press, 2018.
- Bennett, W. L. și S. Livingston, „The disinformation order: Disruptive communication and the decline of democratic institutions“, *European Journal of Communication*, vol. 33, nr. 2, 2018, pp. 122-139.
- Bertolini, A., F. Episcopo și N.-A. Cherciu, „Liability of online platforms“, *European Parliamentary Research Service*, Brussels, 2021.
- Bradford, A., *The Brussels Effect: How the European Union Rules the World*, Oxford, Oxford University Press, 2020.
- Brasseur, C., V. Pachtă și C. Grigolo, „The EU’s External Democracy Action in a New Geopolitical Reality“, *International Idea*, Stockholm, 2023.
- Bruns, A. & B. J., „Truth in Fake News: How Disinformation Laws Are Reframing the Concepts of Truth and Accuracy on Digital Platforms“, *Information, Communication & Society*, vol. 25, nr. 10, 2022, pp. 1350-1366.
- Buzan, B. și O. Wæver, *Regions and Powers: The Structure of International Security*, Cambridge, Cambridge University Press, 2003.
- Buzan, B., O. Wæver și J. de Wilde, *Security: A New Framework for Analysis*, Boulder, Lynne Rienner Publishers, Colorado 1998.
- Buzan, B., *People, States and Fear: The National Security Problem in International Relations*, Brighton, UK, Harvester Wheatsheaf, 1983.
- Bygrave, L. A., „Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions“, in *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights*, Cambridge, Cambridge University Press, 2022, pp. 166-188.
- C. C. G. L. & M. F. Shao, „EUvsDisinfo: A Dataset for Multilingual Detection of Pro-Kremlin Disinformation“, arXiv., 2024.
- Casero-Ripollés, A., J. Tuñón și L. Bouza-García, „The European approach to online disinformation: geopolitical and regulatory dissonance“, *Humanities and Social Sciences Communications*, 2023, pp. 1-10.
- Chiarella, M. L., „Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment“, *Athens Journal of Law*, vol. 9, nr. 1, 2023, pp. 33-58.

- Ciuriak, D., „From Gatekeeper to Gameplayer: Reclaiming Europe’s Strategic Relevance in the Data-Driven Age“, *Centre for the Governance of Change*, Madrid, 2021.
- Cock Buning, M. De, „A multi-dimensional approach to disinformation: Report of the independent high level group on fake news and online disinformation“, *European Commission*, Brussels, 2018.
- Colliver, C., „Cracking the code: An evaluation of the EU code of practice on disinformation“, *Institute for Strategic Dialogue*, London, 2020.
- Conley, H. A. și J.-B. J. Vilmer, „Successfully Countering Russian Electoral Interference“ *Centre for Strategic and International Studies*, Washington, DC, 2018.
- Craufurd Smith, R., „Fake news, French Law and democratic legitimacy: lessons for the United Kingdom?“, *Journal of Media Law*, vol. 11, nr. 1, 2019, pp. 52-81.
- DeNardis, L., *The Internet in Everything: Freedom and Security in a World with No Off Switch*, London, Yale University Press, 2020.
- European Commission, „Assessment of the code of practice on disinformation – Achievements and areas for further improvement“, Brussels, 2020.
- Ferrara, E., „Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election“, arXiv, vol. 22, nr. 8, 2017, pp. 1-33.
- Floridi, L., „The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU“, *Philosophy & Technology*, vol. 35, nr. 1, 2021, pp. 1-11.
- GDI, „Ad-funded COVID-19 conspiracy sites: A look at the EU“, 23 February 2021 [Interactiv]. Available: <https://www.disinformationindex.org/blog/2021-2-23-ad-funded-covid-19-conspiracy-sites-a-look-at-the-eu/>.
- Helm, R. K. și H. Nasu, „Regulatory responses to ‘fake news’ and freedom of expression: Normative and empirical evaluation“, *Human Rights Law Review*, vol. 21, nr. 2, 2021, pp. 302-328.
- Jourová, V. și T. Breton, „Code of Practice on disinformation“, 1 October 2021 [Interactiv]. Available: <https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation>.
- Kalniete, S. și T. Pildegoviēs, „Strengthening the EU’s resilience to hybrid threats“, *European View*, vol. 20, nr. 1, 2021, pp. 23-33.
- Kuczerawy, A., „Fighting Online Disinformation: Did the EU Code of Practice Forget about Freedom of Expression?“, 24 September 2019 [Interactiv]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3453732.
- Linville, D. L. și P. L. Warren, „Troll Factories: How Russian Influence Operations Work and Their Impact on Social Media Discourse“, *Political Communication*, vol. 37, nr. 4, 2020, pp. 447-467.
- Madiega, T., „Reform of the EU liability regime for online intermediaries: Background on the forthcoming digital services act“, *European Parliamentary Research Service*, Brussels, 2020.
- Martin, É., J. Nocetti și C. Tonon, „Europe: Subject or Object in the Geopolitics of Data?“, *Institut français des relations internationales (Ifri)*, Paris, 2018.
- Marwick A. și R. Lewis, „Media manipulation and disinformation online“, *Data & Society Research Institute*, New York, 2017.
- Meyer, T., C. T. Marsden și I. Brown, „Regulating Internet Content with Technology: Analysis of Policy Initiatives Relevant to Illegal Content and Disinformation Online in the European Union“, in *Disinformation and Digital Media as a Challenge for Democracy*, Cambridge, Cambridge University Press, 2021, pp. 309-326.

- Nowotny, H., *In AI We Trust: Power, Illusion and Control of Predictive Algorithms*, Cambridge, Polity Press, 2021.
- Nye, J. S., *The Future of Power*, New York, PublicAffairs Publishing House, 2011.
- O'Hara, K. și W. Hall, *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*, Oxford, Oxford University Press, 2021.
- Pierri, F., A. Artoni și S. Ceri, „Investigating Italian disinformation spreading on Twitter in the context of 2019 European elections“, *PLOS One Journal*, 2019, pp. 1-23.
- Polyakova, A. și S. P. Boyer, „The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition“, *Brookings Institution*, Washington, D.C., 2018.
- Shattock, E., „Self-regulation 2.0? A critical reflection of the European fight against disinformation“, *Misinformation Review*, vol. 2, nr. 3, 2021, pp. 1-8.
- Singer, P. W. și E. T. Brooking, *Like War: The weaponization of social media*, Boston, Massachusetts, Houghton Mifflin Harcourt, 2018.
- Sperling, J. și M. Webber, „NATO and the Ukraine Crisis: Collective Securitisation“, *European Journal of International Security*, vol. 2, nr. 1, 2017, pp. 19-46.
- Sperling, J. și M. Webber, „The European Union: Security Governance and Collective Securitisation“, în *Collective Securitisation and Security Governance in the European Union*, Abingdon, Routledge, 2019, pp. 228-260.
- Stocchetti, M., „(Dis)Information, neoliberalism and the strenght of democracy in the digital age“, în *Disinformation and digital media as a challenge for democracy*, Cambridge, Cambridge University Press, 2021, pp. 47-80.
- Wæver, O., „Securitization and Desecuritization“, în *On Security*, New York, Columbia University Press, 1995, pp. 46-87.
- Wagnsson, C., „What is at stake in the information sphere? Anxieties about malign information influence among ordinary Swedes“, *European Security*, vol. 29, nr. 4, 2020, pp. 397-415.
- Zuiderveen Borgesius, F. J., J. Möller și S. Kruikemeier, „Online Political Microtargeting: Promises and Threats for Democracy“, *Utrecht Law Review*, 14(1), 82-96. <https://doi.org/10.18352/ulr.420>, vol. 14, nr. 1, 2018, pp. 82-96.