

# Propunere de cadru pentru definirea și clasificarea **comportamentului inautentic coordonat (Coordinated Inauthentic Behaviour - CIB)** în contextul DSA

---

Acest document este o prezentare simplă a termenilor legați de comportamentului inautentic coordonat (**Coordinated Inauthentic Behaviour - CIB**), văzut în special în contextul [Regulamentului \(UE\) 2022/2065](#)<sup>1</sup>. Documentul este rezultatul unui proces de consultare și discuții informale pe această temă pe baza unui text propus de **ApTI (coordonat de Andrei Petre)** și a unor membri ai societății civile, cum ar fi **ExpertForum, ActiveWatch și Funky Citizens**. **ANCOM** a prezentat liniile generale ale [Regulamentului \(UE\) 2022/2065](#).

---

Documentul este destinat în special ca material de folosit în relația cu:

- **instituții publice** cu atribuții de reglementare în domenii adiacente, pentru care fenomenul CIB nu reprezintă un obiect de activitate curent;
- **alți actori interesați**, în special organizații neguvernamentale care monitorizează conținut ilegal sau dăunător online și jurnaliști care realizează investigații aferente, pentru a face distincția între incidente punctuale (care pot fi raportate individual) și campanii coordonate (care necesită o analiză mai aprofundată).

**Scopul documentului** este să propună un set de explicații și definiții agreate comun despre CIB, pentru a oferi o imagine generală a fenomenului, utilă în a înțelege riscurile de nivel macro (și nu de cazuri punctuale, individuale) ale folosirii unei infrastructuri care poate să promoveze CIB, dar și problemele specifice de identificare, clasificare (de ex. legal/ilegal) sau chiar folosire legală de metode de coordonare aparent similare.

Deși CIB apare cel mai des în context de dezinformare sau în contexte electorale ori politice, **propunerea noastră este să-l înțelegem într-un cadru mai larg și neutru din punctul de vedere al conținutului**, tocmai pentru a putea identifica caracteristicile generale ale acestui tip de fenomen. În acest context, merită să

---

<sup>1</sup> Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE

subliniem că infrastructura tehnică care permite un CIB poate fi folosită în multiple domenii și, uneori, chiar furnizată ca serviciu (de ex. cumpărare de like-uri).

În același timp, trebuie să clarificăm că **CIB nu este egal cu „conținut ilegal”** (deși, în cele mai multe cazuri, poate fi folosit în scopuri ilicite), fiind suficiente exemple de CIB (sau ceea ce pare a fi) care sunt *de facto* proiecte cu un scop legal, precum activități ale utilizatorilor normali care generează indicatori de creștere organică. Mai mult, actorii coordonatori pot beneficia de amplificarea organică din partea unor utilizatori reali care, acționând din convingere proprie și total în afara coordonării, conferă campaniei o aparență de autenticitate și îngreunează identificarea comportamentului inautentic.

În același timp, este adevărat că, în cele mai multe cazuri, activitatea de tip CIB poate **să urmărească un scop ilegal** sau să fie în sine o activitate ilegală, și de cele mai multe ori, poate încălca termenii și condițiile platformelor.

E important de menționat că, în majoritatea cazurilor, campaniile coordonate inautentic pot fi confundate cu cele coordonate organic în scopuri legitime (activism online, marketing), deoarece se manifestă în feluri similare (de exemplu: o rețea de utilizatori care distribuie în masă același conținut).

În același timp, considerăm că este necesar să existe discuții în spațiul public despre felurile în care putem demarca mai bine campaniile organizate legitim de cele care au un scop mascat, respectiv cele derulate de grupuri care pretind că reprezintă utilizatori independenți, dar care sunt controlate centralizat sau automatizat.

## A. Definiții

Chiar dacă nu există o definiție unanim acceptată pentru comportamentul inautentic coordonat, elementele comune se referă la exploatarea serviciilor furnizate de platforme pentru modificarea sintetică a vizibilității în mediul online. O astfel de influențare a popularității poate să fie instrumentalizată în diverse moduri de actori răuvoitori sau de orice fel de entități care pot transforma vizibilitatea online în beneficii financiare sau de orice altă natură.

Conform actelor normative emise de instituții europene, respectiv a regulamentelor interne ale platformelor online, există următoarele definiții care fac referire direct sau indirect la **Comportamentul Inautentic Coordonat**.

**DSA:** nu menționează direct termenul de CIB, dar vorbește despre responsabilitatea platformelor de a monitoriza **riscuri sistemice ale algoritmilor** (inclusiv cele care au „efecte negative reale sau previzibile asupra discursului civic și a proceselor electorale, precum și a siguranței publice”<sup>2</sup>) cauzate „prin utilizarea neautentică a serviciului, precum crearea de conturi false, utilizarea botilor sau utilizarea înșelătoare a unui serviciu și prin alte comportamente automatizate sau parțial automatizate, care pot conduce la diseminarea rapidă și pe scară largă către public a informațiilor care constituie conținut ilegal sau sunt incompatibile cu condițiile generale de utilizare ale unei platforme online sau ale unui motor de căutare online și care alimentează campaniile de dezinformare.”

Orientările Comisiei către furnizorii de platforme online foarte mari și de motoare de căutare online foarte mari privind atenuarea riscurilor sistemice la adresa proceselor electorale în temeiul articolului 35 alineatul (3) din Regulamentul (UE) 2022/2065<sup>3</sup>, îndeosebi pct. 27 lit. h) din secțiunea 3.2.1 - „Măsuri de atenuare a riscurilor”

**Codul de conduită privind dezinformarea:** Instrument de autoreglementare pentru conformitatea cu obligații din cadrul DSA, care definește în cadrul angajamentului **14 comportamente manipulative inadmisibile**, menționând printre acestea: crearea și utilizarea conturilor false, preluarea conturilor și amplificarea prin boti, crearea conturilor care participă la **comportament inautentic coordonat (CIB)**, precum și achiziționarea de interacțiuni false (*fake engagement*) drept comportamente manipulative inadmisibile pe platformele online. Trebuie subliniat că acest Cod este asumat în mod voluntar de unele platforme (vezi [lista](#)

---

<sup>2</sup> Art 34 (1) c) din textul DSA

<sup>3</sup> [https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=OJ:C\\_202403014](https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=OJ:C_202403014)

[oficială pe site-ul dedicat](#)), iar aplicarea angajamentelor se face în conformitate cu măsurile precizate în Cod.

**[EEAS \(European Union External Action Service\)](#):** Conform definiției STRATCOM-ului EEAS, CIB presupune eforturi organizate, deliberate și manipulative de a induce în eroare publicul prin utilizarea unei rețele de conturi și pagini care colaborează pentru a difuza anumite mesaje sau a desfășura acțiuni specifice, ascunzând în același timp natura acestora. Operațiunile CIB se bazează pe utilizarea la scară largă a unor tactici și tehnici manipulative.

**[Eu Disinfo Lab](#):** o strategie de comunicare manipulativă care distribuie și amplifică conținut într-un fel coordonat și non-organic, care se poate folosi de conturi autentice, false sau un mix.

**[Meta](#):** o rețea de entități inautentice coordonate de un individ/un grup de indivizi, care are scopul să înșele platforma, comunitatea, sau să evite sancțiuni pentru încălcarea „standardelor comunității”.

**[Google](#):** „comportament înșelător” care poate fi făcut de conturi care își ascund identitatea ca să înșele utilizatori.

**[TikTok](#):** rețea de conturi care lucrează împreună ca să înșele sistemul platformei, utilizatorii și să influențeze discursul public.

## B. Moduri de instrumentalizare a comportamentului inautentic coordonat

### campanii de dezinformare și interferență statală (FIMI)

În Moldova, multiple rețele de boți care au generat conținut preponderent AI, au creat peste [10,000 de postări în timpul campaniei parlamentare din 2025 pe platforma TikTok](#), dezvoltând [rețele similare și pe Facebook](#).

[Rețeaua Portal Kombat](#) și [Operațiunea „Doppelgänger”](#): o rețea de site-uri clonate și boți care răspândesc și promovează dezinformare și narative anti-occidentale pe rețelele sociale cu scopul de a reduce încrederea în instituțiile democratice, de a crea haos și de a polua spațiul informațional.

**NOTĂ:** Din cauza felului în care traficul din mediul online poate genera profit prin intermediul reclamelor, actorii din spatele campaniilor de dezinformare pot fi neafiliați vreunui stat și pot avea exclusiv interese financiare. [Un exemplu notoriu](#) este reprezentat de fermele de boți din Macedonia de Nord, care au răspândit conținut partizan politic în timpul prezidențialelor din SUA din 2016 și 2020. Rețeaua se baza pe o strategie de marketing care genera profit ținând publicul republican cu articole false și polarizante.

### fraudă financiară

În România, [escrocheriile](#) de tip „[trading-scam](#)”, s-au folosit de site-uri clonate, deepfake-uri, și de rețele de *boosting* pe rețelele sociale ca să înșele mai multe victime. Un mecanism similar a fost folosit de [o rețea de escroci](#) care promova suplimente alimentare ca „leacuri miraculoase” pentru boli cronice.

### promovare online

*Promovarea unor narațiuni politice, promovarea unor campanii de discreditație sau promovarea politicienilor*

În timpul campaniilor electorale, promovarea prin intermediul unor rețele inautentice a devenit din ce în ce mai populară. În timpul alegerilor prezidențiale din 2024 și mai 2025, [mai mulți politicieni din România](#) au beneficiat de astfel de promovare conform unor [investigații publice](#).

În afară de promovarea online a unor candidați politici, CIB este folosit și în [promovarea unor narațiuni de discreditare a jurnaliștilor](#). Acest comportament apare însă din ce în ce mai mult și în afara alegerilor, normalizând această formă de popularizare artificială.

## diminuarea vizibilității

[La începutul anului](#) 2026, mai multe organizații și publicații din Serbia au fost suspendate de Instagram. Organizațiile au acuzat că au fost atacate de zeci de mii de conturi false care au început să le urmărească pagina, iar asta a determinat sistemul de detecție al platformei să le elimine contul. [În Albania](#), publicația independentă Citizen Channel a fost atacată de o rețea care a formulat sute de raportări către Meta, în care acuzau încălcări a termenilor și condițiilor. Ca urmare, algoritmiile platformei au eliminat o mare parte din postările publicației.

În România, în timpul campaniei prezidențiale din mai 2025, mai mulți [candidați au avut zeci de mii de conturi inautentice pe propriile conturi oficiale, care urmăreau în masă candidații](#), interacționau sau distribuiau postările acestora. [O rețea de conturi false](#) a postat materiale pentru o campanie negativă (multe dintre ele plătite) și a publicat numeroase postări pe Facebook împotriva unor candidați. Unii dintre aceștia au acuzat tehnici de tipul *false flag operations*, adică anticampanie orchestrată de contracandidați care foloseau aceste conturi de CIB pentru a crea poluare informațională și a eroda campania reală a candidaților.

## C. Cadru de analiză pentru clasificarea campaniilor relevante

În baza unor criterii propuse de [Eu Disinfo Lab](#) și [IFTAS](#), dar și plecând de la premisa că CIB trebuie privit drept o tentativă de a manipula serviciile oferite de platformele online astfel încât vizibilitatea conținutului să fie redusă sau amplificată sintetic, propunem o schemă logică de analiză care se bazează pe mai multe criterii cumulative și pe mai multe întrebări ajutătoare

### Coordonare

#### Întrebarea 1: Există un grup de utilizatori care acționează coordonat?

Indicatori posibili:

- Conturi care răspândesc aceeași narativă;
- Conturi care folosesc aceleași hashtaguri, markere vizuale, cuvinte cheie.

Este important de menționat că, de cele mai multe ori, coordonarea în mediul online este făcută de utilizatori normali în scopuri legitime, fără diferențe semnificative față de coordonarea din mediul offline (proteste, flashmob-uri, inițiative civice).

#### Exemple

**1. Campanii politice** în care un partid își încurajează în mod transparent membrii și simpatizanții să posteze mesaje de susținere pentru un anumit candidat sau anumite pachete legislative.

**2. Campanii civice sau de activism cetățenesc** care presupun coordonarea în mediul online prin folosirea unor hashtaguri sau distribuirea unor fotografii, videoclipuri sau mesaje.

- În 2021, mai mulți utilizatori de pe platforma Reddit s-au coordonat să cumpere la bursă acțiuni ale companiei [GameStop](#);
- O campanie prin care utilizatorii români de pe Instagram, YouTube și Facebook s-au coordonat să posteze comentarii negative la postările influencerilor care promovau jocuri de noroc;

- Mai mulți utilizatori din mediul online care, în perioada scrutinelor electorale, își exprimă preferințele politice folosind un anumit hashtag sau promovând un partid sau un candidat.

## Înșelare

### Întrebarea 2: Campania coordonată pe care am identificat-o este una înșelătoare?

O campanie coordonată este înșelătoare atunci când are scopul de a amplifica artificial un anumit conținut, creând impresia **falsă** a unui interes ridicat în societate (like-uri, comentarii, *share*-uri, vizualizări, mesaje de susținere sau de descurajare) și împingând sintetic în agenda publică (sau încercând să restrângă) un subiect sau o informație.

La rândul său, ghidul de analiză realizat de Eu Disinfo Lab subliniază că un element cheie care face ca o coordonare în mediul online să fie inautentică constă în dorința de a disimula identitatea utilizatorilor care se coordonează, **pentru a le spori credibilitatea**. O disimulare a identității poate presupune o infrastructură automatizată care se bazează pe boți, dar și o rețea coordonată de oameni care încearcă să își ascundă o afiliere de partid, respectiv o rețea de influenceri care fac publicitate nemarcată.

Din cauza faptului că algoritmi de recomandare folosiți de rețelele sociale promovează conținutul cu care interacționează cât mai mulți oameni, rețelele automatizate sunt cele mai eficiente unelte pentru o campanie coordonată înșelătoare de succes (care ajunge la cât mai multe potențiale victime). Miza rețelor răuvoitoare este să simuleze un interes ridicat pentru ca un anumit conținut să fie promovat de algoritmi, dar și ca să îi convingă pe utilizatorii obișnuiți să adere la trenduri/mișcări care par legitime de mase mari de oameni.

Deocamdată, **automatizarea** este componenta cea mai comună și ușor de identificat atunci când analizăm o campanie de CIB, iar aceasta are următorii indicatori:

- Conturi care impersonează alte persoane;
- Tipar de postare care nu este realist sau care este sincronizat cu o grupare (postat cu frecvență ridicată; sau, de ex., conturi din Vietnam care interacționează cu conținut din România);
- Conturi anonime, fără informații personale;

- Conturi care folosesc fotografii generate cu AI;
- Conturi care interacționează (aprecieri, comentarii, distribuiri) în masă cu același tip de conținut;
- Metadate legate de postări (de ex. *timestamp*-ul postarilor);
- Conturi care au nume similare;
- Conturi create recent, care promovează același conținut.

E important de menționat că, pe măsură ce platformele online reușesc să implementeze sisteme menite să combată *rețelele de boți*, rețelele de CIB se adaptează și ajung să se folosească de modele de boți care, cu ajutorul modelelor AI, reușesc să copieze comportamente specifice umane (interacționează cu conținut divers, nu au activitate 24/7, mimează orele de odihnă, folosesc fotografii *deepfake*; ex.: [fermă de boți](#) din Vietnam care era operată cu ajutorul inteligenței artificiale).

De asemenea, mai există cazuri în care rețelele de CIB sunt compuse din persoane fizice care își folosesc conturile personale pentru a populariza sintetic un anumit conținut. (ex.: [o rețea](#) din Republica Moldova care racola mai multe persoane fizice și le instruia să răspândească dezinformare și propagandă politică).

Chiar și așa, din motive financiare și logistice, rețelele cu cel mai mare impact se vor folosi într-o oarecare măsură de automatizare. Așadar, putem concluziona că inexistența indicatorilor de automatizare nu e un factor determinant în analiza unei rețele de CIB, dar indică o **probabilitate scăzută**.

**NOTĂ:** În contextul în care rețelele care se folosesc de CIB încearcă să mimeze coordonarea organică, **este esențial ca autoritățile și părțile interesate să țină cont de riscul de a cenzura și limita activitatea utilizatorilor care, de bunăvoie, aleg să se coordoneze în mediul online.**

Putem vorbi despre campanii coordonate care au scopuri înșelătoare, dar care nu se bazează pe automatizare, în următoarele situații:

- Conturi care promovează un produs pe care pretind că l-au utilizat, dar care de fapt urmăresc o miză financiară (de ex. rețele de influenceri care fac publicitate mascată la un produs, conturi false care lasă recenzii în masă);
- Conturi ale unor membri de partid sau plătite de un partid politic care încearcă să își ascundă afilierea politică și care pretind că sunt utilizatori obișnuiți.

În ambele cazuri, observăm că avem de-a face cu utilizatori reali care nu înșeală disimulându-și identitatea (ca în cazul boților, care trebuie să lase impresia că

sunt oameni reali), ci ascunzându-și afilierea politică sau comercială tot cu scopul final de a avea mai multă credibilitate (publicitate mascată, recenzii false).

## Impact negativ

### Întrebarea 3: Care e scopul final urmărit de o grupare care se folosește de CIB?

Odată ce am stabilit că o rețea acționează coordonat, și încearcă să înșele alți utilizatori, ultimul pas este identificarea scopului final urmărit. Pentru a face acest lucru, este important să înțelegem că comportamentul inautentic coordonat este un **mijloc**, nu un scop/este **o unealtă folosită de o rețea** pentru a atinge un scop (*means to an end*).

### Exemple

- În cazul unei grupări de fraudă financiară, scopul pentru care se folosește de CIB este să ajungă la cât mai mulți potențiali cumpărători/investitori care să cumpere un produs sau un serviciu - **înșelăciune**;
- În cazul unei grupări politice, scopul este de a maximiza numărul de utilizatori care își pot face o părere pozitivă/negativă despre un anumit candidat politic. Un alt scop poate fi ascunderea unor subiecte delicate și importante de pe agenda publică. În această situație, maximizarea numărului de persoane influențate se poate face fie prin simpla amplificare a vizibilității unui conținut, fie prin folosirea unei rețele de conturi care să mimeze o nemulțumire/simpatie din societate - **propagandă politică mascată**;
- În cazul unei campanii de interferență statală, scopul este amplificarea unui conținut pentru a polua spațiul informațional sau pentru a reduce încrederea în instituțiile democratice - **acțiuni de tip FIMI (Foreign Information Manipulation and Interference)**;
- În cadrul campaniilor de marketing, CIB poate avea rolul de a promova un anumit produs - **publicitate nemarcată corespunzător**.

### Excepție

Există cazuri care ar trebui permise, atunci când cercetători sau jurnaliști se folosesc de rețele de conturi inautentice care acționează coordonat pe rețelele sociale cu scopul de a analiza algoritmi/a colecta date necesare cercetării.

## D. Observații generale și recomandări

Fiindcă este dificil să distingi între o coordonare autentică și o coordonare inautentică, mai ales că rețelele se pot folosi de oameni sau de boți care mimează comportamentul uman, o abordare eficientă în combaterea efectelor CIB constă în **identificarea infrastructurii care facilitează CIB, nu a nodurilor individuale dintr-o rețea**. Un exemplu de succes este [dosarul SIMCartel](#), în care Europol a destructurat o rețea de fraudă care opera [peste 49 de milioane de conturi false](#).

În același timp, este crucial ca autoritățile să se concentreze pe identificarea riscurilor sistemice (definite conform DSA) care ar permite existența unor astfel de campanii. Încă din 2025, [raportul Comitetului European pentru Servicii Digitale](#) menționa că CIB poate populariza sintetic un anumit conținut din cauza algoritmilor de recomandare de pe rețelele sociale, iar acest lucru reprezintă un risc sistemic care ar trebui să fie adresat prin intermediul DSA.

Așadar, **recomandarea generală principală este abordarea CIB dintr-o perspectivă de ansamblu, care se uită la riscurile sistemice ale platformelor** (definite conform DSA) care permit existența acestor operațiuni de tip CIB (indiferent de temă sau țară). În acest sens, este esențială înțelegerea și dovedirea fenomenului, dar și raportarea sa adecvata prin instrumentele DSA.

1. În cazul entităților ce vizează identificarea de conținut ilegal sau dăunător - dacă estimați (și pe baza analizei de mai sus) că este vorba de o campanie coordonată de tip CIB, **nu pierdeți resurse importante prin analiza punctuală a cazurilor individuale - ci axați-vă pe analiza macro**, urmărind efectul și intenția întregii campanii coordonate.
2. De cele mai multe ori **destructurarea unei rețele care coordonează o activitate ilegală ce implică CIB** - mai ales dacă include aspecte transnaționale - **se poate face doar în colaborare cu organele penale competente**, care sunt singurele ce pot avea acces legal la date informatice de la platformele online, care pot demonstra fără dubiu - inclusiv în cadrul unui proces penal - coordonarea activității ilegale.
3. **Analizele campaniilor CIB** ce afectează spațiul românesc - inclusiv tendințe, narative, tipologii, evoluții sau magnitudine - **sunt relativ disparate**. Recomandăm cercetătorilor interesați de subiect și autorităților publice relevante să se concentreze pe analiza mecanismelor sistemice prin care grupările se coordonează pentru a modifica sintetic vizibilitatea unui conținut și folosirea accesului la date conform art 40 DSA (pentru cercetătorii agreați), pentru maparea spațiului informațional românesc, astfel încât să înțeleagă fenomenul CIB în ansamblu.

4. În cazul propunerilor de revizuire de reglementări - cum ar fi, de exemplu, cele din zona electorală - **este important să fie incluse aspectele esențiale ale CIB** (coordonare, autenticitate, intenție malițioasă, impact) **în definițiile și/sau articolele** care includ **încălcarea legislației** (dacă e relevant) pentru a defini corect cazurile majore ce pot afecta procesele democratice ale societății.
5. Aplicarea în mod eficient a legislației naționale și europene privind finanțarea politică și publicitatea politică și sancționarea încălcărilor în mod disuasiv și proporțional. Este evident că aceste campanii organizate care includ CIB sunt realizate cu resurse financiare sau umane, de cele mai multe ori în mod ilegal. Astfel, trebuie să existe și o colaborare susținută între instituții care pot controla finanțarea politică (AEP), fluxurile financiare (ANAF) și care pot investiga încălcări ale legislației (Poliție, parchete, ONPCSB).