

Către: **PARLAMENTUL ROMÂNIEI, CAMERA DEPUTAȚILOR**

În atenția: **Doamnei Oana MURARIU, Secretar**

26 6b-8/339
07 09

Subiect: Răspuns la adresa nr. 6b-8/280/10.06.2026 privind întrebarea domnului deputat Sebastian Ioan BURDUJA cu nr. 5449A din 04.06.2026

Stimată doamnă Secretar,

Ca urmare a adresei Dvs. nr. 6b-8/280/10.06.2026, transmisă Autorității Naționale pentru Administrare și Reglementare în Comunicații (denumită în continuare ANCOM sau Autoritatea) și înregistrată la ANCOM cu nr. SC/14606/12.06.2026, prin care ne transmiteți întrebarea cu nr. 5449A din 04.06.2026 a domnului deputat Sebastian Ioan BURDUJA, având ca obiect *„Oportunitatea reglementării comportamentului inautentic coordonat și a conturilor automatizate pe platformele online, prin raportare la atribuțiile ANCOM de coordonator național al serviciilor digitale potrivit Legii nr. 50/2024 și Regulamentului (UE) 2022/2065”*, vă comunicăm următoarele:

Prin raportare la reperele cadrului legislativ aplicabil, credem că sunt utile o serie de informații preliminare care să sprijine identificarea punctelor de legătură dintre prevederile Regulamentului (UE) 2022/2065¹ (denumit în continuare *Regulamentul privind serviciile digitale* sau *DSA*) și modalitatea de adresare a situațiilor semnalate de dvs.

Tot cu titlu generic, amintim că pentru aplicarea DSA pe plan național a fost adoptată Legea nr. 50/2024². Potrivit art. 14 din Legea nr. 50/2024, Autoritatea are calitatea de coordonator al serviciilor digitale în România, având competențele stabilite prin dispozițiile art. 51 din Regulamentul privind serviciile digitale.

Din perspectiva sferei de reglementare din materia serviciilor digitale, apare important a fi precizat faptul că nici Regulamentul privind serviciile digitale și nici Legea nr. 50/2024 nu consacră ori nu definesc în mod expres noțiunea de *„comportament inautentic coordonat”* (Coordinated Inauthentic Behaviour – CIB) ca noțiune juridică autonomă.

Însă, după cum rezultă din dispozițiile art. 34 și art. 35 din Regulamentul privind serviciile digitale, referitoare la evaluarea și atenuarea riscurilor sistemice, interpretate în lumina considerentelor (84) și (85) ale aceluiași regulament, legiuitorul european are în vedere și situațiile în care serviciile furnizate de platformele online foarte mari (VLOPs) și de motoarele de căutare online foarte mari (VLOSEs) pot fi utilizate de către *destinatarii serviciului*³ într-o manieră neautentică, inclusiv prin crearea și utilizarea de conturi false, utilizarea sistemelor automatizate (boti) ori alte forme de comportament automatizat sau parțial automatizat susceptibile să influențeze artificial procesele de informare și dezbateră publică.

¹ 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.

² Legea nr. 50/2024 privind stabilirea unor măsuri pentru aplicarea Regulamentului (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, precum și pentru modificarea și completarea Legii nr. 365/2002 privind comerțul electronic.

³ Art. 3 lit. b) din DSA.

Astfel, potrivit art. 34 alin. (1) din DSA, furnizorii de VLOPs și VLOSEs au obligația de a identifica, analiza și evalua riscurile sistemice generate de proiectarea, funcționarea și utilizarea serviciilor lor, inclusiv riscurile care decurg din manipularea deliberată a serviciului, aspect detaliat în considerentele (84) și (85) ale regulamentului. În continuare, art. 35 din DSA instituie obligația adoptării unor măsuri rezonabile, proporționale și eficace pentru diminuarea riscurilor identificate în cadrul evaluării efectuate potrivit art. 34.

Prin urmare, DSA tratează aspectele semnalate mai sus - *comportamentul inautentic coordonat* - din perspectiva unor riscuri sistemice ce trebuie analizate de VLOPs și VLOSEs, în cadrul mecanismelor de evaluare și atenuare a riscurilor prevăzute de DSA.

În ceea ce privește obligațiile prevăzute la art. 34 și art. 35 din DSA, aplicabile furnizorilor de VLOPs și VLOSEs, competențele de supraveghere și asigurare a conformității sunt exercitate în conformitate cu mecanismul prevăzut de Regulamentul privind serviciile digitale, respectiv de Comisia Europeană și de *coordonatorul serviciilor digitale din țara de stabilire*⁴ al furnizorului în cauză. În practică, majoritatea furnizorilor de VLOPs și VLOSEs relevanți pentru piața românească, precum Meta, TikTok, X sau Google, sunt stabiliți în Irlanda, astfel încât competențele directe de supraveghere și intervenție revin autorității competente din respectivul stat membru, în cooperare cu Comisia Europeană.

În ceea ce privește situațiile referitoare la comportamentul inautentic coordonat aduse la cunoștința noastră, ANCOM a trimis informațiile primite către VLOPs în cauză, pentru evaluare conform propriilor termeni și condiții, informând, în același timp, și Comisia Europeană.

În aceste condiții, rolul ANCOM în raport cu astfel de situații este circumscris atribuțiilor de cooperare, coordonare, facilitare și escaladare instituțională prevăzute de DSA și de Legea nr.50/2024, fără a include competențe de intervenție directă asupra modului în care furnizorii de VLOPs și VLOSEs își îndeplinesc obligațiile referitoare la evaluarea și atenuarea riscurilor sistemice.

Suplimentar, în ceea ce privește instrumentele procedurale instituite la nivel național pentru aplicarea Regulamentului privind serviciile digitale, ANCOM a adoptat Decizia nr. 335/2024⁵ privind procedura de soluționare a plângerilor formulate în temeiul art. 53 din DSA și Decizia nr. 336/2024⁶ privind procedura de acordare a statutului de notficator de încredere, aferentă mecanismului prevăzut la art. 22 din Regulamentul privind serviciile digitale. Se observă, însă, că atât mecanismul prevăzut la art. 22 din DSA, cât și cel reglementat de art. 53 din DSA, sunt construite în jurul noțiunii de *conținut ilegal*⁷, astfel cum aceasta este avută în vedere de DSA. În consecință, competențele exercitate în cadrul acestor proceduri vizează exclusiv aspecte referitoare la identificarea, notificarea și gestionarea conținutului pretins ilegal, iar nu evaluarea unor conduite sau practici care, deși pot contraveni termenilor și condițiilor unui furnizor de platformă online, nu constituie prin ele însele încălcări ale legislației aplicabile.

Prin urmare, nici procedura de soluționare a plângerilor reglementată prin Decizia ANCOM nr. 335/2024 și nici mecanismul notificatorilor de încredere detaliat prin Decizia ANCOM nr. 336/2024 nu pot fi utilizate ca instrumente pentru semnalarea ori calificarea unor situații de comportament inautentic coordonat, în măsura în care acestea nu se materializează într-un conținut ilegal în sensul Regulamentului privind serviciile digitale. O eventuală analiză a unor astfel de comportamente poate interveni exclusiv în contextul obligațiilor privind evaluarea și atenuarea riscurilor sistemice prevăzute la art. 34 și art. 35 din DSA, aplicabile furnizorilor de platforme online foarte mari și de motoare de căutare online foarte mari.

Luând în considerare aspectele mai sus menționate, vă rugăm să regăsiți în continuare răspunsurile punctuale la întrebările dvs.

⁴ Art. 3 lit. n) din DSA.

⁵ privind stabilirea procedurii de soluționare a plângerilor privind serviciile digitale.

⁶ privind procedura de acordare a statutului de notficator de încredere.

⁷ Art. 3 lit. h) din DSA.

1. *Apreciați oportună adoptarea unei legi care să reglementeze conduita operatorilor de conturi automatizate și a rețelelor coordonate de conturi false, distinctă de obligațiile aplicabile furnizorilor de platforme online conform DSA și Legii nr. 50/2024?*

Apreciam că orice inițiativă legislativă care urmărește protejarea integrității spațiului digital și limitarea fenomenelor susceptibile să afecteze dezbaterile din mediul online ori să influențeze percepția utilizatorilor trebuie să aibă în vedere că DSA este un act normativ unional, de aplicabilitate generală la nivelul statelor membre, iar adăugarea unor obligații suplimentare în sarcina furnizorilor de servicii intermediare ar putea intra în contradicție cu normele europene. Pe de altă parte, eventualele obligații ce ar putea fi stabilite în sarcina *destinatarii serviciului* (înțelegi în acest context, conform celor menționate de dvs., ca fiind *operatori* de conturi automatizate și a rețelelor coordonate de conturi false) poate fi avută în vedere, dar numai dacă o astfel de obligație ar fi însoțită de reguli clare care să permită VLOPs sau VLOSEs să evalueze cum ar putea implementa, la nivelul platformelor pe care le operează, o normă națională care instituie obligații specifice în cazul destinatarii serviciului din România.

Astfel cum am precizat în debutul acestei adrese, Regulamentul privind serviciile digitale menționează, în contextul obligațiilor privind identificarea, analizarea și evaluarea riscurilor sistemice și a obligațiilor de atenuare a acestora, în conformitate cu dispozițiile art. 34 și art. 35, aplicabile platformelor și motoarelor de căutare online foarte mari (VLOPSEs), utilizarea neautentică a serviciului, inclusiv prin crearea de conturi false, utilizarea boților și alte comportamente automatizate sau parțial automatizate care pot contribui la campanii de dezinformare, potrivit considerentului (84) din Regulamentul privind serviciile digitale.

Utilizarea coordonată a unor asemenea mecanisme poate contribui la răspândirea rapidă a conținutului ilegal sau dăunător, la manipularea serviciilor și la afectarea proceselor democratice, însă, în lipsa unui regim juridic specific la nivel unional sau național, comportamentul inautentic coordonat și utilizarea conturilor automatizate sunt tratate, în principal, prin intermediul politicilor interne ale platformelor.

În acest context, se impune a fi menționat și faptul că unele dintre platformele online și motoarele de căutare online foarte mari, desemnate în temeiul DSA (Youtube⁸, Facebook⁹, Microsoft Bing¹⁰, LinkedIn și TikTok¹¹) sunt semnatare ale *Codului de Conduită privind dezinformarea*¹², aderând la angajamentele din Cod relevante pentru combaterea comportamentului inautentic coordonat (CIC), în speță angajamentele 14 și 16.

Aceste angajamente vizează detectarea și limitarea comportamentelor manipulative inautentice, precum utilizarea conturilor false, amplificarea prin boți și operațiunile coordonate de influență, precum și cooperarea inter-platforme pentru identificarea și perturbarea acestor activități. Mai exact, angajamentul 14 prevede că semnatarii trebuie să adopte și să aplice politici clare împotriva comportamentelor manipulative și inautentice utilizate pentru răspândirea dezinformării, comportamentele vizate explicit fiind: crearea și utilizarea de conturi false; preluarea (compromiterea) conturilor; amplificarea prin boți; impersonarea; *deepfake*-uri malițioase; cumpărarea de interacțiuni false; promovarea netransparentă prin *influenceri*; crearea și utilizarea conturilor care participă la CIC; comportamente care amplifică artificial vizibilitatea. Angajamentul 16 prevede că semnatarii trebuie să creeze canale de schimb de informații pentru: a identifica operațiuni de influență *cross-platform*, a detecta ingerințe străine în spațiul informațional; a preveni migrarea rețelelor manipulative de pe o platformă pe alta; a împiedica reapariția campaniilor coordonate. Codul de Conduită privind dezinformarea a fost integrat în DSA la 1 iulie 2025. Deși aderarea la codurile de conduită prevăzute la articolul 45 din DSA este un act voluntar, pentru semnatarii care sunt desemnați drept platforme online foarte mari (VLOP) și motoare de căutare

⁸ <https://disinfocode.eu/reports/youtube/8?commitmentId=357&chapterId=73&signatorie=55&report=8>

⁹ <https://disinfocode.eu/reports/facebook/8?commitmentId=357&chapterId=73>

¹⁰ <https://disinfocode.eu/reports/microsoft-bing/8?commitmentId=359&chapterId=73&signatorie=58&report=8>

¹¹ <https://disinfocode.eu/reports/tiktok/8?commitmentId=357&chapterId=73>

¹² [The Code of Conduct on Disinformation | Shaping Europe's digital future](#)

online foarte mari (VLOSE), acest lucru poate contribui la asigurarea instituirii unor măsuri adecvate de atenuare a riscurilor.

Nu în ultimul rând, se impune a fi subliniată importanța analizării oricărui demers legislativ și din perspectiva potențialelor riscuri majore pe care acesta le-ar putea genera, dintre care amintim cu titlu de exemplu atribuirea competenței unei autorități administrative de a evalua legalitatea/„adevărul” unui mesaj (ex: politic sau opinie), ceea ce ar putea conduce spre o veritabilă cenzură instituțională, sau reglementarea unor obligații suplimentare în sarcina furnizorilor de servicii intermediare prin legislația națională care să contravină armonizării depline impuse de Regulamentul DSA.

Pe cale de consecință, orice eventuală modificare legislativă prin care s-ar impune obligații pentru destinatarii serviciului ar trebui să urmărească **mijlocul** (conturi false, automatizare etc.), **scopul** (inducerea în eroare) și **subiectul activ** (entitatea care utilizează mijlocul), **cu distincția clară că nu este vizat/incriminat conținutul opiniei/mesajului/criticii**.

2. *Considerați tehnic fezabilă, la nivelul ANCOM, constatarea CIC pe baza indicatorilor obiectivi de coordonare (sincronizare temporală a postărilor, conținut cvasi-identificat distribuit concentrat, infrastructură comună, semnături de automatizare), inclusiv prin mecanismele de acces la date prevăzute de art.40 din DSA?*

Din punct de vedere tehnic, se pot defini unii indicatori de coordonare, însă aceștia au un grad relativ de certitudine, existând riscul să fie interpretați eronat dacă sunt analizați izolat. Singura entitate competentă să identifice astfel de indicatori, cu un grad ridicat de acuratețe, este platforma online în care se manifestă aceste comportamente deoarece doar această entitate deține toate informațiile ce arata la un nivel extins dacă există un factor de coordonare cert pe un anumit subiect.

Astfel, pe lângă indicatorii menționați în *Termenii și Condițiile și Regulile Comunității* platformei, precum spam, automatizare, conturi false sau activități coordonate, platforma online dispune și de date interne suplimentare, care nu sunt accesibile publicului sau cercetătorilor și care cresc precizia detectării comportamentelor inautentice coordonate. Aceste date pot include, fără a se limita la informații tehnice despre utilizarea conturilor și a infrastructurii: tipuri de dispozitive și conexiuni/sisteme de operare, tipare de IP-uri, schimbări de locație, browser și setări tehnice, date de creare a contului, un posibil istoric al datelor utilizate pentru gestionarea acestuia (spre exemplu, dispozitive utilizate în trecut, adrese de e-mail sau numere de telefon asociate), informații asociate utilizatorului, precum data nașterii, postări, conținutul cu care utilizatorul interacționează, căutări efectuate pe platformă, timpul petrecut în relație cu un anumit conținut, precum și alte date pe care platforma le colectează în baza condițiilor de utilizare și a politicii de confidențialitate. Corelarea acestor indicatori poate evidenția situații în care mai multe conturi par să funcționeze din medii tehnice similare sau să fie conectate între ele. De asemenea, platforma poate analiza în detaliu comportamentul utilizatorilor în timp, urmărind indicatori precum momentul postărilor, viteza de reacție, ordinea și simultaneitatea acțiunilor. Astfel, sincronizările sau reacțiile aproape identice în ferestre foarte scurte de timp pot sugera o posibilă coordonare (sau automatizare).

În acest sens, platformele online și-au definit o serie de comportamente care nu sunt permise, în categorii specifice care vizează diferite tipuri de utilizare neautorizată sau abuzivă a serviciilor, oferind astfel un punct de plecare pentru identificarea unor posibili indicatori observabili ai utilizării neautentice. Totuși, este important de precizat că acești indicatori nu au valoare probatorie individuală și trebuie interpretați doar în ansamblu, prin corelarea cu alte semnale și în contextul în care apar, pentru a susține o evaluare relevantă a comportamentului analizat.

În considerarea celor de mai sus, *Regulile Comunității* YouTube¹³ (VLOP), parte a ecosistemului Google, menționează în secțiunea practici înșelătoare: spamul, impersonarea unei entități sau a unui canal pentru a induce în eroare utilizatorii, utilizarea de sisteme automate pentru

¹³ [Politica YouTube privind interacțiunile false](#)

generarea de interacțiuni false și comportamente inautentice coordonate, în special atunci când mai multe canale acționează sincronizat pentru a amplifica artificial conținutul.

În cadrul platformelor Meta¹⁴, Facebook și Instagram (VLOPs), combaterea comportamentului inautentic coordonat face parte dintr-un cadru mai amplu de politici privind integritatea conturilor, autenticitate, dezinformare, manipularea conținutului, prevenirea spamului și combaterea activităților înșelătoare. Platformele nu analizează exclusiv comportamentul unui cont individual, ci și relațiile dintre mai multe conturi, pagini sau alte entități, fiind exemplificate practici precum: distribuirea în mod coordonat a unui conținut interzis, spam, dezinformare sau alte materiale care încalcă politicile, existența unor legături cu conturi deja sancționate (același administrator care controlează mai multe conturi, aceleași date de contact, conturi administrate de pe aceleași dispozitive, modele similare de activitate sau conținut, coordonare cu o rețea de conturi, pagini sau grupuri care încalcă sau evită politicile platformei). De asemenea, platformele în cauză consideră autenticitatea un principiu fundamental al comunității lor, motiv pentru care nu este permisă crearea de conturi multiple care induc în eroare cu privire la identitatea unui utilizator (folosesc informații de profil înșelătoare, utilizează imagini generice de tip arhivă, își redenumesc frecvent pagina/contul). În ceea ce privește comportamentul inautentic, Meta menționează că nu permite crearea și utilizarea de pagini/conturi false pentru a induce în eroare utilizatorii sau pentru a evita sancțiunile. De asemenea, interzice rețelele de conturi care manifestă comportament coordonat și înșelător, inclusiv forme de interferențe străină.

În cadrul platformei TikTok¹⁵ (VLOP) politica de integritate și autenticitate acoperă un cadru mai larg care menționează o serie de riscuri, precum dezinformarea, conținutul manipulat, inclusiv cel generat sau modificat cu instrumente de inteligență artificială, integritatea proceselor civice și electorale și comportamente care afectează încrederea utilizatorilor, categoria privind comportamentele inautentice coordonate fiind privită mai degrabă ca o componentă secundară specifică a comportamentelor abuzive. Această din urmă noțiune se referă la comportamente înșelătoare și interacțiuni false, nefiind permise acțiunile prin care conturile încearcă să inducă în eroare platforma sau utilizatorii prin utilizarea unor tehnici precum: operațiuni de influență ascunsă, uzurparea identității, spam, recenzii false, utilizarea de instrumente de automatizare sau scripturi pentru a crește artificial vizibilitatea, inclusiv prin utilizarea unor servicii pentru creșterea artificială a gradului de implicare (achiziționarea de aprecieri, urmăritori sau distribuiri) și distribuirea de materiale obținute prin acces neautorizat.

Platforma online foarte mare X¹⁶ (VLOP) interzice orice comportament care încearcă să inducă în eroare platforma sau utilizatorii, prin conturi false, automatizare, spam sau prin manipularea artificială a gradului de implicare și a conversațiilor. În acest sens, nu este permisă utilizarea de conturi false sau coordonate pentru a influența vizibilitatea unui conținut sau pentru a-l amplifica artificial prin exploatarea unor hashtaguri sau tendințe, nu sunt acceptate identități false, poze de profil de tip stoc sau generate cu inteligența artificială, detalii despre utilizator copiate de la alți utilizatori sau false, impersonarea unei entități, conturi de tip bot sau scripturi care încalcă regulile platformei.

Referitor la art. 40 din Regulamentul privind serviciile digitale, facem precizarea că acesta stabilește un cadru care obligă VLOPs/VLOSEs să ofere acces la date *cercetătorilor agreeți* („vetted researchers”). Datele accesate în acest mod sunt utilizate pentru investigarea și evaluarea riscurilor sistemice din mediul online în Uniunea Europeană.

În temeiul art. 40 alin. (4) din Regulamentul privind serviciile digitale, cercetătorii care sunt validați de coordonatorul serviciilor digitale din țara de stabilire primesc statutul de *cercetător agreeat* („vetted researcher”) și pot obține acces la informații care, în mod obișnuit, nu sunt disponibile prin canalele standard de acces oferite de platforme. Coordonatorul serviciilor digitale din țara de stabilire, așadar, este responsabil pentru evaluarea cererilor și pentru solicitarea accesului la date de la VLOP/VLOSE în numele cercetătorilor agreeți care îndeplinesc criteriile prevăzute la art.40 din

¹⁴ Standardele comunității Meta privind comportamentul inautentic

¹⁵ Regulile comunității TikTok privind Integritatea și autenticitatea

¹⁶ Regulile comunității X referitoare la autenticitate

DSA. În calitate de coordonator al serviciilor digitale din țara de stabilire pentru 15 dintre cele 25 de VLOPs/VLOSEs desemnate în temeiul DSA, Coimisiún na Meán (coordonatorul serviciilor digitale din Irlanda), va avea un rol important în procesul de acordare a accesului la date pentru cercetătorii agreeți.

3. *Care este, în opinia ANCOM, riscul de preempțiune cu DSA în privința unei legi naționale care reglementează conduita operatorului utilizator/coordonator, iar nu obligații suplimentare ale furnizorilor de platforme? Considerați necesară notificarea TRIS potrivit Directivei (UE) 2015/1535?*

Apreciem că evaluarea compatibilității unei eventuale intervenții legislative cu dreptul Uniunii Europene nu poate fi realizată în abstract, ci trebuie raportată la dispozițiile concrete ale reglementării avute în vedere.

În acest sens, trebuie luat în considerare faptul că DSA urmărește instituirea unui cadru armonizat pentru furnizarea serviciilor intermediare la nivelul Uniunii Europene, în vederea evitării fragmentării pieței interne și a apariției unor obligații naționale divergente. În acest context, statele membre trebuie să se abțină de la adoptarea unor măsuri naționale care ar putea afecta aplicarea uniformă, coerența sau efectul util al normelor armonizate prin regulament.

Ipoteza în care o eventuală inițiativă legislativă ar viza conduita unor persoane fizice sau juridice implicate în activități asociate comportamentului inautentic coordonat și nu ar introduce obligații suplimentare în sarcina furnizorilor de servicii intermediare cu privire la aspecte deja reglementate prin Regulamentul privind serviciile digitale, ar putea fi apreciată drept una pozitivă, care să fie avută în vedere la configurarea textului viitoarei reglementări. Desigur, stabilirea în mod fundamentat a nivelului de compatibilitate dintre o propunere legislativă și dreptul Uniunii Europene necesită o analiză individualizată, realizată în funcție de obiectul, domeniul de aplicare și efectele concrete ale măsurilor propuse.

Totodată, trebuie avută în vedere Directiva (UE) 2015/1535¹⁷, care instituie o procedură de furnizare de informații în domeniul reglementărilor tehnice și al normelor privind serviciile societății informaționale. În măsura în care proiectul de act normativ ar conține dispoziții susceptibile să intre în categoria reglementărilor tehnice, astfel cum această noțiune a fost definită prin directivă, se impune analiza punctuală a incidenței obligației de notificare prealabilă către Comisia Europeană, anterior adoptării actului normativ.

4. *Dispune ANCOM de resursele umane, tehnice și bugetare necesare pentru asumarea rolului de autoritate constatatatoare a CIC, inclusiv pentru elaborarea metodologiei de constatare și a indicatorilor tehnici? Care este estimarea ANCOM privind resursele suplimentare necesare?*

La acest moment, ANCOM nu dispune de resursele umane, tehnice și bugetare necesare pentru asumarea unui rol de autoritate constatatatoare în condițiile în care nu există o listă definitivă de indicatori care să arate cu certitudine eventualul comportament inautentic coordonat. În lipsa unor norme legislative sau măcar a unui proiect de reglementare articulat, orice eventuală "estimare" a potențialelor nevoi în materie de resurse suplimentare necesare ar reprezenta o simplă supoziție lipsită de orice fundament.

5. *Cum apreciază ANCOM oportunitatea introducerii unei obligații generale de identificare prin ROeID pentru deschiderea conturilor de social media de către cetățenii români, prin comparație cu un mecanism voluntar de atestare a calității de utilizator real, cu divulgare minimă? În particular, care ar fi implicațiile asupra conformității cu DSA, cu art.8 din Carta drepturilor fundamentale a UE și cu Regulamentul (UE) 2016/679?*

¹⁷ Directiva (UE) 2015/1535 referitoare la procedura de furnizare de informații în domeniul reglementărilor tehnice și al normelor privind serviciile societății informaționale

În ceea ce privește oportunitatea introducerii unei obligații generale de identificare prin ROeID, facem pentru început precizarea că Regulamentul privind serviciile digitale nu instituie o obligație generală de identificare a utilizatorilor (înțelegi ca *destinatari ai serviciului* în context DSA) și nici nu impune colectarea sau păstrarea unor date suplimentare de identificare. Dimpotrivă, abordarea Regulamentului este una limitată și proporțională, mecanismele instituite prin actul normativ în scopul verificării vârstei utilizatorilor platformelor online fiind analizată **exclusiv** în contextul **accesului minorilor** la serviciile furnizate și al necesității asigurării unui nivel ridicat de confidențialitate, siguranță și securitate pentru aceștia. În conformitate cu art. 28 alin. (1) din Regulamentul privind serviciile digitale, furnizorii de platforme online accesibile minorilor au obligația de a implementa măsuri adecvate și proporționale pentru protejarea acestora. Totodată, art. 28 alin. (3) prevede în mod expres că respectarea acestei obligații nu impune furnizorilor să prelucreze date cu caracter personal suplimentare pentru a evalua dacă utilizatorul este minor.

Această abordare este confirmată și de considerentul (71) al Regulamentului privind serviciile digitale, care prevede că „*în conformitate cu Regulamentul (UE) 2016/679, în special cu principiul reducerii la minimum a datelor prevăzut la articolul 5 alineatul (1) litera (c) din regulamentul respectiv, această interdicție nu ar trebui să determine furnizorul platformei online să păstreze, să obțină sau să prelucreze mai multe date cu caracter personal decât cele pe care le deține deja pentru a aprecia dacă destinatarul serviciului este minor. Prin urmare, această obligație nu ar trebui să îi încurajeze pe furnizorii de platforme online să înregistreze vârsta destinatarului serviciului înainte ca acesta să utilizeze serviciul*”. În consecință, Regulamentul consacră principiul minimizării datelor și exclude instituirea unor mecanisme generale de identificare a utilizatorilor, orice măsură de asigurare a vârstei trebuind să fie limitată la ceea ce este strict necesar pentru confirmarea îndeplinirii pragului de vârstă aplicabil.

Totodată, în aplicarea art. 28 alin. (4), Comisia Europeană a adoptat *Orientările privind protecția minorilor în mediul online*, care prevăd că alegerea mecanismelor de asigurare a vârstei trebuie realizată pe baza unei evaluări a riscurilor asociate serviciului și cu respectarea principiilor proporționalității, protecției vieții private și „privacy by design”. *Orientările* disting între mecanisme de estimare a vârstei și mecanisme de verificare a vârstei, acestea din urmă fiind recomandate în special în cazul serviciilor care prezintă riscuri ridicate pentru minori (cum ar fi vânzarea de produse alcoolice, produse pe bază de tutun sau nicotină, droguri și accesul la orice tip de conținut pornografic), sau atunci când legislația Uniunii sau legislația națională stabilește o vârstă minimă pentru accesarea anumitor servicii.

Prin urmare, atât Regulamentul privind serviciile digitale, cât și *Orientările* Comisiei Europene promovează un model de verificare a vârstei limitat la etapa accesării serviciului și bazat pe prelucrarea strict a datelor necesare pentru confirmarea vârstei, fără crearea unor mecanisme generale de identificare sau de monitorizare a utilizatorilor.

Având în vedere cele menționate anterior, apreciem că aplicația ROeID poate constitui un instrument adecvat pentru verificarea vârstei și pentru asigurarea unui nivel ridicat de protecție a minorilor în mediul online, în conformitate cu obiectivele prevăzute la art. 28 din Regulamentul privind serviciile digitale. Totodată, considerăm că instituirea unei **obligații suplimentare pentru platformele online** de a colecta sau prelucra date referitoare la identificarea utilizatorilor, dincolo de cele strict necesare pentru confirmarea vârstei, ar fi contrară principiului minimizării datelor și dispozițiilor Regulamentului privind serviciile digitale, care nu promovează mecanisme generale de identificare a utilizatorilor în scopul accesării serviciilor online.

6. A primit ANCOM solicitări de cooperare ori notificări din partea Comisiei Europene sau a coordonatorilor altor state membre privind operațiuni de CIC cu impact în România în ultimele 12 luni? În ce stadiu se află acestea?

ANCOM nu a primit astfel de solicitări sau notificări nici din partea Comisiei Europene și nici din partea altor coordonatori ai serviciilor digitale din alte State Membre. Nu excludem, însă,

posibilitatea ca alte instituții din România să fi primit solicitări ori notificări de acest tip prin canalele lor specifice de colaborare.

7. Cum apreciază ANCOM oportunitatea consacrării unei prezumții relative de CIC declanșate de indicatori tehnici obiectivi, cu menținerea sarcinii probei la autoritate și cu posibilitatea persoanei vizate de a o răsturna, prin raportare la standardele DSA și la jurisprudența CEDO?

Orice eventuală soluție legislativă destinată identificării și combaterii comportamentului inautentic coordonat în mediul online trebuie analizată prin raportare atât la obiectivul protejării spațiului digital, cât și la necesitatea respectării drepturilor și libertăților fundamentale.

Din această perspectivă, sunt relevante dispozițiile art. 11 și art. 47 din Carta drepturilor fundamentale a Uniunii Europene, referitoare la libertatea de exprimare și la dreptul la o cale de atac eficientă, precum și prevederile art. 52 alin. (1) din Cartă, potrivit cărora orice limitare a exercitiului drepturilor fundamentale trebuie să fie prevăzută de lege, să respecte substanța acestor drepturi și să respecte, totodată, principiile necesității și proporționalității.

În acest context, compatibilitatea unei eventuale prezumții legale relative, declanșate de indicatori tehnici obiectivi, ar trebui analizată în raport cu ansamblul garanțiilor procedurale instituite, inclusiv menținerea sarcinii probei în sarcina autorităților competente, posibilitatea administrării de probe de către persoana vizată, transparența criteriilor utilizate și existența unor mecanisme efective de contestare a concluziilor rezultate din aplicarea acestora.

De asemenea, trebuie menționat că la nivelul Uniunii Europene există preocupări constante privind diminuarea riscurilor sistemice asociate utilizării neautentice a serviciilor online. Cu toate acestea, orice eventuală intervenție legislativă națională trebuie analizată prin raportare la cadrul juridic european aplicabil, inclusiv la Regulamentul privind serviciile digitale, precum și cu respectarea deplină a principiilor și garanțiilor aferente protecției drepturilor fundamentale.

Cu stimă,

Președinte,

Signed by: Valeriu Stefan

Zgonea

Date: 2026.07.08 16:48

Reason: .

Valeriu Ștefan ZGONEA

ANCOM este instituția care promovează interesele utilizatorilor de servicii de comunicații electronice, servicii poștale și servicii digitale în contextul tranziției la societatea Gigabit, prin valorificarea optimă a mixului de instrumente de administrare și reglementare aflate la dispoziția Autorității. Pentru mai multe detalii despre activitatea ANCOM vizitați www.ancom.ro, infocentru.ancom.ro, www.portabilitate.ro și www.veritel.ro. Pentru a testa și monitoriza calitatea serviciului de internet, accesați www.netograf.ro. Pentru a consulta acoperirea cu semnal mobil a localităților, drumurilor naționale și județene din România, accesați www.aisemnal.ro.