



Nr. 8388, 8389, 8390, 8391, 8392, 8393, 8394, 8395, 8396, 8397, 8398, 8399, 8383, 8384, 8385, 8386/2026

07-07-2026

**Către: Doamna Oana MURARIU
Secretar al Camerei Deputaților**

Ref. la: Răspunsuri la întrebări/interpelări formulate de deputați

Stimată doamnă secretar,

26.07.2026 66-8/345

Vă transmitem, alăturat, răspunsurile instituțiilor vizate cu privire la unele întrebări/interpelări formulate de deputați, potrivit tabelului anexat.

Cu deosebită considerație,

NINI SĂPUNARU

SECRETAR DE STAT

ROMÂNIA
MINISTERUL AFACERILOR INTERNE



VICEPRIM-MINISTRU
MINISTRUL AFACERILOR INTERNE

Exemplar nr. 1
Nr. 16328
București 06.07.2026

Către,
PARLAMENTUL ROMÂNIEI
CAMERA DEPUTAȚILOR
Domnului deputat Sebastian-Ioan BURDUJA

Stimate domnule deputat,

În legătură cu întrebarea dumneavoastră înregistrată la Camera Deputaților cu nr.5441A/2026, având ca obiect „Amenințările generate de rețelele de conturi automatizate și false pe platformele online, capacitatea operațională a structurilor MAI de combatere a acestora și oportunitatea unui cadru normativ de identificare digitală pentru utilizatorii serviciilor de platformă online”, vă comunicăm următoarele:

Acțiunile din spectrul amenințărilor hibride, manifestate prin interferențe informaționale, pot afecta corectitudinea proceselor democratice, informarea obiectivă a cetățenilor și încrederea publicului în instituțiile statului. Prin propagarea coordonată a unor informații false sau manipulatorii și amplificarea artificială a unor mesaje, aceste mecanisme pot influența percepția publică asupra acțiunilor autorităților și pot alimenta polarizarea socială.

În contextul unor situații de urgență sau al altor evenimente de interes major, inundarea spațiului informațional cu narrative de dezinformare poate induce confuzie în rândul populației, diminua încrederea în capacitatea autorităților de a gestiona eficient astfel de situații și poate afecta ordinea publică, cu potențial de perturbare a funcționării normale a instituțiilor statului.

Exemplificăm în acest sens faptul că experiența gestionării pandemiei de COVID-19 a evidențiat, în mod concret, impactul pe care dezinformarea îl poate avea asupra unei situații de urgență. În perioada respectivă au circulat pe scară largă informații neverificate sau false referitoare la existența virusului, modalitățile de transmitere, măsurile de protecție, vaccinarea, achiziția de echipamente și intervențiile autorităților. Mesaje de natura celor în discuție au contribuit la amplificarea neîncrederii, la apariția unor comportamente de risc și la dificultăți suplimentare cu privire la implementarea măsurilor destinate protejării sănătății populației.

Precizăm faptul că prin intermediul platformei naționale „Fii Pregătit”, principalul instrument de informare și educare a populației în domeniul situațiilor de urgență, este promovată și o abordare activă de creștere a rezilienței comunităților în fața riscurilor informaționale. În acest scop, a fost elaborat și pus la dispoziția publicului un ghid dedicat recunoașterii și combaterii dezinformării, care oferă recomandări practice privind verificarea informațiilor, evaluarea credibilității surselor și identificarea principalelor tehnici utilizate pentru răspândirea informațiilor false sau înșelătoare.

Ghidul abordează fenomenul dezinformării dintr-o perspectivă practică, explicând atât scopul, cât și mecanismele prin care informațiile false influențează percepțiile și comportamentele populației. Sunt prezentate obiectivele urmărite prin dezinformare, precum manipularea opiniei publice, generarea neîncrederii în instituții, amplificarea conflictelor sociale sau influențarea procesului decizional al

cetățenilor. În cadrul secțiunii dedicate premiselor sunt analizate condițiile care favorizează succesul dezinformării, inclusiv reacțiile emoționale puternice, consumul rapid de informații și tendința de a accepta informațiile care confirmă convingerile existente. Mai mult, menționăm că sunt descrise principalele metode și semne ale dezinformării, precum utilizarea titlurilor alarmiste, a informațiilor scoase din context, a imaginilor manipulate, a surselor neverificabile sau apelului excesiv la emoții.

Pentru sprijinirea cetățenilor cu privire la identificarea informațiilor false, ghidul propune o serie de întrebări utile privind autorul informației, sursa, dovezile prezentate, data publicării, scopul mesajului și existența unor confirmări din partea altor surse credibile. În plus, capitolul dedicat operațiunilor informaționale explică modul în care informațiile pot fi utilizate în mod coordonat pentru influențarea percepțiilor și comportamentelor colective, evidențiind importanța verificării informațiilor și a consultării surselor oficiale.

În ansamblu, ghidul urmărește dezvoltarea gândirii critice și consolidarea rezilienței populației în fața riscurilor informaționale. Principiile și recomandările promovate prin acest material sunt integrate atât în activitățile de informare desfășurate în mediul *online*, cât și în campaniile de educare și prevenire derulate la nivelul comunității.

Având în vedere cele prezentate, evidențiem faptul că, din perspectiva prevenirii, un rol esențial îl au dezvoltarea culturii de securitate și a educației pentru situații de urgență, consolidarea capacității populației de a identifica și verifica informațiile provenite din mediul *online*, precum și promovarea utilizării surselor oficiale de informare. Comunicarea publică rapidă, transparentă și constantă din partea autorităților contribuie la reducerea vulnerabilității societății în fața campaniilor de dezinformare și la creșterea rezilienței comunităților.

De asemenea, precizăm faptul că, la nivelul structurilor Ministerului Afacerilor Interne (M.A.I.), au fost dezvoltate capacități de detecție, analiză, prevenire și contracarare FIMI¹. Astfel, în prezent, instituția noastră, prin structurile de specialitate, dispune de instrumentele și mijloace necesare pentru efectuarea unor investigații complexe, identificarea actorilor și a modului de operare, precum și a unor eventuale situații care ar putea genera tulburări grave ale ordinii publice.

În acest sens, menționăm faptul că, la nivelul Inspectoratului General al Poliției Române (I.G.P.R.), s-au implementat măsuri pentru creșterea capacității operaționale de investigare a infracțiunilor comise împotriva siguranței sistemelor informatice și a infracțiunilor comise prin intermediul sistemelor informatice prin modificări de natură structurală.

Trendul constant crescător al fenomenului infracțional în domeniul supus atenției, concretizat într-un volum tot mai mare al dosarelor penale pe această linie, a impus adoptarea acestor măsuri de suplimentare a structurilor cu atribuții în ceea ce privește investigarea infracțiunilor informatice la nivelul tuturor structurilor teritoriale subordonate I.G.P.R.

Raportat la aspectele referitoare la stabilirea politicii penale a statului în domeniul de referință, considerăm că asupra oportunității adoptării unor eventuale soluții normative este abilitat să se pronunțe Ministerul Justiției.

În ceea ce privește instituirea unei obligații generale de identificare a utilizatorilor la crearea conturilor pe platformele de social media, instituția noastră consideră că o astfel de soluție ar fi oportună în măsura în care ar contribui semnificativ la limitarea comportamentului neautentic coordonat și nu ar trebui limitată la utilizarea platformei ROeID.

În context, menționăm că M.A.I. furnizează prin intermediul portalului *hub.mai.gov.ro* serviciul *eIdentity*, prin care cetățenii au opțiunea de a vizualiza propriile date cu caracter personal și de a partaja, în mod controlat și temporar, anumite categorii de date cu caracter personal (inclusiv categoria de vârstă – sub/peste 18 ani) către terți, prin intermediul unui cod QR cu o valabilitate de 10 minute.

¹ Foreign Information Manipulation and Interference.

Partajarea datelor se face exclusiv cu acordul explicit al titularului pentru perioada de valabilitate a codului QR.

Această abordare reflectă principiul minimizării datelor consacrat de Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr.910/2014 în ceea ce privește instituirea cadrului european pentru identitatea digitală (eIDAS2), care stă la baza ecosistemului european de identitate digitală și a soluției portofelului european de identitate digitală (EUDIW). În logica acestui cadru, precizăm că dezvăluirea selectivă a unui singur atribut, precum apartenența la categoria de vârstă, sub/peste 18 ani, permite atingerea scopului urmărit fără divulgarea identității titularului. Soluția pe care M.A.I. o pune deja la dispoziție prin serviciul eidentity permite tocmai dovedirea unui astfel de atribut, cu dezvăluire minimă și exclusiv cu acordul titularului, putând susține obiective legitime precum protecția minorilor și controlul accesului la conținut restricționat pe criterii de vârstă.

De asemenea, precizăm faptul că impunerea aplicației ROeID ca aplicație unică de identificare pentru crearea conturilor utilizatorilor în cadrul platformelor de social media ar putea fi în măsură să contravină obligației prevăzute de *Regulamentul (UE) 2024/1183 (eIDAS2)*, care impune obligația statelor membre ale Uniunii Europene de a lansa cel puțin o soluție de portofel european pentru identitate digitală, până la finalul anului 2026, în mod special ținând cont de obligația platformelor mari de integrare a soluției. În acest context și având în vedere scopul urmărit, prin intermediul atestatului privind datele pentru identificare personală (PID), utilizatorul își poate verifica vârsta înainte de accesarea unui serviciu public sau privat, inclusiv în contextul creării unui cont într-o platformă de social media.

Pe de altă parte, menționăm faptul că, în vederea întreprinderii unor măsuri active de protejare a spațiului informațional, M.A.I. a cooperat cu Autoritatea Electorală Permanentă cu ocazia proceselor electorale și a informat în multiple circumstanțe Autoritatea Națională pentru Administrare și Reglementare în Comunicații (A.N.C.O.M.) despre apariția în mediul *online* a unor campanii de tip doppelganger², derulate prin intermediul unor site-uri care imitau elementele vizuale ale unor publicații de presă sau instituții de stat. Ca urmare a acestor sesizări, au fost întreprinse măsuri de comunicare strategică, de raportare a conținutului către platformele de socializare și, după caz, de restricționare a accesului la respectivele site-uri.

Totodată, precizăm faptul că, în prezent, în domeniul prevenirii și combaterii criminalității informatice, I.G.P.R. cooperează cu Parchetul de pe lângă Înalta Curte de Casație și Justiție, A.N.C.O.M., Directoratul Național de Securitate Cibernetică și Institutul Național de Cercetare-Dezvoltare în Informatică.

Cu privire la stadiul cooperării cu Autoritatea Electorală Permanentă, precizăm că, în context electoral, Direcția Generală pentru Evidența Persoanelor din cadrul M.A.I. pune în aplicare dispozițiile art. 46 din *Legea nr. 208/2015*³, prin transmiterea către Autoritatea Electorală Permanentă, în condițiile și termenele stabilite prin protocolul de colaborare, a datelor prevăzute de lege, a cazurilor de interzicere a exercitării drepturilor electorale și cazurilor de punere sub interdicție, actualizărilor intervenite în datele personale ale cetățenilor români cu drept de vot și informațiilor privind persoanele decedate, respectiv cele cu mențiuni de deces, înregistrate în Registrul Național de Evidență a Persoanelor (R.N.E.P.).

Datele comunicate către Autoritatea Electorală Permanentă au caracter periodic și sunt actualizate permanent, în conformitate cu prevederile legale și cu protocolul de colaborare încheiat între cele două instituții. În același timp, este important de subliniat faptul că Direcția Generală pentru Evidența Persoanelor nu administrează și nu operează modificări asupra Registrului Electoral, atribuția sa limitându-se la transmiterea informațiilor prevăzute de art. 46 din *Legea nr. 208/2015*, cu modificările și completările ulterioare.

² Tehnică prin care se imită elementele vizuale ale unei publicații/autorități, în scopuri manipulative;

³ privind alegerea Senatului și a Camerei Deputaților, precum și pentru organizarea și funcționarea Autorității Electorale Permanente, cu modificările și completările ulterioare.

În ceea ce privește raportul dintre o eventuală obligație de identificare digitală a utilizatorilor și dreptul la viață privată, apreciem că un punct de vedere relevant poate fi comunicat de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Cu deosebită considerație,

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE SECRETAR DE STAT
ANGELICA FĂDOR
Marian-Cătălin PREDOIU