



Nr. 5456, 5475, 5498, 5502, 5503, 5504, 5505, 5506, 5507/2026

12 -05- 2026

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

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

Stimată doamnă secretar,

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. 13592

București 08/05/2026

- 1379B -

Către,
PARLAMENTUL ROMÂNIEI
CAMERA DEPUTAȚILOR
Doamnei deputat Andra-Claudia CONSTANTINESCU

Stimată doamnă deputat,

În legătură cu interpelarea dumneavoastră, înregistrată la Camera Deputaților cu nr.1379B/2026, având ca obiect „Escaladarea fraudelor telefonice și a atacurilor de tip phishing prin impersonarea instituțiilor publice și a băncilor”, vă comunicăm următoarele:

Din informațiile puse la dispoziție de Inspectoratul General al Poliției Române rezultă că baza de date a acestei instituții nu este structurată în funcție de criteriile indicate în conținutul interpelării, astfel încât să poată fi extrase informațiile conform solicitării dumneavoastră, întrucât datele statistice sunt stocate prin raportare la infracțiunile sesizate și nu la modurile de operare utilizate de către autori. Prin urmare, „impersonarea instituțiilor publice sau a entităților financiare” nu reprezintă un indicator de clasificare statistică la nivelul Inspectoratului General al Poliției Române.

Cu toate acestea, precizăm faptul că, în ultimul an, la nivelul Inspectoratului General al Poliției Române au fost înregistrate 2959 de dosare penale privind săvârșirea unor infracțiuni informatice, fără a exista o diferențiere în funcție de modul de operare utilizat de făptuitori.

Prevenirea criminalității informatice și siguranța în mediul digital reprezintă un domeniu prioritar de acțiune preventivă la nivelul Poliției Române, fiind abordate problematici legate de prevenirea fraudelor online și prin intermediul apelurilor telefonice.

Astfel, Institutul de Cercetare și Prevenire a Criminalității din cadrul Inspectoratului General al Poliției Române, împreună cu structurile teritoriale de analiză și prevenire a criminalității, desfășoară în mod constant campanii și proiecte naționale de informare și prevenire a infracțiunilor informatice, care urmăresc creșterea nivelului de conștientizare a riscurilor din mediul digital, promovarea unui comportament responsabil online, precum și dezvoltarea abilităților beneficiarilor de verificare a informațiilor accesate/primate.

De asemenea, un efort strategic de prevenire a fraudelor informatice îl reprezintă programul național de prevenire a criminalității informatice *Siguranța Online*, derulat la nivelul Poliției Române în parteneriat cu Directoratul Național de Securitate Cibernetică și Asociația Română a Băncilor, inițiat încă din 2021 și dezvoltat în mai multe etape, conform dinamicii fenomenelor criminalității informatice.

Instrumentul central al proiectului este reprezentat de platforma *sigurantaonline.ro* (un hub digital dedicat cetățenilor), prin intermediul căreia pot fi accesate recomandări practice, informații, ghiduri și materiale video privind protejarea datelor personale, evitarea fraudelor informatice, recunoașterea tentativelor de phishing, atacurilor malware și manipulărilor digitale (inclusiv deepfake-uri).

Menționăm faptul că, în esență, ghidul „*Atenție la deepfake-uri!*” explică ce sunt deepfake-urile, cum pot fi folosite de fraudatori și cum poate fi verificată autenticitatea conținutului accesibil utilizatorilor.

Totodată, precizăm că, în cadrul programului *Siguranța Online*, unul dintre cele mai recente demersuri de prevenire este reprezentat de campania „*Uniți împotriva escrocheriilor*”, care vizează în mod direct fraudele online și telefonice, scopul principal fiind educarea și conștientizarea populației asupra celor mai frecvente tentative și tipuri de fraude digitale, prin simulări și exemple concrete¹, promovând, în același timp, comportamente simple, dar eficiente și sigure (verificare, necomunicarea datelor sensibile).

În condițiile în care metodele infracționale devin tot mai sofisticate, incluzând apeluri telefonice false („spoofing”), clonarea vocii (vishing) sau mesaje de tip phishing, facem precizarea că proiectul *Siguranța Online*, cu toate resursele sale, aduce activitatea de prevenire a criminalității informatice în centrul dialogului public și educației digitale.

La nivelul Poliției Române au mai fost desfășurate o serie de campanii relevante derulate la nivel național atât online, cât și prin acțiuni directe în comunitate, după cum urmează:

- campania de prevenire și conștientizare cu privire la efectele propagării informațiilor false *Vigilența face diferența!*;
- campanii dedicate prevenirii fraudelor de tip „*investiții online*” (crypto/acțiuni);
- campania de prevenire a victimizării seniorilor în mediul online *Hi Digital*.

De asemenea, menționăm că activitatea structurilor cu atribuții în domeniul de referință din cadrul Poliției Române nu se limitează doar la desfășurarea de campanii, ci include elaborarea de ghiduri și recomandări preventive, parteneriate cu instituții publice și private și diseminarea bunelor practici la nivel național și european (prin intermediul Rețelei Europene de Prevenire a Criminalității).

Astfel, abordarea Poliției Române este una proactivă și integrată, în care prevenirea joacă un rol esențial, parteneriatele cu mediul privat și cooperarea cu instituții precum Directoratul Național de Securitate Cibernetică contribuind la eficiența activității de prevenire, la reducerea impactului fraudelor online/telefonice și la creșterea gradului de siguranță a cetățenilor.

Totodată, facem precizarea că, în conformitate cu prevederile *Legii nr. 50/2024*², Inspectoratul General al Poliției Române, în calitate de autoritate relevantă, cooperează cu coordonatorul serviciilor digitale în România, respectiv Autoritatea Națională pentru Administrare și Reglementare în Comunicații (A.N.C.O.M.).

Din perspectiva combaterii unor fenomene infracționale din domeniul criminalității informatice, polițiștii specializați în investigații criminale din cadrul Poliției Române au inițiat demersuri împreună cu reprezentanții A.N.C.O.M. pentru a putea contracara activitățile infracționale desfășurate în mediul online prin metoda „CLI spoofing”, soluția tehnică identificată fiind aplicată de către A.N.C.O.M., prin blocarea apelurilor inițiate din afara teritoriului României, care afișează în mod fals anumite numere naționale, preponderent de telefonie fixă, acest demers fiind de natură să reducă semnificativ fenomenul în discuție.

În cadrul activităților de combatere, la nivelul structurilor de investigații criminale s-a evidențiat o colaborare eficientă cu Asociația Română a Băncilor (A.R.B.), astfel că, în cursul anului 2025, prin intermediul punctelor de contact stabilite de unitățile bancare, s-a realizat blocarea unei sume totale de 9.668.395,63 lei și Active Cripto [152.000 USDT și 19,66 ETH (aproximativ 49.150 USD)], *provenită din săvârșirea infracțiunilor informatice*, fiind astfel restituită persoanelor vătămate, ca urmare a operaționalizării acestei metode de lucru existente între structurile de investigații criminale și unitățile

¹ Un accent important este pus pe explicarea concretă a modului de operare al infractorilor, astfel încât cetățenii să poată identifica rapid riscurile.

² privind stabilirea unor măsuri pentru aplicarea Regulamentului (UE) 2022/2.065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale), precum și pentru modificarea și completarea Legii nr. 365/2002 privind comerțul electronic

bancare. În acest sens, au fost adoptate mai multe măsuri de combatere a infracțiunilor informatice constând în cooperarea cu alte instituții/autorități, instituții bancare și entități din mediul privat.

De asemenea, în vederea combaterii infracțiunilor informatice, evidențiem și faptul că ofițeri din cadrul Inspectoratului General al Poliției Române au fost desemnați persoane de contact în cadrul operațiunilor *HAECHE* și *FIRSTLIGHT*, derulate de către INTERPOL Financial Crime and Anti-Corruption Centre, care vizează următoarele moduri de operare: *Voice Phishing*, *Love/Romance Scam*, *Online Sextortion*, *Investment Fraud*, *Money Laundering Associated with Illegal Online Gambling*, *Business Email Compromise (BEC) Fraud* și *E-Commerce Fraud*.

Totodată, este important de menționat și faptul că, în domeniul de referință, Inspectoratul General al Poliției Române cooperează cu Parchetul de pe lângă Înalta Curte de Casație și Justiție, Autoritatea Națională pentru Administrare și Reglementare în Comunicații, Directoratul Național de Securitate Cibernetică și Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București, inclusiv prin schimb de informații în scopul prevenirii, detectării, investigării și sancționării faptelor de criminalitate informatică și a celor săvârșite prin sisteme informatice sau mijloace de comunicare electronică.

Cu deosebită considerație,



**VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE**

**Marian-Cătălin PREDOIU
SECRETAR DE STAT
ANGELICA FĂDOR**