



SECRETARIATUL GENERAL AL GUVERNULUI
DEPARTAMENTUL PENTRU RELAȚIA CU PARLAMENTUL



**Nr. 3612, 3613, 3614, 3615, 3616, 3617, 3618,
3620, 3632, 3633, 3652, 3653, 3654, 3655,
3656, 3657, 3658, 3659, 3660, 3661, 3662,
3663, 3675, 3676, 3677, 3678, 3610, 3611,
3619, 3631, 3643, 3644, 3645, 3646, 3647,
3648, 3649, 3651, 3674/2025**

16-05-2025

**Către: Domnul Cezar-Mihail DRĂGOESCU
Secretar al Camerei Deputaților**

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

Stimate domnule 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

Către,
PARLAMENTUL ROMÂNIEI
CAMERA DEPUTAȚILOR
Domnului deputat Ioan BALAN

Stimate domnule deputat,

În legătură cu întrebarea dumneavoastră, înregistrată la Camera Deputaților cu nr. 910A/2025, având ca obiect „Necesitatea adoptării unor măsuri și constituirea unor grupuri de lucru interministeriale pentru combaterea înșelăciunilor online sau prin mijloace de comunicare la distanță.”, precizăm următoarele:

Criminalitatea informatică reprezintă una dintre cele mai dinamice și provocatoare amenințări la adresa siguranței cetățenilor și a stabilității economice. Prin urmare, prevenirea criminalității informatice reprezintă o prioritate pentru Poliția Română, iar creșterea gradului de conștientizare în rândul cetățenilor cu privire la cunoașterea și importanța aplicării principalelor măsuri de siguranță în mediul online reprezintă elemente cheie în reducerea posibilităților de succes ale multor forme de criminalitate informatică.

Menționăm că Poliția Română cooperează cu instituțiile omoloage din alte țări membre UE sau din alte state partenere, cu obiectivul schimbului de bune practici în sfera securității cibernetice și a combaterii fraudelor online.

Schimbul de informații între structurile Poliției Române și parteneri din alte state se realizează prin canalele de cooperare existente și gestionate la nivelul Centrului de Cooperare Polițienească Internațională din cadrul Inspectoratului General al Poliției Române, structură specializată în schimbul de informații operative, inclusiv cu statele UE și non-UE și se realizează în baza reglementărilor prevăzute în legislația națională.

Diversificarea continuă a modului de operare al grupărilor infracționale – de la fraude bancare complexe, atacuri cibernetice asupra infrastructurilor critice, până la sofisticate campanii de manipulare online – relevă un fenomen profund transnațional, în continuă adaptare și sofisticare tehnologică.

Această evoluție alarmantă este confirmată și în cel mai recent Raport privind Amenințările Infracționalității Organizate pe Internet (IOCTA), elaborat de Europol, care arată că tipul de criminalitate cibernetică nu doar că s-a extins ca arie de manifestare, dar a devenit și mai agresivă, mai orientată spre profit și mai greu de anticipat. Sunt vizate atât datele financiare, cât și identitatea digitală a cetățenilor, sistemele de plată, rețelele corporative sau chiar instituțiile publice.

Telefon: 021.264.87.07/Fax: 021.264.87.40/ e-mail: dgi_sccretariat@mai.gov.ro
Piata Revoluției, nr.1A, sector 1, C.P.010066
RO – București

DGJ/S2/CG

Nr. 3648 / DRP
DATA 14.05.2025

Nesecret

Nr. ex. 1

București,

Nr. 12659 din 13.05.2025

Convenția Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001 (ratificată de România prin Legea nr. 64/2004) servește drept bază pentru cooperarea internațională între părțile la convenție, sens în care părțile sunt membre ale Comitetului Convenției și fac schimb de informații și de experiență, evaluează punerea în aplicare a convenției sau interpretează convenția prin intermediul unor note de orientare.

În anul 2024, la București, a avut loc Conferința cu tema C-PROC: 10 ani de cooperare pentru consolidarea capacităților în domeniul criminalității informatice între România și Consiliul Europei la care au participat reprezentanți din cadrul Ministerului Justiției, Parchetului de pe lângă Înalta Curte de Casație și Justiție, Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, Poliției Române, Directoratului Național de Securitate Cibernetică, Serviciului Român de Informații, Oficiului Național de Prevenire și Combateră a Spălării Banilor.

Menționăm faptul că, în octombrie 2013, Consiliul Europei a semnat cu Guvernul României un memorandum pentru înființarea unui birou dedicat programelor de asistență în domeniul criminalității informatice [Cybercrime Programme Office (C-PROC)] în București cu un obiectiv clar: sprijinirea țărilor din întreaga lume în întărirea capacităților autorităților judiciare în ceea ce privește criminalitatea informatică și probele electronice.

În acest context, România își asumă un rol activ și responsabil în cadrul EMPACT (Platforma multidisciplinară europeană împotriva amenințărilor infracționale), instrument-cheie al Uniunii Europene pentru combaterea criminalității grave și organizate fiind desemnată co-driver pentru pilonul dedicat fraudelor online, alături de Franța (în calitate de driver) și Grecia. În cadrul EMPACT 2022-2025 criminalitatea informatică este tratată ca o prioritate strategică, iar țara noastră participă cu specialiști și resurse operaționale la misiuni comune, acțiuni de prevenire, schimburi de informații și dezvoltarea de bune practici în investigarea infracțiunilor informatice.

De asemenea, menționăm faptul că, în cursul anului 2024, între Parchetul de pe lângă Înalta Curte de Casație și Justiție, Inspectoratul General al Poliției Române și Asociația Română a Băncilor a fost semnat un protocol de colaborare, prin care au fost instituite unele măsuri de cooperare între instituțiile bancare și instituțiile de aplicare a legii.

Acesta reprezintă un instrument de o reală utilitate în scopul îmbunătățirii modului de lucru cu instituțiile financiar bancare privind, pe de-o parte, punerea în executare cu celeritate a dispozițiilor procedurale referitoare la obținerea de date privind situația financiară a unei persoane, obținerea datelor privind tranzacțiile financiare ale unei persoane, date informatice, obiecte sau înscrisuri care pot servi ca mijloc de probă, sesizarea unor fapte penale sau instituirea de măsuri asiguratorii, în conformitate cu dispozițiile Codului de procedură penală, iar pe de altă parte, realizarea obiectivelor și obligațiilor legale prudentiale prevăzute de legislația privind prevenirea și combaterea riscurilor de fraudă și spălare de bani în realizarea activității specifice a instituțiilor financiar bancare.

În prezent, este în curs de dezvoltare soluția tehnică ce va permite schimbul de date în mod eficient și securizat în vederea punerii în aplicare a protocolului.

România, prin Ministerul Afacerilor Interne a sprijinit atât înființarea la nivelul EUROPOL a Centrului European de combatere a criminalității informatice (EC3) pentru a ajuta statele

membre să ancheteze infracțiunile online și să destructureze rețelele infracționale, precum și consolidarea cooperării cu această structură specializată.

Astfel, au fost numeroase cazuri în care s-a cooperat cu EC3 în dosare penale de criminalitate informatică, în care cetățeni români au fost autori ai activităților ilegale sau situații în care cetățeni români, autorități sau instituții private din România au fost victime. Colaborarea a constat în schimb de date și informații, realizarea de întruniri operative cu alte state membre UE sau terțe.

Totodată, participăm activ la Joint Cybercrime Action Taskforce (J-CAT) din cadrul EC3 care aduce un aport operativ prin investigații și operațiuni transfrontaliere la combaterea criminalității informatice în interiorul și în afara UE.

În susținerea celor menționate, exemplificăm o operațiune internațională care a dus la confiscarea mai multor domenii de internet care au fost folosite de infractorii cibernetici pentru a vinde malware care a fost condusă de FBI și susținută de Europol și Joint Cybercrime Action Taskforce (J-CAT). State participante: Australia, Canada, Croația, Finlanda, Germania, Malta, Țările de Jos, Nigeria, România și SUA¹.

De asemenea, la 01 octombrie 2024 cea de a treia fază a Operațiunii Cronos a implicat efortul colectiv și de lungă durată al autorităților de aplicare a legii din 12 țări (Canada, Franța, Germania, Japonia, Spania, Suedia, Elveția, Țările de Jos, România, UK, SUA), Europol și Eurojust, care și-au unit forțele pentru a destructura la toate nivelurile operațiunile criminale ale grupului de ransomware LockBit².

În același timp, trebuie subliniat că Strategia ProtectEU, lansată de Comisia Europeană, include în mod clar criminalitatea informatică printre domeniile prioritare ale efortului comun european împotriva criminalității grave. România sprijină principiile acestei strategii și se află în etapa de analiză a mecanismelor prin care direcțiile de acțiune vor fi implementate la nivel național, în completarea angajamentelor deja asumate prin EMPACT și alte instrumente europene.

De asemenea, România dezvoltă relații de cooperare bilaterală cu statele vecine – în special Republica Moldova și Ucraina.

Dezvoltarea cooperării internaționale în vederea prevenirii și combaterii criminalității transfrontaliere, mai ales a celei informatice, reprezintă o preocupare constantă a Ministerului Afacerilor Interne, fiind desfășurate acțiuni concrete pentru îmbunătățirea acesteia, precum:

- realizarea de întâlniri operative și schimburi de date și informații cu ofițerii de legătură aflați la post în România, în vederea probării cauzelor penale aflate în lucru sau acordării de sprijin operațional unităților de poliție similare din Republica Moldova sau Ucraina;
- realizarea unui schimb permanent de date și informații cu structurile de aplicare a legii din străinătate (INTERPOL, EUROPOL, S.E.L.E.C., ofițeri de legătură, atașați de afaceri interne etc.), în vederea identificării grupărilor infracționale de criminalitate organizată itinerante și a membrilor acestora. În acest context, se urmărește acordarea/solicitarea în permanență a sprijinului polițienesc de către și către autoritățile statelor vizate de activitățile infracționale, care să contribuie în mod efectiv la destructurarea grupărilor de criminalitate organizată transfrontalieră implicate;

¹ În acest sens este și comunicatul de presă de pe site-ul Europol din data de 12.02.2024;

² În acest sens este și comunicatul de presă de pe site-ul Europol din data de 01.10.2024.

- punerea în aplicare a formelor de asistență judiciară în materie penală (comisii rogatorii, ordine europene de anchetă, echipe comune de anchetă – joint investigation teams, etc).

Totodată, menționăm că structurile de aplicare a legii din cele trei state (România, Republica Moldova, Ucraina) cooperează în baza Acordului între Guvernul României, Guvernul Republicii Moldova și Cabinetul de Miniștri al Ucrainei privind colaborarea în combaterea criminalității, semnat la Kiev, la 06 iulie 1999, ratificat prin Legea nr. 70/2001.

De asemenea, Ministerul Afacerilor Interne din România urmărește consolidarea cooperării cu autoritățile din Ucraina, pentru prevenirea și combaterea criminalității transfrontaliere, ce include fenomenul criminalității informatice, fiind în prezent întreprinse demersuri pentru identificarea de acțiuni și proiecte concrete ce ar putea fi desfășurate de structurile operative ale ministerului nostru împreună cu Serviciul de Stat pentru Comunicații Speciale și Protecția Informațiilor din Ucraina (SSCSPI) în domeniul cyber.

În relația cu Republica Moldova, Ministerul Afacerilor Interne urmează să implementeze împreună cu Ministerul Afacerilor Interne din Republica Moldova, proiectul “Centru Operațional Cyber la nivelul MAI din RMD”, dezvoltat în cadrul Programului Interreg NEXT RO-RMD 2021-2027. Proiectul va contribui la creșterea capacității de reacție în cazul unor atacuri cibernetice asociate infrastructurii IT&C care deservește managementul frontierei România – Republica Moldova și va contribui și la intensificarea schimbului de date/informații în domeniul cyber, în general (termenul estimat pentru inițierea activităților este iunie 2025).

În ceea ce privește cooperarea interinstituțională, la nivel național sunt derulate inițiative consolidate care vizează prevenirea și combaterea criminalității informatice. Un exemplu relevant este proiectul de conștientizare #SiguranțaOnline, desfășurat în parteneriat între Poliția Română, Directoratul Național de Securitate Cibernetică și Asociația Română a Băncilor, care are drept scop informarea cetățenilor cu privire la riscurile asociate fraudelor de tip spoofing și promovarea comportamentului responsabil în mediul digital. De asemenea, la nivelul Poliției Române a fost înființată pagina www.sigurantaonline.ro, proiect prin care Poliția Română a informat cetățenii cu privire la noile moduri de operare din sfera criminalității informatice, inclusiv modul de operare „investment fraud”, furnizând, totodată, sfaturi pentru creșterea gradului de conștientizare și educație a populației privind riscurile potențiale ale diverselor fraude informatice.

Acest tip de colaborare demonstrează eficiența unei abordări comune și proactive în fața amenințărilor cibernetice care vizează direct populația, în special prin utilizarea tehnicilor de inginerie socială.

Totodată, considerăm că aceste inițiative trebuie completate și extinse printr-o cooperare structurată cu mediul privat, mediul academic și societatea civilă în special cu actorii din domeniile financiar, telecomunicații, IT și e-commerce, care dețin infrastructuri critice sau interacționează direct cu utilizatorii vizați de fraude informatice. Implicarea acestora în eforturile de prevenție, reacție rapidă și educație digitală este esențială pentru consolidarea unui ecosistem național de securitate cibernetică eficient și adaptat realităților în continuă schimbare.

În context, precizăm faptul că instituția noastră, prin structurile cu competențe în domeniu, colaborează cu alte instituții implicate în aplicarea legii, de regulă, prin intermediul sistemului judiciar, care funcționează potrivit reglementărilor procesual penale, procesual civile, dar și în

conformitate cu legislația primară și secundară care reglementează atribuțiile și competențele structurilor ce compun acest sistem.

De asemenea, ne manifestăm în continuarea disponibilitatea de a participa la orice inițiative de natură să consolideze colaborarea instituțională și de a acorda sprijin de specialitate, potrivit competențelor.

Suntem într-o competiție globală pentru inovare și dezvoltare tehnologică în care colaborarea internațională este esențială pentru dezvoltarea în siguranță a infrastructurii digitale, iar sectoarele IT și cel bancar, trebuie să aibă o contribuție semnificativă pe acest palier. Succesul acestor inițiative va depinde și de capacitatea noastră de a valorifica capitalul și cunoașterea existente la nivelul companiilor private, transformând provocările în oportunități. Statul nu poate și nu trebuie să fie singurul motor al asigurării unei infrastructuri digitale sigure.

Prin stimularea dialogului public-privat și dezvoltarea de mecanisme comune de alertare, intervenție și informare, putem reduce semnificativ expunerea cetățenilor și a companiilor la riscurile generate de criminalitatea informatică și putem crea un front unit în protejarea cetățenilor români și în salvagardarea intereselor acestora.

Cu deosebită considerație,


P **VICEPRIM-MINISTRU,**
MINISTRUL AFACERILOR INTERNE

Marian-Cătălin PREDOIU

SECRETAR DE STAT
SILVIU NICU MACOVEI