ÎNTREBARE PARLAMENTARĂ

Nr.5448A/04.06.2026

A/PNL/364
4.06.2026

Către: Domnului Marian Pîrvu, Președinte al Oficiului Național de Prevenire și Combatere a Spălării Banilor (ONPCSB)

De la: Sebastian-Ioan Burduja, Deputat PNL, Circumscripția Electorală Nr. 42 București

Obiectul întrebării: Capacitatea operațională a Unității de Informații Financiare a României de detectare, analiză și diseminare a indicatorilor de risc privind canalele de plată ruse (Korona Pay, Profee, Unistream, Mir Card, SBP), ecosistemul cripto rusesc și rețelele paravan de tip „A7". Cooperarea Egmont Group și cu serviciile naționale de informații. Tipologii de spălare a banilor, finanțare a terorismului de stat și utilizare a fluxurilor financiare pentru întreținerea operativilor serviciilor ruse de informații

Stimate Domnule Președinte,

În perioada 2022-2026, în paralel cu adoptarea progresivă a celor 20 de pachete de sancțiuni ale Uniunii Europene împotriva Federației Ruse, regimul de la Moscova și rețelele aliate au reconstruit, prin procese de remediere financiară, o arhitectură de canale de plăți și transferuri menite să eludeze regimul sancționatoriu. Această arhitectură include sisteme de plăți rezidente (Mir Card, Sistem de plăți rapide SBP), sistemul rusesc alternativ de mesagerie financiară SPFS, operatori de remitențe transfrontaliere cu acoperire în spațiul UE și Comunitatea Statelor Independente (Korona Pay/Zolotaya Korona, Profee, Unistream), un ecosistem cripto operat din și pentru beneficiari ruși și belarusi, precum și rețele financiare-paravan operate prin jurisdicții terțe, dintre care „A7 network", sancționată de Regatul Unit la 26 mai 2026, este cel mai documentat exemplu de rețea Kremlin-linked care utilizează Kîrgîzstanul pentru ascunderea originii fondurilor.

Korona Pay, operat de RNKO Platezhny Tsentr, parte a grupului CFT (Centrul de Tehnologii Financiare), a fost, în 2022-2024, unul dintre cele mai utilizate canale alternative pentru transferul de bani din Uniunea Europeană către Federația Rusă, ulterior fiind inclus în regimul european de sancțiuni. Profee, un alt operator de remitențe utilizat de comunitățile ruse din UE pentru transferuri directe de pe carduri europene către carduri rusești, a fost adăugat regimului sancționatoriu prin pachetul 19 al Consiliului UE, adoptat la 23 octombrie 2025. Pachetul 20, adoptat în aprilie 2026, a introdus un ban sectorial cuprinzător pe toate tranzacțiile cu furnizorii de servicii cu cripto-active stabiliți în Federația Rusă și Belarus, restricție care marchează schimbarea de paradigmă a regimului european.

Cu toate acestea, indicii operaționale documentate de mass-media de specialitate și de rapoarte ale think-tank-urilor europene de profil semnalează că, pe teritoriul mai multor state membre UE, inclusiv în România, instrumente precum Korona Pay și echivalentele continuă să fie accesibile, fie direct, fie prin redirecționare către jurisdicții terțe (Serbia, Kazahstan, Kîrgîzstan, Turcia, Emiratele Arabe Unite), prin utilizarea unor agenți de tip „cash-in/cash-out" și prin recurs la cripto-active mixate prin protocoale de tip mixer. Tipologiile identificate de FATF, FinCEN, Europol Financial Intelligence Group și de centrele de cercetare independente (Royal United Services Institute, Atlantic Council) includ utilizarea acestor canale pentru: finanțarea bugetului de război al Federației Ruse prin redirecționarea veniturilor petroliere ale flotei-fantomă, întreținerea oligarhilor sancționați rezidenți în UE, menținerea unei finanțări permanente a operațiunilor de influență hibridă, plata cu prudență a unor categorii de operativi acoperiți ai serviciilor ruse de informații (FSB, SVR, GRU) și de combatere a contrainteligenței, precum și, în ipoteza unor anchete deschise în statele baltice și Polonia, finanțarea unor activități criminale conexe (proxenetism, trafic de armament cu rază scurtă, droguri de sinteză, trafic de persoane) organizate de structuri legate de rețelele Bratva și Solntsevskaya care folosesc spațiul european ca platformă logistică.

Statele membre care au tratat această problematică cu seriozitate operațională au răspuns. Republica Letonă a închis sucursalele Rietumu Banka pe componente de afaceri rusești și a anchetat sistematic ABLV Bank pentru fluxuri de spălare. Republica Lituania a interzis Mir Card și a aplicat un regim de sancțiuni secundare împotriva entităților terțe. Regatul Unit a sancționat, la 26 mai 2026, „A7 network", 18 entități și persoane fizice acuzate de oferirea de servicii financiare, tehnologie și resurse Guvernului Federației Ruse, inclusiv prin operațiuni în Kîrgîzstan. Statele Unite au sancționat anterior, prin OFAC, Garantex Europe OÜ și operațiuni conexe. România, în calitate de stat membru UE și NATO și stat de frontieră cu Republica Moldova și Ucraina, are obligația juridică, operațională și politică de a se ridica la același standard.

Toleranța de facto a unor instrumente sancționate ori care funcționează în zona gri a regimului european de sancțiuni transformă teritoriul național, prin chiar inacțiunea autorităților, într-o platformă indirectă de alimentare cu lichidități a Federației Ruse și a complexului ei militar-industrial, în paralel cu utilizarea acelorași canale de către structuri ostile de informații pentru întreținerea operativilor acoperiți, transferul de resurse către agenți recrutați, plata informatorilor și transmiterea de plăți codate ca formă de comunicare operațională. În contextul în care Federația Rusă a atacat cu dronă teritoriul național la 29 mai 2026 (Galați), continuarea operării unor canale prin care cetățeni români direcționează lichidități în Federația Rusă pune România în poziția unui participant indirect, prin omisiune, la efortul de război al unui stat agresor.

Oficiul Național de Prevenire și Combatere a Spălării Banilor este Unitatea de Informații Financiare (FIU) a României, conform art. 1 din Legea nr. 129/2019 privind

prevenirea și combaterea spălării banilor și finanțării terorismului. ONPCSB este destinatar primar al rapoartelor de tranzacții suspecte (STR), al rapoartelor de tranzacții cu numerar peste prag și al rapoartelor de transfer extern, este responsabil pentru analiza tactică și strategică a informațiilor financiare, pentru diseminarea către organele de urmărire penală, pentru cooperarea cu FIU-urile partenere prin Egmont Group și cu Europol Financial Intelligence Public Private Partnership (EFIPPP), precum și pentru cooperarea operativă cu SRI, SIE, DGIA, DGPI și DIICOT.

Având în vedere aceste considerente, în temeiul art. 112 alin. (1) din Constituția României, republicată, precum și al art. 194-201 din Regulamentul Camerei Deputaților, cu modificările și completările ulterioare, vă adresez, în scris, următoarele întrebări:

1. Câte STR-uri (Suspicious Transaction Reports) și SAR-uri (Suspicious Activity Reports) au fost primite de ONPCSB în perioada 24 februarie 2022 - 1 iunie 2026 cu indicator de risc „Federația Rusă / Belarus / sanctions evasion”? Dezagregarea solicitată pe categorii: (i) cetățeni ruși/belaruși PEP și sancționați; (ii) cetățeni români cu rude apropiate pe listele UE de sancțiuni; (iii) entități juridice cu acționariat rusesc/belarus peste 40%; (iv) operatori de remitențe (Korona Pay, Profee, Unistream, Western Union retail, MoneyGram retail); (v) CASP-uri și exchange-uri cripto cu fluxuri identificate către wallet-uri din ecosistem rusesc?
2. Care este tipologia consolidată ONPCSB a indicatorilor de risc pentru transferurile prin Korona Pay și echivalentele în zona gri a regimului european de sancțiuni? Tipologia ONPCSB include „smurfing” transfrontalier prin agenți cash-in/cash-out, layering prin jurisdicții terțe (Serbia, Kazahstan, Kîrgîzstan, EAU), utilizarea cripto-asseturilor mixate prin mixere de tip Tornado Cash echivalente, „chain hopping” cross-blockchain și utilizarea „nested accounts” în CASP-uri din terțe jurisdicții?
3. Cum apreciază ONPCSB integrarea operațională a metodologiei „Russia-specific red flags” publicate de FATF în Recomandarea 21 și în Recomandarea 16 (Travel Rule), precum și a Notei FinCEN FIN-2022-Alert001 privind evaziunea sancțiunilor împotriva Rusiei? Sunt aceste tipologii transpuse în Ghidul de tipologii ONPCSB transmis entităților raportoare conform art. 11 din Legea nr. 129/2019?
4. ONPCSB a deschis, în perioada de referință, dosare de analiză strategică privind utilizarea canalelor financiare ruse pentru: (i) întreținerea pe teritoriul național a unor operativi acoperiți ai FSB, SVR, GRU; (ii) plata informatorilor recrutați; (iii) transmiterea de plăți codate cu funcție de semnalizare operațională (signaling payments) sub valoarea de raportare; (iv) finanțarea unor structuri criminale ruse de tip Solntsevskaya, Bratva, Tambovskaya cu activitate identificată în spațiul european? Care sunt rezultatele acestor analize și ce diseminări s-au făcut către SRI, SIE și DIICOT?

5. Cum se materializează cooperarea ONPCSB cu FIU-urile partenere prin Egmont Group, în special cu FIU-urile statelor baltice (FIA Estonia, Kontrolē Latvia, FNTT Lituania), cu FIU-ul polonez (GIIF), cu FIU-ul ucrainean (SFMS) și cu unitățile din Cipru și Germania (FIU Germany - Zollkriminalamt), pe componenta canalelor de plată ruse? Câte schimburi bilaterale s-au realizat pe această temă în 2025-2026 și ce informații operaționale au fost obținute?
6. Care este capacitatea ONPCSB de chain analysis pe ecosistem cripto, prin raportare la furnizorii de soluții comerciale (Chainalysis Reactor, TRM Labs, Elliptic) și la capabilitățile OSINT proprii? Câți analiști specializați pe blockchain forensics operează la 2 iunie 2026 și care este bugetul anual al ONPCSB pentru subscripții la astfel de instrumente?
7. ONPCSB participă la Anti-Money Laundering Operational Network (AMON) al Europol și la EFIPPP (Europol Financial Intelligence Public Private Partnership)? Care este contribuția ONPCSB la grupul AP Sustrans (Sanctions Evasion) al Europol și la operațiuni JIT (Joint Investigation Teams) coordonate prin Eurojust pe cauze de evaziune a sancțiunilor?
8. Cum apreciază ONPCSB compatibilitatea capacității sale operaționale cu noul cadru AMLA (Authority for Anti-Money Laundering and Countering the Financing of Terrorism), cu sediul la Frankfurt, înființată prin Regulamentul (UE) 2024/1620, în privința supravegherii directe a entităților raportoare cu risc ridicat? Care este planul de transfer de date, de competențe și de personal asumat de ONPCSB pentru perioada de pre-operaționalizare AMLA 2026-2028?
9. Care este planul ONPCSB privind emiterea unui ghid specific privind canalele financiare ruse, asemănător celui publicat de FIU-ul britanic (NCA NECC), pentru entitățile raportoare (instituții de credit, instituții de plată, operatori de remitențe, CASP-uri, notari, avocați, contabili autorizați, agenții imobiliare, dealeri de metale prețioase și pietre)? Care este orizontul de adoptare?
10. Care este poziția ONPCSB privind utilizarea, în România, de către cetățeni ruși și cetățeni români cu legături rusești, a unor structuri SRL românești și de tip „shell” pentru spălare de bani, prin schemă de tip „layering” imobiliar și prin achiziții supraevaluate de active reale? Care este numărul cazurilor de „unexplained wealth” identificate la titulari ruși/belaruși pe teritoriul național în perioada de referință?
11. ONPCSB are cunoștință și a transmis diseminări către DIICOT privind utilizarea unor canale financiare ruse pentru finanțarea unor activități infracționale conexe, cu participarea unor cetățeni ruși sau a unor structuri legate de aceștia, în privința traficului de armament, traficului de droguri sintetice, traficului de persoane sau proxenetismului, pe teritoriul național? Care este, la nivelul ONPCSB, calificarea acestor fluxuri ca finanțare a terorismului de stat conform Legii nr. 535/2004 privind prevenirea și combaterea terorismului?

Solicit răspuns în scris, în termenul prevăzut de Regulamentul Camerei Deputaților.

Cu deosebit respect,

Sebastian-Ioan BURDUJA

Deputat PNL