

Aprobat în ședința Guvernului din ____/____/2026
prin decizia protocolară nr. ____/2026

Proiect

L E G E
pentru modificarea Legii nr. 72/2025
comunicațiilor electronice

Parlamentul adoptă prezenta lege organică.

Articolul I. – Legea nr. 72/2025 comunicațiilor electronice (Monitorul Oficial al Republicii Moldova, 2025, nr. 226-228, art. 266), se completează cu articolul 125¹, cu următorul cuprins:

„**Articolul 125¹** – Identificarea abonaților serviciilor de comunicații electronice mobile accesibile publicului

(1) Furnizorii de servicii de comunicații electronice mobile accesibile publicului sunt obligați să identifice abonații serviciilor respective, indiferent de tipul ofertei (abonament sau cartelă preplătită), la momentul încheierii contractului de abonament sau, în cazul cartelelor preplătite, cel târziu la momentul activării acestora.

(2) Identificarea abonaților se realizează în baza unui act de identitate valabil sau prin mijloace de identificare electronică, cu colectarea cel puțin a următoarelor date:

1) pentru persoanele fizice care se identifică cu acte de identitate emise de Republica Moldova – numele, prenumele, IDNP, datele actului de identitate (denumirea, seria, numărul); furnizorul verifică datele și valabilitatea acestuia prin interogarea gratuită a Sistemului informațional automatizat „Registrul de stat al populației”, în condițiile legii;

2) pentru persoanele fizice care se identifică cu acte de identitate emise de alte state – numele, prenumele, datele actului de identitate (denumirea, seria, numărul și data expirării); furnizorul poate reține o copie a actului de identitate, în condițiile legislației privind protecția datelor cu caracter personal;

3) pentru persoanele juridice din Republica Moldova – denumirea, IDNO, precum și datele prevăzute la subpunctele 1) sau 2) referitoare la persoana împuternicită să reprezinte abonatul în legătură cu identificarea acestuia, cu verificarea datelor prin interogarea gratuită a Sistemului informațional „Registrul de stat al unităților de drept”, în condițiile legii;

4) pentru persoanele juridice din alte state – denumirea, țara de origine și numărul de înregistrare în registrul comercial al statului străin, precum și datele prevăzute la subpunctele 1) sau 2) referitoare la persoana împuternicită să

reprezintă abonatul în legătură cu identificarea acestuia, furnizorul reține copia documentului care atestă înregistrarea, cu traducere legalizată în limba română, în condițiile legii.

(3) La alegerea furnizorilor, identificarea abonaților serviciilor de comunicații electronice mobile accesibile publicului poate fi efectuată prin una sau mai multe dintre următoarele metode:

- 1) în punctele de vânzare proprii ale furnizorului;
- 2) în punctele de vânzare ale persoanelor împuternicite de furnizor, în baza unui contract sau a unui alt temei juridic corespunzător;
- 3) la distanță, prin:
 - a) mijloace de identificare electronică (semnătură electronică calificată sau avansată), sau alte mijloace electronice oferite de către un prestator de servicii de încredere calificat, în condițiile Legii nr. 124/2022 privind identificarea electronică și serviciile de încredere și ale actelor normative subsecvente;
 - b) mijloace digitale, constând într-un proces de identificare și de verificare a identității persoanei fizice în baza actelor de identitate prezentate, a măsurătorilor semnalmentelor biometrice faciale, a comparării de imagini și a informațiilor comunicate de persoana fizică și preluate gratuit din Sistemul informațional automatizat „Registrul de stat al populației”, utilizând mijloace digitale;
 - c) sistemul guvernamental de identitate digitală (EVO), administrat de autoritatea publică competentă;
 - d) alte mijloace electronice oferite de către furnizor, în cazul în care datele de identificare ale abonatului au fost anterior verificate în legătură cu un alt număr prin una dintre metodele prevăzute la subpunctele 1) - 3).

(4) Până la finalizarea procesului de identificare, cartelele SIM/eSIM pot fi utilizate doar pentru serviciile tehnice minime necesare stabilite de autoritatea de reglementare, dacă este fezabil.

(5) Furnizorii de servicii de comunicații electronice mobile accesibile publicului păstrează datele de identificare ale utilizatorilor ale căror cartele au fost activate, pe întreaga durată de utilizare a serviciului și pentru o perioadă de 12 luni de la încetarea utilizării numărului, în conformitate cu art. 125 alin. (3) și cu legislația privind protecția datelor cu caracter personal.

Articolul II. – Prezenta lege intră în vigoare la expirarea a 24 de luni de la data publicării în Monitorul Oficial al Republicii Moldova și se aplică doar numerelor activate după data intrării în vigoare a prezentei legi.

PREȘEDINTELE PARLAMENTULUI

NOTA DE FUNDAMENTARE
la proiectul de lege pentru modificarea Legii comunicațiilor electronice nr. 72/2025

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ
1.1 Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ <i>Autor:</i> Ministerul Afacerilor Interne
2. Condițiile ce au impus elaborarea proiectului actului normativ
2.1 Temeiul legal sau, după caz, sursa proiectului actului normativ În perioada anilor 2022-2025, Republica Moldova s-a confruntat cu o creștere accelerată a criminalității comise prin intermediul comunicațiilor electronice, pe fondul intensificării amenințărilor hibride și al utilizării pe scară tot mai largă a tehnologiilor mobile în activități ilicite. Actualul cadru normativ, care permite procurarea și utilizarea cartelelor SIM preplătite fără identificarea titularului, nu mai corespunde realităților de securitate, generând o vulnerabilitate majoră pentru securitatea națională și pentru ordinea publică. Cartelele preplătite anonime au devenit un instrument preferat al grupărilor infracționale, fiind utilizate în escrocherii bancare și fraude informatice, în trafic de droguri (inclusiv droguri sintetice de tip PVP comercializate prin „magazine online”), în scheme de înșelăciune pe platforme digitale, în apeluri false către 112 și în activități de crimă organizată, inclusiv operarea dronelor în scopuri ilegale. Investigațiile recente privind finanțarea ilegală a campaniilor electorale au evidențiat folosirea a zeci de mii de astfel de cartele, demonstrând caracterul sistemic al problemei și impactul direct asupra proceselor democratice. În lipsa unui mecanism legal de identificare obligatorie, atribuirea certă a unui număr de telefon unei persoane concrete este extrem de dificilă. Această situație întârzie identificarea suspectilor, îngreunează administrarea probelor digitale și reduce eficiența urmăririi penale. Totodată, anonimatul cartelelor sporește riscul erorilor de atribuire, cu consecințe asupra drepturilor fundamentale ale persoanelor neimplicate. Contextul regional complicat accentuează și mai mult această vulnerabilitate. În condițiile în care în multiple state membre ale Uniunii Europene a fost introdusă deja obligativitatea înregistrării cartelelor preplătite, Republica Moldova riscă să devină o sursă de cartele anonime pentru rețele criminale transfrontaliere. Analiza cadrului juridic al Uniunii Europene relevă un punct de plecare fundamental: în prezent, nu există o reglementare armonizată la nivelul UE care să impună sau să interzică în mod specific înregistrarea obligatorie a utilizatorilor de cartele SIM preplătite. Această problemă este lăsată, prin urmare, la latitudinea și competența legislativă a fiecărui stat membru, care poate decide dacă impune astfel de măsuri pe teritoriul său național. Această lipsă de armonizare, deși confirmă autonomia statală, a generat o vulnerabilitate de securitate transfrontalieră semnificativă. Un document de lucru recent al Președinției Poloneze a Consiliului a evidențiat această problemă ca fiind o amenințare directă la adresa securității publice în spațiul UE¹. Documentul argumentează că infractorii exploatează în mod activ „lipsa unor norme armonizate” prin practicarea unui „arbitraj infracțional”. Aceștia „<i>achiziționează în mod anonim cartele SIM din state membre care nu impun înregistrarea identității și le utilizează ulterior pentru a comite fapte ilegale în alte state membre care au controale mai stricte</i>”.

¹ <https://data.consilium.europa.eu/doc/document/ST-5556-2025-INIT/en/pdf>

Amenințările specifice identificate ca fiind facilitate de anonimatul cartelelor SIM preplătite sunt diverse și grave. Acestea includ facilitarea comunicațiilor criptate (întrucât majoritatea aplicațiilor de mesagerie securizată, precum Signal sau Telegram, necesită un număr de telefon valid pentru activare), traficul de droguri, fraudă, terorismul și diverse forme de criminalitate cibernetică. Documentul polonez subliniază că „accesul nerestricționat” la cartelele SIM preplătite „face accesul la acest tip de comunicare mult mai ușor pentru infractori”.

Această situație creează o discrepanță juridică complexă între obiectivele Pieței Unice (libera circulație a serviciilor) și imperativele justiției și afacerilor interne. La o primă vedere, absența unei Directive specifice privind înregistrarea SIM-urilor ar putea fi interpretată greșit ca un „vid juridic” care oferă unui stat o libertate legislativă totală. Această interpretare este incorectă și ar conduce la elaborarea unei legislații vulnerabile.

Vidul de reglementare se aplică strict normelor specifice pieței telecomunicațiilor. Acest vid este însă imediat și complet complementat de legislația orizontală a Uniunii Europene privind drepturile fundamentale, care se aplică oricărei prelucrări de date cu caracter personal. Actele normative relevante în acest context sunt Regulamentul general privind protecția datelor (RGPD) și Directiva asupra confidențialității și a comunicațiilor electronice (ePrivacy).

Prin urmare, deși un stat membru este liber să legislaze în acest domeniu, legislația națională nu va fi evaluată în raport cu o inexistentă „*Directivă SIM*”. Măsura va fi examinată exclusiv prin prisma conformității cu standardele stricte de derogare prevăzute la articolul 23 din RGPD și articolul 15 din Directiva ePrivacy. Justificarea măsurii nu poate avea un caracter comercial, ci trebuie concepută *ab initio* ca o derogare în materia securității publice, respectând riguros testele de necesitate și proporționalitate impuse de acquis-ul UE în domeniul protecției datelor și de jurisprudența Curții de Justiție a Uniunii Europene (CJUE).

Actul constitutiv principal care reglementează piața telecomunicațiilor în UE este Directiva (UE) 2018/1972 privind instituirea Codului european al comunicațiilor electronice. Obiectivele sale sunt preponderent economice: promovarea concurenței, stimularea investițiilor în rețele de foarte mare capacitate, dezvoltarea pieței interne de comunicații electronice și asigurarea unui nivel ridicat de protecție a consumatorilor.

În contextul unei măsuri naționale privind înregistrarea SIM-urilor, Codului european al comunicațiilor electronice conține o „clauză de salvagardare” esențială, enunțată în Considerentul (6). Acesta precizează că Directiva nu aduce atingere posibilității statelor membre de a adopta „*măsurile necesare pentru a asigura protecția intereselor esențiale de securitate, pentru a proteja ordinea și siguranța publică și pentru a permite investigarea, depistarea și urmărirea penală a infracțiunilor*”, cu respectarea strictă a articolului 52 alin. (1) din Carta Drepturilor Fundamentale, care consacră principiul proporționalității.

Considerentul (6) acționează, așadar, ca o „poartă juridică”. El nu oferă un temei juridic pozitiv pentru instituirea unei măsuri de înregistrare, ci recunoaște competența preexistentă a statului în domeniul securității și confirmă că reglementarea pieței telecomunicațiilor, astfel cum este stabilită de Codul european al comunicațiilor electronice, se subordonează imperativelor legitime de securitate publică ale statelor membre.

Pentru un stat membru, implicația practică este clară: autoritatea națională de reglementare în comunicații va fi responsabilă de implementarea tehnică a măsurii față de operatori. Totuși, justificarea juridică fundamentală a măsurii nu derivă din legislația comunicațiilor electronice, ci din legislația în domeniul securității naționale și afacerilor

interne, care, la rândul ei, trebuie să fie riguros conformă cu RGPD și cu Carta Drepturilor Fundamentale.

În acest context, după stabilirea faptului că justificarea măsurii de înregistrare nu derivă din legislația sectorială a comunicațiilor electronice, ci din cadrul general privind protecția datelor și securitatea publică, devine necesară o analiză detaliată a cerințelor impuse de acquis-ul UE în materia protecției datelor.

Astfel, regimul juridic aplicabil al RGPD și Directiva ePrivacy, stabilește că orice măsură de înregistrare a cartelelor SIM implică în mod inevitabil prelucrarea datelor cu caracter personal și prin urmare, intră simultan sub incidența RGPD (ca normă generală) și Directivei ePrivacy (ca normă specială pentru comunicațiile electronice). Pornind de la această premisă, cadrul european impune o arhitectură juridică în trei pași, care urmează să fie respectată în mod cumulativ la elaborarea prezentului proiect.

Primul pas a constat în identificarea temeiului juridic adecvat în conformitate cu articolul 6 din RGPD. S-a stabilit că, în lipsa unui temei juridic clar, măsura ar fi fost incompatibilă cu legislația europeană încă din faza inițială. În cazul de față, temeiul a fost reprezentat de obligația legală instituită operatorilor de telecomunicații prin actul legislativ național, evitând orice prelucrare lipsită de fundament juridic și garantând conformitatea formală încă din etapa adoptării legii.

Totuși, stabilirea temeiului juridic nu a fost suficientă, întrucât măsura implica o interferență cu drepturile fundamentale garantate de Carta Drepturilor Fundamentale (articolele 7 și 8), legislația europeană impune un al doilea pas: justificarea restricționării acestor drepturi în temeiul în baza RGPD. Obiectivele relevante pentru măsura propusă sunt enumerate la articolul 23 (1): „(a) securitatea națională;... (c) securitatea publică; (d) prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor penale... inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora”. Această etapă a fost esențială pentru a demonstra că ingerința urmărea un obiectiv legitim, securitatea națională, securitatea publică și prevenirea infracțiunilor și că restricția era necesară și proporțională.

În final, chiar dacă s-a demonstrat atât temeiul juridic, cât și obiectivul legitim al măsurii, acquis-ul european nu permite aplicarea nelimitată a derogărilor. Pentru a preveni abuzurile și pentru a asigura compatibilitatea cu drepturile fundamentale, a intervenit al treilea pas: respectarea cerințelor detaliate impuse de Orientările 10/2020 ale EDPB privind aplicarea articolului 23². Aceste orientări au impus standarde stricte de calitate legislativă, precum precizia definițiilor, limitarea clară a scopului, duratei și accesului la date, garanțiile procedurale și mecanismele de control, astfel încât măsura să fie nu doar justificată, ci și implementată într-un mod responsabil și previzibil.

În ansamblu, cele trei etape au constituit lanțul logic și juridic necesar pentru a demonstra compatibilitatea măsurii de înregistrare a cartelelor SIM cu dreptul UE. Prin asumarea și respectarea strictă a acestor principii, statul a urmărit și urmează în continuare să asigure o implementare care să fie legală, necesară și proporțională, în acord cu scopul general: garantarea securității publice fără a compromite protecția drepturilor fundamentale.

2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative

Anonimatul cartelelor SIM preplătite este exploatat pe scară largă în comiterea infracțiunilor de fraudă telefonică și informatică, escrocherii, trafic de droguri, activități ale grupărilor criminale organizate, apeluri false la serviciile de urgență, precum și în

² https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-102020-restrictions-under-article-23-gdpr_en

operarea dispozitivelor conectate, inclusiv drone și alte sisteme controlate prin rețele mobile. Evoluția tehnologiilor digitale și a metodelor de comunicare criptată amplifică aceste riscuri și facilitează utilizarea abuzivă a serviciilor de comunicații electronice.

Din perspectiva fenomenului infracțional, cartelele preplătite anonime sunt utilizate masiv în:

- escrocherii telefonice și bancare, bazate pe manipulare psihologică și platforme criptate, săvârșite prin apeluri sau mesaje transmise prin aplicații de comunicare (Viber, Telegram, WhatsApp), în cadrul cărora infractorii se prezintă drept angajați ai instituțiilor bancare și solicită date confidențiale;

- trafic de droguri, inclusiv gestionarea „magazinelor online” de distribuție a drogurilor sintetice (PVP), comunicarea cu clienții și localizarea „ascunzișurilor”. Aceste cartele sunt folosite pentru crearea de canale Telegram și pentru comunicări securizate între membrii rețelei;

- scheme de înșelăciune pe platforme de anunțuri comerciale (999.md, makler.md), unde infractorii creează conturi și poartă negocieri exclusiv prin cartele preplătite, oferind bunuri sau servicii inexistente și inducând în eroare cetățenii în scopul obținerii mijloacelor bănești;

- apeluri false și abuzive la Serviciul Național Unic pentru Apeluri de Urgență 112, efectuate de la numere de cartele preplătite, o mare parte din acestea purtând un caracter abuziv, non-urgente sau chiar false, care generează costuri bugetare considerabile;

- activități ale grupărilor criminale organizate, care utilizează anonimatul pentru a evita identificarea și interceptarea legală;

- operarea dronelor utilizate pentru contrabandă sau transport ilicit de bunuri. În acest context, cartelele SIM preplătite sunt folosite pentru controlarea la distanță a dronelor prin rețele mobile sau pentru comunicarea criptată între membrii grupurilor criminale implicați în aceste operațiuni, asigurând anonimitatea și îngreunând identificarea autorilor.

Operațiunile recente ale instituțiilor de aplicare a legii din Europa, Statele Unite ale Americii și regiunile învecinate au evidențiat rolul critic pe care îl joacă cartelele SIM preplătite anonime sau neînregistrate în facilitarea criminalității organizate, a fraudei la scară largă și a rețelilor de infractori cibernetici.

La 10 octombrie 2025, o acțiune majoră creată din echipa comună de investigații din Austria, Estonia, Letonia și Finlanda coordonată de Europol și Eurojust, denumită Operațiunea „Simcartel”, a destructurat o rețea sofisticată de tip SIM-box care oferea infrastructură de tip cybercrime-as-a-service pentru infractori din întreaga Europa. Autoritățile au confiscat aproximativ 1.200 de dispozitive SIM-box și 40.000 de cartele SIM active și au arestat șapte suspecți implicați în mii de cazuri de fraudă, cu pierderi cumulate de aprox. 5 mln. euro pentru victime din Austria și Letonia. Această rețea a facilitat crearea a milioane de conturi false online și a fost utilizată pentru phishing, smishing, preluare de identitate și alte infracțiuni.³

În Lituania, în anul 2025, Poliția Criminală din Vilnius a descoperit trei locații ale unei rețele SIM-box care operau în oraș, legate de fraude telecom și abuzuri în crearea conturilor. Ancheta a identificat aproape 200 de SIM-boxuri și aproximativ 75.000 de cartele SIM de la operatori internaționali.⁴ În mod similar, Guardia Civil din Spania a destructurat o infrastructură extinsă de tip SIM-farm care trimitea milioane de SMS-uri frauduloase și apeluri scam. Sistemul capabil să trimită până la 2,5 milioane de SMS-uri zilnic folosea mii de cartele SIM activate cu identități false pentru a viza victimele. Astfel, s-au descoperit 35 de SIM-box-uri echipate cu 865 de modemuri, 852 de cartele SIM

³ <https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested>

⁴ <https://vilnius.policija.lrv.lt/en/news/vilnius-criminal-police-operation-strikes-sim-box-network-VB9/>

active, peste 60.000 de cartele SIM naționale pentru utilizare imediată, 10.000 de cartele SIM noi, un număr mare de dispozitive informatice, numerar și criptomonede⁵.

În septembrie 2025, Serviciul Secret al SUA a destructurat o rețea de dispozitive electronice amplasate la o distanță de 56 de kilometri de reuniunea globală a Adunării Generale a Națiunilor Unite, care a avut loc la New York, unde au fost descoperite peste 300 de servere SIM colocate și 100.000 de cartele SIM în mai multe locații⁶.

Autoritățile naționale din afara UE au raportat modele similare. Poliția Cibernetică din Ucraina a închis ferme de roboți unde erau folosite peste 250 de dispozitive care fac legătura între rețelele de telefonie mobilă (GSM) și rețelele de telefonie pe internet și aproximativ 150.000 de cartele SIM ale diverșilor operatori de telefonie mobilă, pentru a înregistra conturi false pe rețelele sociale și a desfășura fraude și activități ilegale online.⁷ În Kazahstan, poliția a destructurat 57 de dispozitive frauduloase SIM-box și peste 38.000 de cartele SIM neînregistrate utilizate în scheme de phishing și apeluri frauduloase pentru colectarea de date personale și financiare.⁸

Aceste cazuri demonstrează un model consistent că rețelele infracționale exploatează cartelele SIM preplătite neînregistrate sau anonime pentru a-și ascunde identitatea, a trimite mesaje și apeluri frauduloase în masă și a extinde operațiunile ilegale transfrontaliere. În acest context, implementarea unei obligații de înregistrare a cartelelor SIM preplătite pe identități verificabile devine esențială. Aceasta facilitează identificarea rapidă a infractorilor, reduce posibilitatea ca SIM-urile să fie utilizate pentru fraude și crește costul și riscul operațional pentru rețelele organizate care caută anonim.

În Europa, peisajul normativ privind înregistrarea SIM-urilor preplătite este variat, iar țări precum Austria, Belgia, Bulgaria, Cipru (începând cu 2025), Franța, Germania, Grecia, Ungaria, Italia, Lituania (începând cu 2025), Luxemburg, Polonia, Slovacia, Spania, Suedia, Elveția, Macedonia de Nord, Muntenegru, Serbia, Belarus, Rusia și Norvegia impun obligația de înregistrare a SIM-urilor preplătite. Alte state, inclusiv Cehia, Danemarca, Estonia, Finlanda, Irlanda, Letonia (propunere în curs), Malta, Țările de Jos, Portugalia, România, Slovenia, Ucraina și Regatul Unit, nu au astfel de reglementări⁹.

Această practică este susținută de precedentul CEDO în cauza *Breyer v. Germany* (Aplicația nr. 50001/12, 30 ianuarie 2020), în care Curtea a confirmat că legea germană care impunea colectarea și stocarea datelor de identitate de bază ale utilizatorilor de SIM preplătite nu a încălcat Articolul 8 CEDO (dreptul la respectarea vieții private). *Curtea a constatat că interferența cu viața privată a fost limitată și proporțională, măsura a urmărit scopuri legitime de prevenire a criminalității și siguranță publică și au existat garanții adecvate pentru utilizarea corectă a datelor.*¹⁰

Astfel, combinația dintre experiența instituțiilor de aplicare a legii, bunele practici de reglementare și precedentul CEDO confirmă că înregistrarea obligatorie a SIM-urilor preplătite este un instrument eficient și compatibil cu drepturile fundamentale, permițând autorităților să reducă anonimatul, să sporească trasabilitatea și să protejeze cetățenii și afacerile împotriva fraudei și a criminalității organizate.

⁵ <https://web.guardiacivil.es/en/destacados/noticias/Desmantelada-una-red-de-infraestructura-tecnologica-que-recopilaban-datos-para-ponerlos-a-disposicion-de-ciberdelincuentes/>

⁶ <https://www.secretservice.gov/newsroom/releases/2025/09/us-secret-service-dismantles-imminent-telecommunications-threat-new-york>

⁷ <https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-organizatoriv-botoferm-yaki-poshyryuvaly-vorozhu-propagandu-ta-zajmalysya-internet-shaxrajstvamy-7156/>

⁸ <https://polisia.kz/ru/57-moshennicheskikh-sim-box-ustrojstv-vyyavila-politsiya/>

⁹ https://prepaid-data-sim-card.fandom.com/wiki/Registration_Policies_Per_Country?utm_source=

¹⁰ https://hudoc.echr.coe.int/app/conversion/pdf/?filename=Judgment+Breyer+v.+Germany+-+registration+and+storage+of+pre-paid+SIM+card+users&id=003-6624862-8792771&library=ECHR&utm_source=

În prezent, Republica Moldova este una dintre puținele jurisdicții europene în care cartelele preplătite pot fi folosite fără niciun mecanism de identificare. Această situație creează un risc semnificativ ca teritoriul național să fie utilizat ca sursă de cartele anonime pentru rețele criminale transfrontaliere, în special în condițiile în care în multiple state din UE s-a introdus deja cerințe obligatorii de înregistrare pe baza unui act de identitate.

Astfel, lacunele existente în legislația comunicațiilor electronice, combinate cu evoluția fenomenelor infracționale și cu obligațiile asumate la nivel național și internațional, fac necesară adoptarea unei reglementări clare, proporționale și aliniate la standardele europene privind identificarea utilizatorilor de cartele SIM preplătite și conexiuni M2M (*Machine-to-Machine*) sau IoT (*Internet of Things*) la momentul achiziției sau activării.

Pentru limitarea impactului asupra utilizatorilor și operatorilor, se propune adoptarea unui model echilibrat, structurat pe trei principii:

1. Aplicare exclusiv pentru viitor (non-retroactivitate). Obligația de identificare va viza doar cartelele SIM și conexiunile noi, activate după intrarea în vigoare a modificărilor normative. Baza actuală de utilizatori preplătiți nu va fi supusă unei campanii de re-înregistrare, ceea ce evită costuri logistice ridicate și riscul de întrerupere a serviciilor.

2. Colectarea unui set minim de date. Vor fi solicitate doar datele strict necesare pentru identificarea titularului și atribuirea numărului (persoană fizică sau juridică), cu respectarea principiilor legalității, proporționalității și minimizării datelor prevăzute de legislația în domeniul protecției datelor.

3. Neutralitate tehnologică. Operatorii vor avea libertatea de a stabili modalitatea de identificare: fizică, digitală sau la distanță, în funcție de propriile modele de business și infrastructură tehnică, asigurând flexibilitate și eficiență.

Modelul propus este proporțional, modern, orientat spre viitor, nu afectează utilizatorii existenți și nu creează poveri excesive pentru operatori. Adoptarea sa va reduce semnificativ anonimatul infracțional și va contribui la creșterea nivelului de securitate publică.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul de act normativ propune completarea Legii nr. 72/2025 comunicațiilor electronice pentru a reglementarea procedura prin care furnizorii de rețele publice de comunicații electronice să solicite datele de identitate al utilizatorului la achiziționarea serviciilor preplătite noi activate, cu următorul conținut:

- Completarea legii vizate cu un nou **articol 125¹**, care instituie un cadru juridic uniform și preventiv pentru identificarea utilizatorilor serviciilor de comunicații electronice mobile, indiferent de tipul ofertei (abonament sau cartelă preplătită), vizând direct cauzele identificate ale problemei și urmăresc eliminarea vulnerabilităților generate de utilizarea anonimă a cartelelor SIM.

- Prin **alineatul (1)** se introduce, obligația furnizorilor de a identifica toți abonații serviciilor de comunicații electronice mobile accesibile publicului, inclusiv utilizatorii cartelelor SIM preplătite, cel târziu la momentul activării acestora, care înlătură principala cauză a problemei identificate și anume lipsa unei obligații legale exprese de identificare, care a permis utilizarea anonimă a serviciilor în scopuri ilicite. *Aceasta va spori trasabilitatea utilizatorilor, va consolida capacitatea de prevenire și investigare a infracțiunilor și va reduce utilizarea serviciilor de comunicații electronice ca instrument de anonimizare.*

- **Alineatul (2)** definește exhaustiv datele minime de identificare care urmează a fi colectate, diferențiat în funcție de categoria abonatului (persoane fizice din Republica Moldova, persoane fizice din alte state, persoane juridice naționale și străine). Este

introdusă obligația verificării gratuite a datelor prin registrele de stat relevante, menită să asigure exactitatea și fiabilitatea datelor. *Aceasta va asigura un echilibru între necesitatea identificării și respectarea principiilor de legalitate, proporționalitate și minimizare a datelor, prevăzute de legislația privind protecția datelor cu caracter personal.*

▪ **Alineatul (3)** introduce un spectru larg de metode de identificare, inclusiv identificarea la distanță prin mijloace de identificare electronică, soluții digitale și reutilizarea datelor deja verificate, care reprezintă o inovație tehnologică importantă, adaptată evoluției digitale și cerințelor de accesibilitate. *Aceasta va reduce povara administrativă pentru furnizori și utilizatori, facilitarea accesului legal la servicii și asigurarea unei implementări eficiente, fără a afecta concurența pe piața comunicațiilor electronice.*

▪ Prin **alineatul (4)** se instituie o soluție tranzitorie, permițând utilizarea cartelelor SIM/eSIM doar pentru servicii tehnice minime până la finalizarea identificării, având un caracter preventiv și eliminând riscul utilizării anonime nelimitate imediat după achiziție. *Aceasta va preveni utilizarea abuzivă a cartelelor neidentificate și reducerea riscurilor imediate pentru securitatea publică.*

▪ **Alineatul (5)** prevede obligația furnizorilor de a păstra datele de identificare pe durata utilizării serviciului și pentru o perioadă limitată de 12 luni după încetarea acestuia, în conformitate cu legislația privind protecția datelor, constituind o inovație de claritate și predictibilitate juridică, în absența unor reglementări explicite anterioare. *Aceasta va asigura un cadru clar pentru accesul legal al autorităților competente la datele de identificare, fără a institui un regim general de retenție excesivă.*

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

În procesul de elaborare a proiectului de lege, au fost analizate mai multe opțiuni alternative, însă acestea nu au fost considerate eficiente sau adecvate, din următoarele motive:

▪ Menținerea regimului actual al cartelelor preplătite anonime: anonimatul utilizatorilor preplătiți continuă să reprezinte una dintre principalele vulnerabilități ale securității publice, fiind exploatat în activități infracționale și acte de fraudă. Menținerea status quo-ului nu ar fi permis îmbunătățirea capacității operative a autorităților de aplicare a legii.

▪ Introducerea identificării voluntare a utilizatorilor cartelelor SIM preplătite. Această opțiune a fost exclusă, întrucât nu asigură un nivel adecvat de acoperire și nu elimină posibilitatea utilizării anonime a serviciilor de comunicații electronice în scopuri ilicite, limitând semnificativ efectul preventiv al măsurii.

▪ Limitarea cantitativă a cartelelor SIM preplătite neidentificate. Această soluție nu a fost considerată adecvată, deoarece nu asigură identificarea efectivă a utilizatorilor finali și poate fi ușor eludată prin achiziții repetate, utilizarea unor intermediari sau distribuirea cartelelor între mai multe persoane.

Opțiunea selectată a fost eliminarea anonimatului și instituirea obligativității colectării și păstrării datelor de identificare, deoarece:

1. este singura soluție care reduce substanțial vulnerabilitățile de securitate asociate serviciilor preplătite;
2. permite identificarea rapidă și eficientă a utilizatorilor în cazuri operative și de urgență;
3. este conformă cu practicile standard din majoritatea statelor europene;
4. oferă un cadru normativ coerent și maximizează beneficiile pentru securitatea publică cu un cost administrativ rezonabil.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Prezentul proiect va produce efecte semnificative, contribuind la consolidarea securității și la eficientizarea activității autorităților competente. Pentru sectorul public, introducerea obligativității de identificare a utilizatorilor serviciilor preplătite și clarificarea procedurilor interne ale furnizorilor determină o creștere substanțială a capacității operative. Autoritățile vor avea acces mai rapid și mai precis la datele necesare pentru investigarea infracțiunilor, ceea ce reduce timpul de reacție și optimizează resursele implicate. De asemenea, obligarea furnizorilor să colecteze, să păstreze și să ofere date structurate contribuie la diminuarea solicitărilor repetate din partea organelor de drept și la îmbunătățirea calității cooperării instituționale. În același timp, noile prevederi întăresc mecanismele de răspuns în situații de urgență și incidente critice, prin facilitarea corelării între datele tehnice și identitatea reală a utilizatorilor.

4.2 Impactul financiar și argumentarea costurilor estimative

Implementarea opțiunii recomandate implică costuri de conformare pentru furnizorii de servicii de comunicații electronice mobile, determinate de necesitatea adaptării sistemelor informatice existente, dezvoltării și integrării soluțiilor de identificare electronică a utilizatorilor, ajustării fluxurilor operaționale și comerciale (inclusiv în punctele de vânzare), precum și instruirii personalului propriu și a partenerilor de distribuție.

În funcție de arhitectura tehnică, gradul de digitalizare și complexitatea sistemelor fiecărui operator, investițiile inițiale necesare pentru integrarea mecanismelor de identificare în platformele Billing/CRM, dezvoltarea interfețelor securizate și a procedurilor standardizate de validare a identității, precum și implementarea soluțiilor digitale de identificare (inclusiv la distanță, după caz), sunt estimate, la nivel agregat, între 3,0 mln. și 6,8 mln. MDL. Diferențele între operatori sunt determinate, în principal, de dimensiunea bazei de clienți, numărul și distribuția punctelor de vânzare, nivelul cerut de securitate (autentificare, jurnalizare, trasabilitate), precum și de necesitatea interoperabilității cu sisteme interne și, eventual, cu infrastructuri externe de identificare electronică.

Aceste costuri reflectă atât cheltuieli de capital (dezvoltare/achiziție de module software, integrare, testare, securizare, audit tehnic), cât și cheltuieli asociate conformării proceselor (revizuirea procedurilor, actualizarea contractelor și a condițiilor comerciale, elaborarea instrucțiunilor interne, formarea personalului). În mod specific, implementarea presupune setarea unor mecanisme de control pentru prevenirea utilizării neautorizate, consolidarea măsurilor de protecție a datelor cu caracter personal (limitarea accesului, minimizarea datelor, păstrarea evidențelor și trasabilitatea operațiunilor), precum și asigurarea continuității operaționale în perioadele de tranziție (migrare, paralelizarea fluxurilor, suport pentru clienți).

Totodată, pe lângă investițiile inițiale, se anticipează apariția unor costuri operaționale recurente aferente mentenanței și licențelor, administrării și actualizării sistemelor, suportului tehnic, precum și măsurilor de securitate cibernetică și conformitate (monitorizare, audit periodic, gestionarea incidentelor). În aceste condiții, se justifică instituirea unei perioade de tranziție adecvate și a unui mecanism de monitorizare a implementării, inclusiv pentru ajustarea etapizării și a cerințelor tehnice, astfel încât obligațiile să fie aplicabile efectiv și sustenabile din punct de vedere economic, fără a compromite obiectivele de securitate și protecție a datelor.

4.3 Impactul asupra sectorului privat

Implementarea obligativității identificării utilizatorilor de cartele SIM preplătite va genera un impact considerabil asupra sectorului privat, întrucât modelul actual de distribuție al serviciilor preplătite se bazează aproape integral pe canale nespecializate.

Potrivit datelor comunicate de furnizori, cea mai mare parte a cartelelor SIM preplătite sunt comercializate prin rețele de distribuție gestionate de terțe persoane, inclusiv în magazine gestionate de parteneri și în puncte de vânzare aparținând partenerilor (chioscuri, oficii poștale, stații PECO, supermarketuri), precum și prin alți comercianți cărora partenerii le livrează cartelele preplătite pe întreg teritoriul țării. Aceste puncte nu dispun, de regulă, de infrastructura și competențele necesare pentru validarea actelor de identitate și pentru respectarea cerințelor aferente prelucrării datelor cu caracter personal, iar furnizorii avertizează că o parte semnificativă dintre ele ar putea renunța la comercializarea cartelelor SIM, ceea ce ar reduce accesul la servicii, în special în zonele rurale și în localitățile cu ofertă limitată.

De asemenea, produsele digitale precum eSIM, concepute pentru activare complet online, pot deveni dificil sau imposibil de comercializat în lipsa unor proceduri funcționale și proporționale de identificare la distanță, întrucât verificarea identității ar necesita fie proceduri video complexe, fie prezență fizică, diminuând beneficiile modelului digital și crescând fricțiunea pentru consumator.

Nu în ultimul rând, furnizorii menționează că sistemele de facturare și gestiune a relației cu clientul nu sunt proiectate, în mod curent, pentru asocierea și administrarea datelor personale ale utilizatorilor preplătiți, iar modificările arhitecturale necesare implică riscuri operaționale semnificative, termene extinse de dezvoltare și cicluri lungi de testare.

4.4 Impactul social

Impactul este pozitiv, datorită reducerii vulnerabilităților exploatate frecvent în activități infracționale precum fraudele telefonice, amenințările sau utilizarea cartelelor preplătite în scopuri ilegale. Eliminarea anonimatului contribuie la crearea unui mediu comunicațional mai sigur și la diminuarea riscurilor pentru cetățeni. Crește astfel nivelul general de securitate publică și încrederea populației în capacitatea instituțiilor statului de a acționa eficient. Deși pot exista anumite preocupări privind protecția datelor cu caracter personal, acestea sunt temperate de caracterul proporțional al măsurii, de limitarea temporală strictă a păstrării datelor și de cadrul legal clar care reglementează accesul autorităților. Procedura simplă de identificare, realizată o singură dată la activarea serviciului, nu generează sarcini considerabile pentru utilizatori și nu afectează accesul la servicii. În ansamblu, modificările promovează un echilibru adecvat între necesitatea de asigurare a securității publice și respectarea dreptului la viață privată.

4.4.1 Impactul asupra datelor cu caracter personal

Modificările propuse au un impact direct asupra datelor cu caracter personal, însă acest impact este proiectat într-un cadru legal echilibrat, necesar și proporțional, orientat spre consolidarea securității publice și prevenirea abuzurilor în utilizarea serviciilor de comunicații electronice. Introducerea obligativității de identificare a utilizatorilor serviciilor preplătite și extinderea responsabilităților furnizorilor în ceea ce privește colectarea și păstrarea acestor date determină o prelucrare suplimentară a datelor cu caracter personal, însă această prelucrare este limitată strict la ceea ce este necesar pentru atingerea obiectivelor de interes public major.

În primul rând, măsura elimină anonimatul utilizatorilor de cartele preplătite, o practică care, deși comodă, a generat în mod repetat vulnerabilități grave utilizate în fraude, șantaj, amenințări, precum și în activități organizate ce împiedică identificarea rapidă a persoanelor implicate. Prelucrarea datelor suplimentare devine astfel o intervenție justificată, întrucât permite corelarea elementelor tehnice (IMEI, Cell ID, număr apelant) cu identitatea persoanei, prevenind folosirea rețelelor de comunicații în scopuri ilegale fără posibilitatea de a atribui responsabilitatea.

În al doilea rând, regimul juridic de prelucrare a datelor rămâne unul riguros, limitat în timp și însoțit de garanții clare. Datele de identificare se păstrează pentru o perioadă

determinată de 12 luni, după care sunt distruse în mod ireversibil prin proceduri automatizate. Accesul autorităților este reglementat strict de lege, fiind permis doar în condițiile prevăzute de cadrul procedural existent și doar pentru prevenirea, investigarea și combaterea infracțiunilor. Astfel, nu există riscul utilizării arbitrare a datelor, iar proporționalitatea măsurii este menținută prin limitarea accesului exclusiv la situațiile justificate din punct de vedere legal.

Totodată, furnizorii vor institui proceduri interne detaliate privind colectarea, păstrarea și furnizarea datelor, ceea ce contribuie la respectarea principiilor-cheie de protecție a datelor: legalitate, transparență, integritate, securitate și minimizare. Procedurile interne vor fi conforme cu legislația privind protecția datelor cu caracter personal, inclusiv în ceea ce privește măsurile tehnice și organizatorice pentru prevenirea accesului neautorizat.

În ansamblu, impactul asupra protecției datelor cu caracter personal este gestionat printr-o arhitectură normativă robustă, care previne abuzurile, limitează prelucrarea la ceea ce este necesar și introduce garanții clare împotriva riscurilor. Măsurile propuse nu urmăresc extinderea supravegherii, ci eliminarea unei lacune majore în securitatea comunicațiilor, oferind un echilibru legitim și proporțional între interesul public de securitate și dreptul fundamental la protecția datelor cu caracter personal.

4.4.2 Impactul asupra echității și egalității de gen

Nu se aplică.

4.5 Impactul asupra mediului

Nu se aplică

4.6 Alte impacturi și informații relevante

Practica comparată oferă repere utile privind contextul și condițiile de implementare a obligației de înregistrare a cartelelor SIM preplătite. În acest sens, înainte de intrarea în vigoare a cadrului anti-terorism adoptat în anul 2016, în Polonia a fost raportat un volum ridicat de alerte false privind amplasarea unor dispozitive explozive, care a generat întreruperi semnificative ale activității unor obiective publice și private și a determinat mobilizarea repetată a resurselor de intervenție (poliție, echipe specializate, servicii de urgență), cu efecte operaționale și economice aferente. Autoritățile au indicat că reducerea anonimatului în utilizarea serviciilor preplătite, prin introducerea obligativității înregistrării cartelelor SIM preplătite (cu o perioadă de tranziție până în februarie 2017), a facilitat identificarea mai rapidă a utilizatorilor/terminalelor și a contribuit la creșterea eficienței investigațiilor.

În comunicările oficiale și materialele de analiză ale autorităților poloneze se menționează o scădere a numărului de alerte false după introducerea obligației de înregistrare a cartelelor preplătite, concomitent cu îmbunătățirea ratei de depistare a făptuitorilor, inclusiv prin posibilitatea de a corela mai rapid numărul/serviciul utilizat cu o identitate declarată. Totodată, este relevant că intervenția legislativă a constituit un pachet mai amplu (inclusiv înăsprirea sancțiunilor pentru astfel de fapte), ceea ce impune o interpretare prudentă a relației cauzale exclusive, însă susține concluzia că reducerea anonimatului operațional reprezintă un instrument utilizat în practică pentru descurajare și pentru creșterea trasabilității.

Datele comparative și indicatorii menționați de autoritățile poloneze sunt sintetizați în tabelul¹¹ de mai jos, care reflectă evoluțiile raportate înainte și după introducerea obligativității de înregistrare a cartelelor SIM preplătite. Lecțiile de implementare care rezultă din practica comparată subliniază importanța unei perioade de tranziție, a unor mecanisme funcționale de identificare (inclusiv opțiuni la distanță, după caz), a soluțiilor

¹¹ https://cdn.netzpolitik.org/wp-upload/2025/10/2025-02-05_Poland_Police_Prepaid-SIM-cards.pdf

aplicabile pentru nerezidenți/vizitatori, precum și a stabilirii garanțiilor de conformitate în materia protecției datelor (minimizare, securitate, evidență și trasabilitate), inclusiv prin mecanisme de monitorizare și ajustare a aplicării.

Indicator statistic de referință	Perioada pre-reglementare (2010 - 2015)	Perioada post-reglementare (2016 - prezent)	Dinamica evolutivă și impactul operațional
Volumul alertelor false cu bombă	3.000 - 4.000 rapoarte false / anual	aprox. 200 rapoarte false / anual	Scădere drastică de aproximativ 93% - 95%. Fenomenul a fost redus de la o criză sistemică la incidente izolate.
Rata de detecție (identificarea și reținerea făptuitorilor)	30% - 40% (rată scăzută din cauza imposibilității de atribuire tehnică a identității).	60% - 70% (creștere majoră a succesului investigativ).	Creșterea ratei de detecție cu până la 100% (de la 35% medie la 65% medie). Efect de descurajare masiv.
Timpul mediu de alocat investigației	Extrem de ridicat (necesita monitorizare îndelungată, analize de tipar, supraveghere fizică, resurse analitice).	Redus semnificativ.	Permite identificarea imediată a locației conexiunii și a proprietarului de drept al dispozitivului.
Alocarea resurselor de intervenție	Resurse critice deviate zilnic către alarme false, generând costuri uriașe la bugetul de stat.	Resurse alocate eficient către urgențe reale.	Salvarea bugetelor structurilor de intervenție rapidă (Pompieri, Poliție, Ambulanță).

Aceste date indică o schimbare operațională majoră, volumul alertelor false scade de la un nivel „sistemic” (3.000-4.000/an) la un nivel relativ izolat (~200/an), iar capacitatea de identificare a făptuitorilor aproape se dublează (de la 30%-40% la 60%-70%). Concomitent, durata investigațiilor se reduc semnificativ (prin atribuirea mai rapidă a numărului unei identități), iar resursele de intervenție nu mai sunt consumate masiv de alarme false, putând fi orientate către urgențe reale.

În aceeași logică, Europol arată, în *Position Paper on Caller-ID Spoofing*¹², că abilitatea infractorilor de a-și ascunde identitatea și originea împiedică sever capacitatea autorităților de aplicare a legii de a trasa și urmări penal autorii. Tot acolo, Europol menționează explicit că „serviciile preplătite anonime” reprezintă o provocare persistentă pentru trasarea activităților ilicite și semnalează necesitatea consolidării verificării identității (KYC) în telecom.

5. Compatibilitatea proiectului actului normativ cu legislația UE

5.1. Măsurile normative necesare pentru transpunerea actelor juridice ale UE în legislația națională

Nu se aplică

5.2. Măsurile normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

¹² <https://www.europol.europa.eu/cms/sites/default/files/documents/Position-Paper-Caller-ID-Spoofing.pdf>

Nu se aplică
6. Avizarea și consultarea publică a proiectului actului normativ
În vederea respectării prevederilor Legii nr. 100/2017 cu privire la actele normative și Legii nr. 239/2008 privind transparența în procesul decizional, a fost plasat anunțul privind inițierea elaborării proiectului de lege: https://particip.gov.md/ro/document/stages/anunt-privind-initierea-procesului-de-elaborare-a-proiectului-de-lege-pentru-modificarea-cadrului-no/16061. De asemenea, urmare a plasării anunțului privind inițierea elaborării proiectului de lege pe platforma www.particip.gov.md, în perioada 03.02.2026-16.02.2026 au fost recepționate comentarii și observații din partea unui utilizator al platformei, precum și poziția oficială a Asociației Naționale a Companiilor din Domeniul TIC (ATIC). În procesul de analiză, s-a constatat că o parte semnificativă a acestor obiecții au un caracter preponderent evaluativ sau speculativ, fără prezentarea unor date argumentate, indicatori comparabili ori argumente care să demonstreze în mod convingător lipsa necesității măsurii sau disproporționalitatea acesteia în raport cu scopul urmărit. Totodată, unele afirmații vizează ipoteze generale (posibilitatea eludării prin roaming, utilizarea aplicațiilor OTT, riscuri de incluziune), care au fost deja avute în vedere la elaborarea proiectului și au fost tratate prin soluții de reducere a impactului (inclusiv opțiuni de identificare la distanță, aplicarea măsurii doar pentru numerele activate după intrarea în vigoare a legii și termen de tranziție de 24 luni). Prin urmare, deși observațiile recepționate au fost consemnate și examinate, acestea nu oferă un temei suficient pentru a justifica renunțarea la inițiativă sau modificarea obiectivelor de reglementare stabilite, urmând a fi analizate în continuare în cadrul procesului de consultare publică a proiectului de lege. Totodată, în cadrul ședinței din 08.12.2025 cu instituțiile naționale interesate (CNPDCP, ANRCETI și MDED), participanții au convenit asupra Opțiunii D – „Digital First”, iar MDED, în urma examinării propunerilor de modificare a Legii comunicațiilor electronice și a coordonării cu conducerea ministerului, a confirmat că aceasta reprezintă cea mai optimă soluție din perspectiva implementării, fiind reflectată în redacția actuală a proiectului de lege.
7. Concluziile expertizelor
Proiectul urmează a fi supus expertizelor anticorupție și expertizei juridice, conform art. 34 alin. (3) din Legea nr. 100/2017 cu privire la actele normative.
8. Modul de încorporare a actului în cadrul normativ existent
Proiectul se încorporează în cadrul normativ existent prin completarea Legii nr. 72/2025 privind comunicațiile electronice cu un nou articol (art. 125 ¹), care instituie obligația de identificare a utilizatorilor serviciilor de comunicații electronice mobile accesibile publicului, inclusiv pentru cartelele preplătite și eSIM. Aplicarea se realizează prin corelare cu cadrul național privind identificarea electronică și protecția datelor.
9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ
Pentru operatorii de comunicații electronice, stabilirea unui termen de implementare de 24 de luni este strict necesară pentru asigurarea unei aplicări sigure, funcționale și conforme cu cerințele de securitate și protecție a datelor ale modificărilor propuse. Această necesitate rezultă din analiza etapelor tehnice, operaționale și financiare aferente, precum și din contextul unui sector care implementează simultan mai multe reglementări majore. Unul din operatori indică faptul că implementarea soluției de identificare online presupune un proces complex de achiziție și evaluare a conformității tehnice, care include elaborarea caietului de sarcini, definirea cerințelor de arhitectură, planificarea bugetară, organizarea procedurilor de achiziție, evaluarea ofertelor și contractarea furnizorului, cu un termen estimat de 6-8 luni.

De asemenea, integrarea noii soluții cu sistemele interne (inclusiv cele de billing), precum și cu **sistemele informaționale ale statului** (registrele de stat și, eventual, platforma guvernamentală EVO), presupune eforturi tehnice semnificative, cu un termen estimat de **8-10 luni** pentru dezvoltare și integrare. Este de menționat că identificarea prin EVO poate reprezenta o opțiune solicitată de cetățeni, fiind necesară reflectarea acesteia în cadrul normativ.

Etapa de **testare și lansare în producție**, realizată în cooperare cu platformele de stat, este esențială pentru stabilitatea și securitatea sistemelor și necesită un termen suplimentar de **6-8 luni**.

Totodată, acesta implementează concomitent alte cerințe legale majore, precum noua Lege a comunicațiilor, cerințele privind serviciul 112 și e-Call și noile reglementări în domeniul securității cibernetice, toate având termene-limită până în **anul 2027** și utilizând aceleași resurse umane și financiare. Suprapunerea acestor proiecte impune perioade adecvate de testare și stabilizare, pentru a preveni disfuncționalități operaționale și riscuri de securitate.

Un alt operator menționează că implementarea noilor prevederi legale vor fi realizate atât prin resurse interne, cât și prin furnizori externi selectați în cadrul procedurilor de achiziție publică, care pot fi demarate doar după intrarea în vigoare a legii și pot dura **între 6 și 18 luni**. După semnarea contractelor, este necesară o perioadă suplimentară pentru prestarea serviciilor de dezvoltare, integrarea soluțiilor cu sistemele existente și testarea completă a acestora.

Al treilea operator menționează că, un factor determinant îl constituie **ajustarea proceselor interne și dezvoltarea/integrările IT** necesare atât în sistemele operatorului, cât și în cele ale partenerilor din distribuția cartelelor prepay. Această etapă, care presupune modificarea aplicațiilor de activare, facturare și gestiune a utilizatorilor pentru colectarea, stocarea și verificarea datelor de identificare, necesită un termen estimat de circa **18 luni**.

Integrarea cu bazele de date ale registrelor de stat pentru verificarea identității implică interconectări tehnice securizate, ajustări procedurale și de protecție a datelor, precum și modificări ale mecanismelor de validare, cu un termen estimat de aproximativ **8 luni**.

În paralel, este necesară selectarea unui furnizor pentru mecanismul de identificare la distanță (eKYC sau semnătură electronică), proces care include elaborarea cerințelor tehnice, organizarea procedurilor de achiziție, evaluarea ofertelor și integrarea soluției alese, cu un termen estimat de circa **8 luni**.

De asemenea, este necesară renegocierea contractelor de distribuție cu dealerii și sub-distribuitorii, pentru includerea noilor obligații legale, etapă estimată la **6 luni**, precum și instruirea personalului operatorului și al partenerilor de distribuție, estimată la **3 luni**. Informarea populației cu privire la noile obligații legale și modalitățile de înregistrare a cartelelor prepay necesită campanii de comunicare publică desfășurate pe o perioadă de minimum **3 luni**.

Drept urmare, se propune ca intrarea în vigoare să aibă loc în termen de 24 de luni de la data publicării proiectului în Monitorul Oficial al Republicii Moldova.

Tabelul comparativ

la proiectul de proiectul de lege pentru modificarea Legii nr. 72/2025 comunicațiilor electronice

Conținutul normei în vigoare	Modificarea propusă	Conținutul normei după modificare
	„Articolul 125¹ – Identificarea abonaților serviciilor de comunicații electronice mobile accesibile publicului (1) Furnizorii de servicii de comunicații electronice mobile accesibile publicului sunt obligați să identifice abonații serviciilor respective, indiferent de tipul ofertei (abonament sau cartelă preplătită), la momentul încheierii contractului de abonament sau, în cazul cartelelor preplătite, cel târziu la momentul activării acestora. (2) Identificarea abonaților se realizează în baza unui act de identitate valabil sau prin mijloace de identificare electronică, cu colectarea cel puțin a următoarelor date: 1) pentru persoanele fizice care se identifică cu acte de identitate emise de Republica Moldova – numele, prenumele, IDNP, datele actului de identitate (denumirea, seria, numărul), cu verificarea datelor și valabilității acestuia prin interogarea gratuită a Sistemului informațional automatizat „Registrul de stat al populației”, în condițiile legii; 2) pentru persoanele fizice care se identifică cu acte de identitate emise de alte state – numele, prenumele, datele actului de identitate (denumirea, seria, numărul și data expirării), furnizorul poate reține o copie a actului de identitate, în condițiile legislației privind protecția datelor cu caracter personal; 3) pentru persoanele juridice din Republica Moldova – denumirea, IDNO, precum și datele prevăzute la subpunctele 1) sau 2) referitoare la	Articolul 125. Regimul juridic al accesului autorităților competente la datele utilizatorilor de servicii de comunicații electronice și la comunicațiile acestora. [...] „Articolul 125¹ – Identificarea abonaților serviciilor de comunicații electronice mobile accesibile publicului (1) Furnizorii de servicii de comunicații electronice mobile accesibile publicului sunt obligați să identifice abonații serviciilor respective, indiferent de tipul ofertei (abonament sau cartelă preplătită), la momentul încheierii contractului de abonament sau, în cazul cartelelor preplătite, cel târziu la momentul activării acestora. (2) Identificarea abonaților se realizează în baza unui act de identitate valabil sau prin mijloace de identificare electronică, cu colectarea cel puțin a următoarelor date: 1) pentru persoanele fizice care se identifică cu acte de identitate emise de Republica Moldova – numele, prenumele, IDNP, datele actului de identitate (denumirea, seria, numărul), cu verificarea datelor și valabilității acestuia prin interogarea gratuită a Sistemului informațional automatizat „Registrul de stat al populației”, în condițiile legii; 2) pentru persoanele fizice care se identifică cu acte de identitate emise de alte state – numele,

	persoana împuternicită să reprezinte abonatul în legătură cu identificarea acestuia, cu verificarea datelor prin interogarea gratuită a Sistemului informațional „Registrul de stat al unităților de drept”, în condițiile legii; 4) pentru persoanele juridice din alte state – denumirea, țara de origine și numărul de înregistrare în registrul comercial al statului străin, precum și datele prevăzute la subpunctele 1) sau 2) referitoare la persoana împuternicită să reprezinte abonatul în legătură cu identificarea acestuia, furnizorul reține copia documentului care atestă înregistrarea, cu traducere legalizată în limba română, în condițiile legii. (3) La alegerea furnizorilor, identificarea abonaților serviciilor de comunicații electronice mobile accesibile publicului poate fi efectuată prin una sau mai multe dintre următoarele metode: 1) în punctele de vânzare proprii ale furnizorului; 2) în punctele de vânzare ale persoanelor împuternicite de furnizor, în baza unui contract sau a unui alt temei juridic corespunzător; 3) la distanță, prin: a) mijloace de identificare electronică (semnătură electronică calificată sau avansată), sau alte mijloace electronice oferite de către un prestator de servicii de încredere calificat, în condițiile Legii nr. 124/2022 privind identificarea electronică și serviciile de încredere și ale actelor normative subsecvente; b) mijloace digitale, constând într-un proces de identificare și de verificare a identității persoanei fizice în baza actelor de identitate prezentate, a măsurătorilor semnalmentelor biometrice faciale, a comparării de imagini și a informațiilor comunicate de persoana fizică și preluate gratuit din Sistemul informațional automatizat „Registrul de stat al populației”, utilizând mijloace digitale;	prenumele, datele actului de identitate (denumirea, seria, numărul și data expirării), furnizorul poate reține o copie a actului de identitate, în condițiile legislației privind protecția datelor cu caracter personal; 3) pentru persoanele juridice din Republica Moldova – denumirea, IDNO, precum și datele prevăzute la subpunctele 1) sau 2) referitoare la persoana împuternicită să reprezinte abonatul în legătură cu identificarea acestuia, cu verificarea datelor prin interogarea gratuită a Sistemului informațional „Registrul de stat al unităților de drept”, în condițiile legii; 4) pentru persoanele juridice din alte state – denumirea, țara de origine și numărul de înregistrare în registrul comercial al statului străin, precum și datele prevăzute la subpunctele 1) sau 2) referitoare la persoana împuternicită să reprezinte abonatul în legătură cu identificarea acestuia, furnizorul reține copia documentului care atestă înregistrarea, cu traducere legalizată în limba română, în condițiile legii. (3) La alegerea furnizorilor, identificarea abonaților serviciilor de comunicații electronice mobile accesibile publicului poate fi efectuată prin una sau mai multe dintre următoarele metode: 1) în punctele de vânzare proprii ale furnizorului; 2) în punctele de vânzare ale persoanelor împuternicite de furnizor, în baza unui contract sau a unui alt temei juridic corespunzător; 3) la distanță, prin: a) mijloace de identificare electronică (semnătură electronică calificată sau avansată), sau alte mijloace electronice oferite de către un prestator de servicii de încredere calificat, în condițiile Legii nr. 124/2022 privind identificarea
--	--	--

	c) alte mijloace electronice oferite de către furnizor, în cazul în care datele de identificare ale abonatului au fost anterior verificate în legătură cu un alt număr prin una dintre metodele prevăzute la subpunctele 1) - 3). (4) Până la finalizarea procesului de identificare, cartelele SIM/eSIM pot fi utilizate doar pentru serviciile tehnice minime necesare stabilite de autoritatea de reglementare, dacă este fezabil. (5) Furnizorii de servicii de comunicații electronice mobile accesibile publicului păstrează datele de identificare ale utilizatorilor ale căror cartele au fost activate pe întreaga durată de utilizare a serviciului și pentru o perioadă de 12 luni de la încetarea utilizării numărului, în conformitate cu art. 125 alin. (3) și legislației privind protecția datelor cu caracter personal.	electronică și serviciile de încredere și ale actelor normative subsecvente; b) mijloace digitale, constând într-un proces de identificare și de verificare a identității persoanei fizice în baza actelor de identitate prezentate, a măsurătorilor semnalmentelor biometrice faciale, a comparării de imagini și a informațiilor comunicate de persoana fizică și preluate gratuit din Sistemul informațional automatizat „Registrul de stat al populației”, utilizând mijloace digitale; c) alte mijloace electronice oferite de către furnizor, în cazul în care datele de identificare ale abonatului au fost anterior verificate în legătură cu un alt număr prin una dintre metodele prevăzute la subpunctele 1) - 3). (4) Până la finalizarea procesului de identificare, cartelele SIM/eSIM pot fi utilizate doar pentru serviciile tehnice minime necesare stabilite de autoritatea de reglementare, dacă este fezabil. (5) Furnizorii de servicii de comunicații electronice mobile accesibile publicului păstrează datele de identificare ale utilizatorilor ale căror cartele au fost activate pe întreaga durată de utilizare a serviciului și pentru o perioadă de 12 luni de la încetarea utilizării numărului, în conformitate cu art. 125 alin. (3) și legislației privind protecția datelor cu caracter personal. [...] Articolul 126. Aplicarea derogărilor temporare pentru furnizorii de servicii de comunicații interpersonale fără număr privind prelucrarea datelor personale în scopul combaterii abuzului sexual online asupra copiilor.
--	---	---



Nr. 38/ 695 din 23.02.2026

Cancelaria de Stat

**Cerere
privind înregistrarea de către Cancelaria de Stat a proiectul de lege pentru
modificarea Legii comunicațiilor electronice nr. 72/2025**

Nr. crt.	Criterii de înregistrare	Nota autorului
1.	Categoria și denumirea proiectului	Proiectul de lege pentru modificarea Legii comunicațiilor electronice nr. 72/2025
2.	Autoritatea care a elaborat proiectul	Ministerul Afacerilor Interne
3.	Justificarea depunerii cererii	Scopul proiectului proiectului este de a institui obligația de identificare și verificare a identității utilizatorilor de cartele SIM preplătite la activare, în vederea reducerii utilizării anonime a serviciilor preplătite în activități ilegale, consolidării securității publice și a încrederii în serviciile de comunicații electronice, cu aplicarea proporțională a măsurii și respectarea cerințelor de protecție a datelor cu caracter personal.
3.	Referința la documentul de planificare care prevede elaborarea proiectului (PNA, PND, PNR, alte documente de planificare sectoriale)	-
4.	Lista autorităților și instituțiilor a căror avizare este necesară	1. Ministerul Justiției; 2. Ministerul Finanțelor; 3. Procuratura Generală; 4. Ministerul Dezvoltării Economice și Digitalizării; 5. Serviciul Tehnologia Informației și Securitate Cibernetică; 6. Agenția Națională pentru Reglementare în Comunicații; 7. Agenția Servicii Publice;

		8. Consiliul Concurenței; 9. Agenția de Guvernare Electronică; 10. Cancelaria de Stat; 11. Inspectoratul de Stat pentru Supravegherea Produselor Nealimentare și Protecția Consumatorilor; 12. Serviciul de Informații și Securitate; 13. Centrul Național pentru Protecția Datelor cu Caracter Personal. Expertizare: 1. Ministerul Justiției; 2. Centrul Național Anticorupție.
5.	Termenul-limită pentru depunerea avizelor/expertizelor	10 zile
6.	Persoana responsabilă de promovarea proiectului	Ștefan Buzu, ofițer principal al Secției politici în domeniul ordinii și securității publice a Direcției politici în domeniul ordinii și securității publice, combaterii criminalității al MAI, email: stefan.buzu@mai.gov.md , tel: 022 255-750.
7.	Anexe	1. Proiectul actului normativ; 2. Nota de fundamentare; 3. Tabelul comparativ.
8.	Data și ora depunerii cererii	Conform semnăturii electronice
9.	Semnat electronic	Daniella MISAIL-NICHITIN Ministrul afacerilor interne