Aprobat în ședința Guvernului din __/____2026
prin decizia protocolară nr._____/2026

Proiect

L E G E
pentru completarea cu articolul 125[1]
a Legii comunicațiilor electronice nr. 72/2025

Parlamentul adoptă prezenta lege organică.

Articolul I. – Legea comunicațiilor electronice nr. 72/2025 (Monitorul Oficial al Republicii Moldova, 2025, nr. 226-228, art. 266) cu modificările ulterioare, se completează cu articolul 125[1], cu următorul cuprins:

„**Articolul 125[1].** Identificarea utilizatorilor serviciilor de comunicații electronice mobile accesibile publicului și protecția confidențialității datelor.

(1) Furnizorii de servicii de comunicații electronice mobile accesibile publicului sunt obligați să identifice utilizatorii 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 utilizatorilor se realizează în baza unui act de identitate valabil sau prin mijloace de identificare electronică, cu colectarea următoarelor date:

a) pentru persoanele fizice care se identifică cu acte de identitate emise de Republica Moldova – numele, prenumele, IDNP, datele actului de identitate (denumirea, seria, numărul), iar furnizorul de servicii de comunicații electronice mobile accesibile publicului verifică datele și valabilitatea acestuia cu interogarea Sistemului informațional „Registrul de stat al populației”, prin intermediul platformei de interoperabilitate MConnect, în condițiile Legii nr.142/2018 cu privire la schimbul de date și interoperabilitate;

b) 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), iar furnizorul de servicii de comunicații electronice mobile accesibile publicului reține o copie a actului de identitate, în condițiile legislației privind protecția datelor cu caracter personal.

c) pentru persoanele juridice din Republica Moldova – denumirea, IDNO, precum și datele prevăzute la lit. a) sau b) referitoare la persoana împuternicită să reprezinte utilizatorul în legătură cu identificarea acestuia;

d) 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 lit. a) sau b) referitoare la persoana împuternicită să reprezinte utilizatorul în legătură cu identificarea acestuia, iar furnizorul de servicii de comunicații electronice mobile accesibile publicului reține copia documentului care atestă înregistrarea persoanei juridice în registrul comercial al statului străin.

(3) La alegerea furnizorilor de servicii de comunicații electronice mobile accesibile publicului, identificarea utilizatorilor 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 de servicii de comunicații electronice mobile accesibile publicului;

2) în punctele de vânzare ale persoanelor împuternicite de operator, astfel cum sunt definite în art. 4 al Legii nr. 195/2024 privind protecția datelor cu caracter personal, în baza unui contract sau a unui alt temei juridic corespunzător;

3) la distanță, prin:

a) mijloace de identificare electronică (semnătură electronică calificată) 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, cu interogarea, în măsura în care este aplicabil, a Sistemului informațional „Registrul de stat al populației”, prin intermediul platformei de interoperabilitate MConnect, în condițiile Legii nr. 142/2018 cu privire la schimbul de date și interoperabilitate;

c) alte mijloace electronice oferite de către furnizorul de servicii de comunicații electronice mobile accesibile publicului, în cazul în care datele de identificare ale utilizatorului au fost anterior verificate în legătură cu un alt număr prin una dintre metodele prevăzute la subpct. 1) și 2), precum și la lit. a) și b).

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

(5) În procesul de identificare, 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.

(1) Prezenta lege intră în vigoare la expirarea a 12 luni de la data publicării în Monitorul Oficial al Republicii Moldova.

(2) Prevederile prezentei legi se aplică doar numerelor activate după data intrării în vigoare a prezentei legi.

(3) Până la intrarea în vigoare a prezentei legi, Agenția Națională pentru Reglementare în Comunicații:

a) va aproba reglementările privind stabilirea serviciilor tehnice minime necesare menționate la art. I, în partea ce vizează redacția art. 125^1 alin. (4) al Legii comunicațiilor electronice nr. 72/2025;

b) își va aduce actele sale normative în concordanță cu prezenta lege.

PREŞEDINTELE PARLAMENTULUI

NOTA DE FUNDAMENTARE
la proiectul de lege pentru completarea cu articolul 125[1] a Legii comunicațiilor electronice nr. 72/2025

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ

Autorul proiectului: Ministerul Afacerilor Interne.

2. Condițiile ce au impus elaborarea proiectului actului normativ

2.1 Temeiul legal sau, după caz, sursa proiectului actului normativ

Temeiul legal al intervenției rezidă în obligația statului de a asigura ordinea și securitatea publică. Din perspectiva dreptului Uniunii Europene, deși piața comunicațiilor este reglementată de Directiva (UE) 2018/1972 (Codul european al comunicațiilor electronice), temeiul acțiunii este „clauza de salvgardare" de la art. 1 alin. (3) lit. c) și Considerentul (6) din Directivă, care permite statelor membre să deroge de la normele pieței comunicațiilor electronice pentru a asigura ordinea publică, siguranța publică și pentru a permite investigarea infracțiunilor. La nivelul drepturilor fundamentale și protecției datelor cu caracter personal, intervenția se fundamentează pe art. 6 alin. (1) lit. c) și art. 23 alin. (1) din Regulamentul (UE) 2016/679 (GDPR), precum și pe dispozițiile specifice ale Directivei ePrivacy. Legalitatea și proporționalitatea instituirii acestei obligații sunt validate direct de jurisprudența Curții de Justiție a UE (cauza Ministerio Fiscal, 2018) și a Curții Europene a Drepturilor Omului (cauza Breyer c. Germaniei, 2020), care au statuat definitiv că identificarea utilizatorilor de cartele SIM reprezintă o ingerință limitată și justificată de scopurile securității naționale și prevenirii criminalității.

La nivel național, intervenția se va realiza prin completarea Legii comunicațiilor electronice nr. 72/2025 cu un nou articol (art. 125[1]), instituind astfel obligația furnizorilor de a identifica utilizatorii serviciilor mobile preplătite cel târziu la momentul activării acestora. Modificarea Legii nr. 72/2025 creează „obligația legală" imperativă care va servi drept temei juridic pentru prelucrarea datelor cu caracter personal de către operatori, în strictă corespundere cu art. 5 alin. (1) lit. c) din noua Lege nr. 195/2024 privind protecția datelor cu caracter personal.

Proiectul actului normativ a fost elaborat din proprie inițiativă de către Ministerul Afacerilor Interne, cu scopul de a soluționa un vid legislativ (o lacună normativă) critic pentru securitatea statului. Intervenția a fost impusă de necesitatea curmării accesului neîngrădit și anonim la cartelele SIM preplătite, care, în perioada anilor 2020-2025, s-a transformat dintr-o vulnerabilitate administrativă într-un instrument logistic de bază exploatat pe scară largă pentru crima organizată transfrontalieră, fraude informatice, escrocherii, alerte false cu bombă la infrastructuri critice și coordonarea de la distanță a echipamentelor cu dublă destinație (ex: drone implicate în contrabandă). Totodată, proiectul aliniază standardele de siguranță națională la eforturile generale de integrare a Republicii Moldova în Piața Unică Digitală a Uniunii Europene.

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

În prezent, piața națională numără 1.595.986 de cartele SIM preplătite active (reprezentând aprox. 42,7% din totalul conexiunilor mobile). Vulnerabilitatea derivă din arhitectura lanțului de distribuție: 88% din vânzări se realizează printr-o rețea indirectă de peste 3.700 de puncte comerciale terțe nespecializate (chioșcuri, stații PECO, oficii poștale), unde achiziția, activarea și utilizarea se fac complet anonim.

Cauza principală a problemei o constituie acest acces facil și nerestricționat la instrumente de telecomunicații neidentificabile, care a transformat cartelele preplătite în instrumentul logistic de bază pentru criminalitate. Doar în anul 2025, s-au înregistrat 1.190 de alerte false cu bombă și apeluri intenționat false la serviciile de urgență. Din cauza anonimatului, rata de impunitate este de peste 95% (doar 1 din 29 de dosare a ajuns în instanță în 2025), statul suportând prejudicii economice de peste 1.000.000 MDL per incident (exemplu: o alertă falsă cu bombă la Aeroportul Internațional „Eugen Doga").

Paralel, escrocheriile financiare și campaniile de tip phishing (inclusiv schema „ruda implicată în accident"), facilitate de validarea conturilor false (Viber, WhatsApp, Telegram) folosind numere anonime, au produs victimelor prejudicii de până la 100 de milioane MDL în ultimii 5 ani. Fenomenul a escaladat și în zona echipamentelor cu dublă destinație: dronele

implicate în contrabandă la frontieră (cu o creștere a incidentelor de 920% în ultimii 5 ani, ajungând la 129 în 2025) sunt teleghidate prin rețele mobile utilizând cartele SIM anonime de tip M2M/IoT, împiedicând identificarea operatorilor de drone iliciți.

Părțile afectate de aceste probleme sunt multiple:

Cetățenii, care devin victime ale fraudelor financiare și suferă din cauza paralizării infrastructurilor critice (instanțe de judecată, instituții de învățământ, aeroporturi chiar și spitale etc.);

Sistemul public și bugetul de stat, prin deturnarea și irosirea resurselor forțelor de intervenție (Poliție, Pompieri, Ambulanță) și imposibilitatea recuperării prejudiciilor în instanță;

Operatorii de comunicații electronice, care suportă indirect costuri logistice de gestionare a incidentelor și riscuri asupra integrității rețelelor.

Din punct de vedere normativ, domeniul este reglementat de Legea comunicațiilor electronice nr. 72/2025. Articolul 125 din această lege reglementează regimul juridic al accesului organelor de drept la datele reținute de operatori. Cu toate acestea, norma este ineficientă operativ în cazul serviciilor preplătite, deoarece obligă furnizorul să ofere autorităților date de identificare (nume, prenume) pe care acesta, legal, nu a fost obligat să le colecteze.

Astfel, se constată un vid legislativ structural ex-ante. Prezentul proiect acoperă această lacună prin introducerea noului articol 125^1, condiționând activarea tehnică a serviciilor de identificarea prealabilă a utilizatorului. Această modificare aliniază piața telecomunicațiilor la cerințele art. 5 alin. (1) lit. c) din noua Legea nr. 195/2024 privind protecția datelor cu caracter personal, creând obligația legală care justifică procesarea datelor.

Practica internațională și actele UE La nivelul Uniunii Europene, deși nu există un regulament unic de armonizare privind cartelele preplătite, legislația UE stipulează prioritatea intereselor de securitate națională. Intervenția propusă este fundamentată pe „clauza de salvgardare" din Directiva (UE) 2018/1972 (Codul european al comunicațiilor electronice) – mai exact art. 1 alin. (3) lit. c) și Considerentul (6) – care statuează expres că normele pieței telecomunicațiilor nu aduc atingere dreptului suveran al statelor membre de a adopta măsurile necesare pentru a asigura ordinea publică, securitatea publică și pentru a permite investigarea, depistarea și urmărirea penală a infracțiunilor.

Documentarea bazată pe rapoartele instituțiilor internaționale demonstrează că lipsa reglementării transformă jurisdicțiile permisive într-o sursă furnizoare de „turism SIM".

Un document de lucru recent al Președinției Poloneze a Consiliului UE (ST-5556-2025-INIT) a catalogat lipsa unor norme armonizate privind identificarea cartelelor SIM drept o amenințare directă la adresa securității publice, favorizând fenomenul de „arbitraj infracțional" transfrontalier.

Operațiunile recente ale autorităților europene demonstrează amploarea problemei. În octombrie 2025, prin Operațiunea „Simcartel", autoritățile din Austria, Estonia, Letonia și Finlanda au destructurat o rețea uriașă de tip cybercrime-as-a-service, confiscând 40.000 de cartele SIM anonime utilizate pentru a cauza fraude de aproximativ 5 milioane EUR.

Din perspectiva respectării drepturilor fundamentale și a conformității cu prevederile art. 23 din Regulamentul (UE) 2016/679 (GDPR), măsura este susținută de o jurisprudență consolidată a instanțelor europene:

Prin Hotărârea din cauza Ministerio Fiscal (C-207/16, 2018), CJUE a stabilit distincția juridică fundamentală, confirmând că accesul autorităților exclusiv la datele de identitate civilă ale abonatului, fără a viza datele de trafic sau localizare, este o imixtiune care nu poate fi calificată drept „gravă", fiind pe deplin proporțională pentru investigarea infracțiunilor.

Prin Hotărârea în cauza Breyer c. Germaniei (Cererea nr. 50001/12, 2020), instanța a validat explicit regimurile de identificare obligatorie a cartelelor SIM preplătite, statuând că aceasta constituie o ingerință limitată și justificată, necesară într-o societate democratică pentru combaterea criminalității.

În baza acestor documentări, precum și a analizei din statele care au aplicat măsura (ex. Polonia a raportat o scădere a alertelor false cu 93-95% și dublarea ratei de detecție a făptuitorilor de la 30% la 70%), prezentul proiect a fost calibrat sub forma modelului „Digital First", oferind un răspuns direct problemelor expuse, adaptat specificului național și în deplină concordanță cu legislația și practicile UE.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul de act normativ propune completarea Legii comunicațiilor electronice nr. 72/2025 cu un nou articol – 125^1 – care instituie obligația identificării utilizatorilor de servicii mobile preplătite. Pentru a asigura un echilibru între securitatea publică, protecția datelor cu caracter personal și viabilitatea economică, proiectul implementează versiunea agreată interinstituțional „Digital First" (Opțiunea D), care include următoarele elemente noi și soluții tehnice:

Se instituie obligația furnizorilor de a identifica utilizatorii cel târziu la momentul activării cartelei. Prin această normă, comercializarea fizică a cartelelor în cele peste 3.700 de puncte terțe nespecializate (chioșcuri, oficii poștale, stații PECO) rămâne complet nerestricționată, cartelele fiind vândute ca produse neactivate. Aceasta elimină blocajele logistice și riscurile majore de scurgeri de date asociate colectării actelor de identitate la ghișeu de către personal neinstruit.

Proiectul definește exhaustiv și limitativ setul de date colectate (nume, prenume, IDNP/datele actului de identitate). Pentru cetățenii și persoanele juridice rezidente, se interzice expres reținerea copiilor de pe actele de identitate. Verificarea identității acestora se va realiza strict automatizat. Reținerea copiei actului de identitate sau a documentului de înregistrare este permisă de lege exclusiv în cazul persoanelor fizice și juridice nerezidente (străine), deoarece statul nu deține acces la registrele altor state pentru a le verifica datele electronic, aceasta fiind singura modalitate de a asigura trasabilitatea.

Identificarea va fi validată prin verificarea datelor și valabilitatea acestora cu interogarea Sistemului informațional „Registrul de stat al populației", prin intermediul platformei de interoperabilitate MConnect, în condițiile Legii nr.142/2018 cu privire la schimbul de date și interoperabilitate.

Pentru a nu periclita dezvoltarea tehnologiei eSIM și accesul diasporei sau al turiștilor, legea reglementează metode de identificare la distanță: utilizarea mijloacelor de identificare electronică (semnătura electronică calificată, conform Legii nr. 124/2022), portofele pentru identitate digitală furnizate de stat, proceduri biometrice (eKYC) cu raportare la sursa autentică și reutilizarea datelor deja verificate de operator. Aceasta digitalizează și simplifică procesul pentru utilizator.

Pentru a preveni utilizarea anonimă a cartelei imediat după achiziție, se instituie regula conform căreia, până la finalizarea identificării, cartela SIM/eSIM poate fi utilizată doar pentru „servicii tehnice minime". Pentru a asigura adaptabilitatea legii la inovațiile tehnologice, definirea exactă a acestor servicii (ex: exclusiv apeluri la 112 sau trafic de date strict către portalul de identificare) este delegată autorității de reglementare (ARCOM) prin acte normative subsecvente.

Pentru a asigura conformitatea cu normele de protecție a datelor cu caracter personal (GDPR / Legea nr. 195/2024), obligația de stocare a datelor de identificare este strict limitată la durata utilizării serviciului și o perioadă de exact 12 luni de la încetarea utilizării numărului. Această perioadă este pragul minim necesar pentru a asigura trasabilitatea în cazul investigațiilor.

Pentru a asigura predictibilitatea pentru sectorul privat și a nu perturba piața comunicațiilor electronice, implementarea noilor norme este însoțită de două garanții legale majore, incluse în Articolul II din proiect:

Obligația de identificare se aplică exclusiv numerelor noi, activate după data intrării în vigoare a legii. Această abordare protejează baza actuală de aproximativ 1,6 milioane de clienți preplătiți existenți, eliminând riscul de pierdere a utilizatorilor, prevenind blocajele comerciale și protejând integral veniturile curente ale operatorilor.

Legea va intra în vigoare la expirarea unui termen de 12 luni de la publicare. Această perioadă de tranziție este timpul necesar și suficient oferit furnizorilor pentru a planifica bugetele, a derula procedurile de achiziție, a dezvolta/integra soluțiile digitale de identificare la distanță (eKYC) și a adapta sistemele interne de facturare și gestiune (Billing/CRM), fără a periclita calitatea serviciilor prestate. Termenul este deplin justificat și realizabil, luând în considerare faptul că operatorii dispun deja, în mare parte, de expertiza, fluxurile și infrastructura necesară, procesele de identificare, validare și stocare securizată a datelor cu caracter personal fiind deja dezvoltate și aplicate cu succes în prezent pentru utilizatorii de servicii pe bază de contract (abonamente).

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

Pentru a asigura un echilibru între necesitățile de securitate națională, constrângerile economice ale industriei TIC și rigorile privind protecția datelor cu caracter personal, au fost analizate și respinse următoarele opțiuni alternative:

Opțiunea zero (Menținerea regimului actual și identificarea voluntară):

Această opțiune a fost respinsă deoarece menținerea anonimatului structural perpetuează o vulnerabilitate majoră exploatată direct în activități infracționale (fraude bancare, alerte false, escrocheriile, teleghidarea dronelor). Promovarea exclusivă a identificării voluntare (prin acordarea de bonusuri) s-a dovedit ineficientă, întrucât persoanele care utilizează comunicațiile în scopuri ilicite nu optează voluntar pentru declararea identității. Păstrarea vidului legislativ ar menține Republica Moldova ca sursă de „turism SIM" pentru rețelele criminale transfrontaliere, un risc confirmat de documentele de securitate ale Consiliului UE (ST-5556-2025-INIT).

Opțiunea identificării fizice obligatorii la momentul comercializării (inclusiv aplicarea retroactivă):

Această opțiune (care presupune prezentarea, copierea și stocarea actului de identitate la chioșc/magazin) a fost respinsă categoric din rațiuni logistice, economice și de securitate a datelor. Conform datelor furnizate de operatori, 88% din cartelele preplătite sunt vândute printr-o rețea de distribuție de peste 3.700 de puncte terțe nespecializate (chioșcuri de ziare, stații PECO, oficii poștale). Aceste locații nu dispun de infrastructura tehnică securizată și de personalul calificat necesar pentru prelucrarea datelor cu caracter personal, generând un risc major de scurgeri de date pe piața neagră. Din punct de vedere juridic, tentativele similare din alte state au eșuat tocmai din cauza acestor deficiențe de colectare. De exemplu, în România, măsurile de înregistrare au fost declarate neconstituționale (Decizia Curții Constituționale nr. 440/2014) din cauza lipsei garanțiilor de securitate pentru datele colectate fizic și a aplicării retroactive, aspecte care au generat un caracter intruziv disproporționat. De asemenea, impunerea acestei măsuri ar fi blocat complet dezvoltarea segmentului de tehnologie eSIM (activare online) și ar fi redus accesibilitatea serviciilor în mediul rural.

Spre deosebire de opțiunile enunțate, s-a decis implementarea modelului de reglementare agreat „Digital First" (Opțiunea D), evaluat ca fiind soluția proporțională și fezabilă. Acest model decuplează comercializarea de procesul de identificare: cartelele vor fi vândute în continuare liber în rețelele terțe ca produse neactivate, fără identificare la ghișeu sau alt punct de vânzare. Identificarea se mută strict în sarcina furnizorului de comunicații și se realizează exclusiv într-un mediu securizat (digital prin instrumente eKYC, identitate digitală, interogare automatizată MConnect, sau fizic exclusiv în punctele de vânzare proprii ale furnizorului sau ale persoanelor împuternicite de acesta, în baza unui contract ori a unui alt temei juridic corespunzător), cel târziu la momentul activării serviciului. Această variantă respectă rigorile Legii nr. 195/2024 privind protecția datelor cu caracter personal și a fost consultată și validată oficial de Ministerul Dezvoltării Economice și Digitalizării, prin comunicarea din 19 decembrie 2025, drept „cea mai optimă din perspectiva implementării".

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Intervenția legislativă va genera efecte pozitive directe asupra sectorului public, în special pentru sistemul național de urgență, organele de drept și bugetul de stat, prin eliminarea vulnerabilităților generate de anonimatului comunicațiilor.

Prin atribuirea certă a unui număr de telefon unei identități reale, autoritățile obțin elementul de trasabilitate necesar în faza inițială a investigațiilor, reducând timpul alocat profilării suspecților. Practica statelor europene care au implementat măsuri similare (ex: Polonia) demonstrează că eliminarea anonimatului dublează rata de identificare a făptuitorilor, înregistrându-se o creștere a detecției de la o medie de 30% la 60-70%.

În anul 2025, la Serviciul 112 s-au înregistrat 1.190 de apeluri apeluri intenționat false și alerte cu bombă efectuate de pe cartele neidentificate. O singură mobilizare a forțelor specializate (IGP, IGSU, IGC) extrage din bugetul public peste 10.132 MDL, statul cheltuind anual aproximativ 10 milioane de lei exclusiv pentru reacția la alerte false. Conform datelor comparative, impunerea identificării are un efect de descurajare, înregistrându-se o reducere cu

93-95% a numărului de alerte false (de la aproximativ 4.000 la 200 de cazuri anual). Pe lângă criza alertelor false, trebuie subliniat impactul masiv asupra organelor de drept implicate în investigarea escrocheriilor și a fraudelor cibernetice (precum schemele „ruda implicată în accident" sau phishing), care au produs prejudicii considerabile de peste 10 de milioane MDL în ultimul an. În prezent, eforturile de investigare care sunt frecvent epuizate sau blocate de imposibilitatea asocierii numerelor cu o identitate, fenomen care a condus la clasarea majorității dosarelor penale (ex: 33 din 57 dosare clasate în 2024) și a garantat practic impunitatea infractorilor. Identificarea utilizatorilor va debloca resursele umane și operaționale ale poliției, transformându-le din investigații de lungă durată și deseori fără finalitate într-un proces operativ mult mai țintit.

Alertele false la adresa infrastructurilor critice (ex: Aeroportul Internațional „Eugen Doga") paralizează activitatea și generează prejudicii economice directe de peste 1.000.000 MDL per incident. Este important de evidențiat impactul specific al alertelor cu bombă efectuate prin intermediul apelurilor telefonice: spre deosebire de amenințările transmise prin e-mail, apelurile vocale efectuate de pe numere mobile (frecvent cartele preplătite anonime) implică, conform protocoalelor stricte de evaluare a riscurilor, un grad ridicat de iminență. Aceasta obligă autoritățile să declanșeze imediat măsurile maxime de securitate, precum evacuarea totală a aeroporturilor sau instanțelor, deturnarea curselor și blocarea terminalelor. În prezent, din cauza imposibilității asocierii numărului cu un făptuitor, rata de impunitate este de peste 95%, doar 1 din 29 de dosare penale pornite în 2025 ajungând în instanță. Identificarea certă a utilizatorilor va oferi statului și entităților afectate instrumentul juridic necesar pentru a înainta acțiuni civile în regres, recuperând astfel costurile intervențiilor și daunele direct din contul infractorilor.

Obligarea furnizorilor de a colecta și valida datele prin intermediul platformei guvernamentale MConnect și al registrelor de stat asigură exactitatea bazei de date. Această arhitectură tehnică diminuează drastic numărul solicitărilor birocratice formulate de organele de drept pentru clarificarea unor identități false și optimizează calitatea și viteza schimbului interinstituțional de informații.

4.2 Impactul financiar și argumentarea costurilor estimative

Implementarea regimului de identificare digitală (Opțiunea D) necesită adaptarea sistemelor interne ale operatorilor (Billing/CRM) și integrarea soluțiilor la distanță (eKYC). Conform datelor oficiale furnizate direct de operatorii de telefonie mobilă în cadrul consultărilor tehnice (prin scrisorile nr. 01-07/9974 din 19.11.2025 și nr. 19504-11/25 din 21.11.2025), investițiile inițiale la nivelul operatorilor sunt estimate între 3,0 și 6,8 milioane MDL. Cifrele sunt expuse agregat pentru a proteja secretul comercial al entităților.

Verificarea identității va genera costuri tranzacționale. Schimbul de date cu participanții privați are loc în conformitate cu prevederile Legii nr. 142/2018 cu privire la schimbul de date și interoperabilitate și ale Hotărârii Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect) și este cu titlu oneros, în baza contractului încheiat cu autoritatea competentă. În conformitate cu pct. 60 și 61 din Regulamentul aprobat prin Hotărârea Guvernului nr. 211/2019, furnizorii vor achita o taxă unică de configurare de 1.000 MDL și un tarif de 0,25 MDL pentru fiecare interpelare. Suplimentar, vor exista costuri anuale de mentenanță tehnică și pentru licențele soluțiilor de identificare.

Efortul financiar plasat pe sectorul privat este proporțional și atenuat prin trei garanții legale:

1. Măsura se aplică exclusiv numerelor activate după intrarea în vigoare a legii. Prin urmare, operatorii sunt scutiți de plata taxelor MConnect și de costurile logistice pentru reînregistrarea celor aproximativ 1,59 milioane de cartele preplătite deja active.
2. Abordarea „Digital First" decuplează vânzarea de activare, scutind operatorii de costuri nesustenabile pe care le-ar fi generat echiparea IT și instruirea personalului în cele peste 3.700 de puncte terțe de distribuție (chioșcuri, stații PECO, oficii poștale).
3. Termenul de 12 luni asigură timpul și predictibilitatea financiară necesare pentru planificarea bugetelor CAPEX, realizarea achizițiilor și testarea sistemelor, fără riscul unor întreruperi operaționale.

4.3 Impactul asupra sectorului privat

Implementarea obligației de identificare generează un impact direct asupra modelului de afaceri al operatorilor de comunicații. Pentru a proteja mediul privat, a preveni blocajele

comerciale, proiectul adoptă după multiple consultări modelul agreat „Digital First” (Opțiunea D), care neutralizează constrângerile majore pe următoarele direcții:

Conform datelor furnizate, 88% din cartelele preplătite sunt comercializate prin peste 3.700 de puncte de vânzare nespecializate, cum ar fi chioșcuri, oficii poștale și stații PECO. Aceste locații nu dispun de infrastructura tehnică și competențele necesare pentru a verifica actele de identitate și a respecta normelor de protecție a datelor. Pentru a preveni acest fenomen canal comercial, proiectul decuplează comercializarea de activare. Cartelele vor fi vândute în continuare liber, ca produse neactivate, scutind micii comercianți de orice procedură de identificare.

Impunerea prezenței fizice pentru identificare ar fi blocat comercializarea produselor digitale (eSIM) și ar fi creat impedimente pentru turiști sau diasporă. Proiectul soluționează aceasta prin reglementarea expresă a procedurilor de identificare la distanță. Operatorii pot utiliza mijloace de identificare electronică, interogarea automatizată prin platforma MConnect și soluții eKYC (cu verificare biometrică), menținând astfel un flux de activare digital, rapid și sigur.

Sistemele interne de facturare și gestiune a clienților ale operatorilor necesită modificări pentru a asocia și administra datele personale ale utilizatorilor preplătiți. Pentru a preîntâmpina riscurile de întrerupere a serviciilor și a asigura predictibilitatea, proiectul instituie două garanții majore pentru sectorul privat:

1. Norma se aplică exclusiv numerelor activate după data intrării în vigoare a legii. Aceasta scutește operatorii de sarcina logistică și financiară de a reînregistra baza actuală de aproximativ 1,59 milioane de utilizatori preplătiți, protejând veniturile curente.

2. Stabilirea termenului de 12 luni de la publicare până la intrarea în vigoare oferă furnizorilor timpul imperativ necesar pentru a derula achizițiile, a dezvolta interfețele IT și a realiza testarea sistemelor, fără a periclita calitatea serviciilor prestate.

4.4 Impactul social

Proiectul generează un impact social pozitiv, bazat pe creșterea siguranței fizice și financiare a cetățenilor.

Anonimatul cartelelor este exploatat direct pentru a ținti categoriile sociale vulnerabile, în special persoanele în etate. În ultimii ani, escrocheriile telefonice (de tip „ruda implicată în accident” sau phishing bancar ș.a.) au cauzat victimelor prejudicii până la 100 de milioane MDL. Paralel, alertele false perecletează activitatea obiectelor de infrastructură critică (spitale, aeroport, instanțe de judecată etc.), care pune în pericol direct siguranța cetățenilor. Eliminarea anonimatului blochează instrumentul logistic de bază al acestor infracțiuni.

Pentru a răspunde obiecțiilor privind riscul îngrădirii accesului la comunicații pentru populația din mediul rural (care reprezintă 56,2% din populație) și persoanele cu mobilitate redusă, proiectul adoptă Opțiunea D. Aceasta nu impune deplasarea cetățenilor în centre raionale. Achiziția fizică a cartelelor rămâne neschimbată, acestea vor putea fi cumpărate liber, sub formă neactivată, din orice chioșc sau magazin. Identificarea se efectuează la activare și poate fi realizată prin metode la distanță (eKYC, identitate digitală) sau în rețelele autorizate, asigurând accesul rapid. De asemenea, prin aplicarea neretroactivității, legea nu va impune nicio sarcină birocratică celor peste 1,5 milioane de utilizatori preplătiți existenți.

Pentru a elimina riscurile ca datele personale ale cetățenilor să fie sustrase sau vândute pe piața neagră, s-a exclus intenționat obligativitatea prezentării și copierii actelor de identitate în cele peste 3.700 de puncte de vânzare terțe nespecializate (stații PECO, chioșcuri, oficii poștale). Validarea identității se va face automatizat, exclusiv în mediul securizat al furnizorului sau prin platforma MConnect, cu respectarea principiului principiul reducerii la minimum a datelor prevăzut de Legea nr. 195/2024. Datele vor fi păstrate strict pe durata utilizării numărului și 12 luni după încetarea serviciului.

4.4.1 Impactul asupra datelor cu caracter personal

Modificările propuse implică prelucrarea datelor cu caracter personal, însă acest impact este încadrat într-un regim juridic strict, proporțional și fundamentat pe excepțiile prevăzute de art. 23 din Regulamentul (UE) 2016/679 (GDPR) și Legea nr. 195/2024 privind protecția datelor cu caracter personal. Ingerința este limitată la ceea ce este necesar pentru atingerea obiectivelor de securitate publică și prevenire a infracțiunilor, fiind guvernată de următoarele garanții tehnice și juridice:

Colectarea exclusivă a datelor de identitate civilă la momentul activării, fără a reține date de trafic sau de localizare, constituie o ingerință „limitată”. Legalitatea acestui regim a fost validată definitiv de Curtea de Justiție a Uniunii Europene (cauza Ministerio Fiscal, 2018) și de Curtea Europeană a Drepturilor Omului (cauza Breyer c. Germaniei, 2020), măsura este pe deplin proporțională cu scopul securității naționale.

Pentru a preveni colectarea abuzivă și a respecta principiul minimizării prevăzut de Legea nr. 195/2024, proiectul definește o listă exhaustivă a datelor prelucrate (nume, prenume, IDNP/datele actului de identitate). Reținerea copiei actului este permisă în cazul cetățenilor și entităților străine (nerezidenți), ca unică metodă tehnică de asigurare a trasabilității, în lipsa posibilității de verificare automatizată a acestora în registrele de stat naționale.

Prin adoptarea modelului „Digital First” (Opțiunea D), se elimină vulnerabilitatea colectării și stocării nesigure a datelor pe suport de hârtie în cele peste 3.700 de puncte de vânzare terțe nespecializate. Validarea identității cetățenilor se va realiza strict automatizat, cu interogarea Sistemului informațional „Registrul de stat al populației”, prin intermediul platformei de interoperabilitate MConnect, în condițiile Legii nr.142/2018 cu privire la schimbul de date și interoperabilitate. Această variantă asigură criptarea transmisiunilor și jurnalizarea (MLog) fiecărei accesări, garantând trasabilitatea operațiunilor și prevenind tehnic furtul de identitate.

Datele de identificare vor fi stocate de către furnizorii de comunicații doar pe durata utilizării serviciului și pentru o perioadă strict determinată de 12 luni de la încetarea utilizării numărului de telefon. Acest termen reprezintă pragul minim necesar pentru a asigura trasabilitatea în cadrul investigațiilor.

Operatorii de comunicații electronice rămân operatori de date cu drepturi și obligații depline privind securitatea informației. Introducerea noilor soluții de identificare digitală la distanță (eKYC) impune operatorilor, în baza dispozițiilor generale și obligatorii ale Legii nr. 195/2024 (și a art. 23-25 din Legea nr. 133/2011), obligația de a efectua o Evaluare a Impactului asupra Protecției Datelor (DPIA) și de a consulta în prealabil Centrul Național pentru Protecția Datelor cu Caracter Personal, nefiind necesară dublarea acestor obligații procedurale în textul legii.

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

Modificarea propusă are un impact direct asupra capacității statului de a contracara amenințările hibride. Dincolo de comunicațiile interumane (apeluri, SMS), cartelele preplătite anonime sunt exploatate pe scară largă în conexiunile de tip M2M/IoT (Machine-to-Machine / Internet of Things). Aceste conexiuni netrasabile sunt utilizate ca instrumente logistice pentru teleghidarea dronelor de contrabandă și operarea sistemelor tehnice ilicite.

Menținerea cadrului normativ actual transformă Republica Moldova într-o sursă furnizoare de „turism SIM” pentru rețelele de criminalitate organizată transfrontalieră. La nivelul Uniunii Europene, nu există în prezent un regulament unic armonizat care să impună înregistrarea obligatorie a cartelelor preplătite, decizia fiind lăsată în competența națională. Această abordare decurge din prevederile Directivei (UE) 2018/1972 (Codul european al comunicațiilor electronice), care instituie o „clauză de salvgardare” la art. 1 alin. (3) lit. c), stipulând expres că normele europene nu aduc atingere acțiunilor întreprinse de statele membre pentru a asigura ordinea publică, siguranța publică și investigarea infracțiunilor.

Implementarea obligației de identificare aliniază statul la standardele de securitate aplicate în prezent de majoritatea statelor membre ale Uniunii Europene. Conform datelor comparative, această practică este implementată de 16 din cele 27 de state membre ale UE (inclusiv state precum Germania, Franța, Spania și Polonia), regimul de identificare obligatorie acoperind în prezent aproximativ 81,85% din populația Uniunii Europene. Această aliniere este esențială pentru facilitarea schimbului operativ de date și a cooperării polițienești transfrontaliere în cadrul mecanismelor europene de Justiție și Afaceri Interne (JAI), precum sistemul Prüm II (Regulamentul (UE) 2024/982).

Vulnerabilitatea generată de lipsa unei armonizări depline a fost recunoscută oficial la nivelul Consiliului UE. Președinția Poloneză a Consiliului a avertizat, prin documentul de lucru ST-5556-2025-INIT, că infractorii exploatează acest vid prin „arbitraj infracțional", achiziționând cartele anonime din state fără obligații de înregistrare pentru a comite fapte ilegale în alte state cu controale stricte. Experiența practică a Poloniei demonstrează necesitatea și eficiența măsurii: după introducerea obligativității înregistrării în 2016, volumul alertelor false cu bombă a scăzut drastic cu 93-95% (de la aprox. 4.000 la 200 de cazuri anual), iar rata de identificare a făptuitorilor s-a dublat de la 30% la 60-70%.

În prezent, rata infracțiunilor comise prin intermediul cartelelor anonime (alerte false cu bombă, escrocherii) este una ridicată. Identificarea certă a titularilor numerelor de telefon va oferi organelor de urmărire penală elementul de trasabilitate inițial necesar pentru identificarea suspecților. Mai mult, obținerea identității făptuitorilor va oferi statului și entităților afectate instrumentul juridic imperativ pentru a iniția acțiuni civile în regres, permițând recuperarea prejudiciilor economice și a costurilor de intervenție (care depășesc 10.000 MDL pentru fiecare mobilizare a forțelor MAI) direct din contul infractorilor.

5. Compatibilitatea proiectului actului normativ cu legislația UE

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

Nu se aplică

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

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 ale Legii nr. 239/2008 privind transparența în procesul decizional, anunțul privind inițierea elaborării proiectului de lege, însoțit de nota de fundamentare, a fost plasat pentru consultare publică pe platforma guvernamentală particip.gov.md:

(link: https://particip.gov.md/ro/document/stages/*/16061).

Suplimentar procedurilor standard, pe parcursul elaborării și definitivării inițiativei, proiectul a fost supus unor consultări tehnice ample și ședințe ale grupului de lucru cu participarea reprezentanților mediului de afaceri, în special a operatorilor de comunicații electronice (S.A. „Moldtelecom", S.A. „Moldcell", Î.M. „Orange Moldova" S.A.) și a Asociației Naționale a Companiilor din Domeniul TIC (ATIC).

Au fost organizate ședințe de lucru interinstituționale (în datele de 4, 8 și 24 decembrie 2025) cu participarea MAI, Ministerului Dezvoltării Economice și Digitalizării (MDED), ANRCOM, Centrului Național pentru Protecția Datelor cu Caracter Personal (CNPDCP) și a reprezentanților industriei. În rezultatul acestor consultări și al examinării poziției oficiale a ATIC (nr. 757 din 18.02.2026), au fost preluate și integrate propunerile mediului de afaceri privind atenuarea riscurilor logistice, fiind agreat consensul tehnic pentru adoptarea modelului „Digital First" (Opțiunea D). Această opțiune a fost validată oficial și de MDED drept cea mai optimă soluție din perspectiva implementării.

În procesul de avizare externă, proiectul a fost expediat autorităților și instituțiilor publice. Propunerile și recomandările pertinente au fost luate în considerare, acceptate și integrate în textul final al proiectului. Argumentarea detaliată pentru fiecare decizie se regăsește în Tabelul de sinteză a obiecțiilor și propunerilor, anexat la prezentul proiect.

7. Concluziile expertizelor

Proiectul de act normativ a fost supus expertizei anticorupție și expertizei juridice, rezultatele fiind examinate și reflectate detaliat în Tabelul de sinteză a obiecțiilor și propunerilor:

Potrivit Raportului de expertiză anticorupție nr. ELO26/11429 din 06.05.2026 elaborat de Centrul Național Anticorupție, s-a constatat că prevederile proiectului corespund rigorilor de transparență, iar în redacția propusă, proiectul nu conține factori și riscuri de corupție.

Prin Avizul nr. 04/2-5654 din 22.05.2026, Ministerul Justiției a formulat o serie de observații conceptuale și de tehnică legislativă privind asigurarea proporționalității în prelucrarea datelor cu caracter personal, claritatea unor norme și uniformizarea terminologiei.

Urmare a examinării, unele din propunerile Ministerului Justiției au fost acceptate sau acceptate parțial, iar cele neacceptate au fost concretizate și argumentate în sinteza de propuneri și obiecții.

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 cu caracter personal.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Implementarea prevederilor prezentului proiect de lege necesită măsuri complexe de ordin normativ, tehnic și organizatoric, care vor fi realizate pe parcursul termenului de tranziție de 12 luni de la publicare, după cum urmează:

Autoritatea de reglementare în domeniul comunicațiilor electronice (ARCOM) va elabora, va supune consultărilor și va aproba actele normative necesare. În mod prioritar, va stabili explicit „serviciile tehnice minime” care vor putea fi utilizate de consumatori pe cartelele noi până la finalizarea procesului de identificare.

În perioada de tranziție, operatorii de comunicații mobile vor parcurge următoarele etape logistice și tehnologice:

Ajustarea sistemelor interne (aplicații de activare, Billing/CRM) și realizarea integrărilor securizate cu sistemele informaționale ale statului pentru validarea identității (interogarea prin platforma guvernamentală MConnect).

Testarea integrată a fluxurilor operaționale pentru garantarea protecției datelor cu caracter personal și a stabilității rețelelor.

Ministru **Daniella MISAIL-NICHITIN**

SINTEZA
la proiectul de lege pentru completarea cu articolul 125[1] a Legii comunicațiilor electronice nr. 72/2025

Participantul la avizare, consultare publică, expertizare	Nr. crt.	Conținutul obiecției, propunerii, recomandării, concluziei	Argumentarea autorului proiectului
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			
Utilizator www.particip.gov.md Data expediere: 05.02.2026	1.	Ceea ce propuneți Dvs este o trăsătură a statelor cu libertăți limitate. Republica Moldova va fi un stat mai incomod datorită unei astfel de schimbări. La moment este un mare, mare avantaj pentru turismul din Moldova faptul că poți cumpăra eSIM cu câteva clickuri pe telefon, fără nevoi birocratice. Ceea ce propuneți Dvs complică viața cetățenilor, complică viața turiștilor, pentru beneficii marginale și riscuri semnificative. Actorii care comit infracțiuni serioase vor găsi cum să-și cumpere SIM oricum. Nu uitați că este posibil să cumperi cartele SIM prepaid în alte țări, și să le folosești în roaming în Moldova. Asta doar ca exemplu. Există aplicații digitale unde poți cumpăra eSIM pentru 50-100 de țări odată, fără să dai buletinul la toate acele state. Deci dacă sarcina este să identificăm _toți_ utilizatorii de telefonie mobilă și internet mobil, este un lucru imposibil de atins. Cei care vor dori, vor găsi moduri de a activa pe teritoriul Moldovei fără prezentarea actelor proprii. Dar propunerea Dvs va adăuga birocrație la procesul simplu de achiziție a unei cartele prepaid, și va crea o sumedenie de ocazii ca datele personale să fie scurse.	**Nu se acceptă.** Proiectul urmărește un scop legitim de ordine și securitate publică: reducerea anonimatului asociat utilizării numerelor naționale preplătite și consolidarea capacității de atribuire/investigare a faptelor (inclusiv în situații de fraudă, extorcări, alerte false, abuzuri în mediul online), fără a viza conținutul comunicațiilor și fără a institui mecanisme de supraveghere generală. Standardul de evaluare al unei asemenea politici publice este eficiența rezonabilă și proporționalitatea măsurii, nu eliminarea absolută a tuturor modalităților de eludare. Faptul că pot exista SIM/eSIM emise în alte jurisdicții și utilizate în roaming nu anulează utilitatea reglementării pe segmentul asupra căruia statul are competență deplină serviciile mobile accesibile publicului furnizate pe piața națională, unde efectul practic este de descurajare a utilizării anonime și de creștere a calității investigațiilor. În același timp, proiectul nu urmărește „identificarea tuturor utilizatorilor mobili la nivel global", ci instituie o obligație clară de identificare pentru utilizarea serviciilor în regim preplătit în Republica Moldova, ca măsură de reducere substanțială a riscurilor, aliniată practicilor și reperelor europene privind echilibrul dintre securitate și viața privată. În privința turismului și a „birocrației", proiectul permite identificarea inclusiv prin mijloace digitale/identificare electronică, ceea ce menține posibilitatea unui flux rapid de achiziție și activare, inclusiv pentru eSIM. Totodată, termenul de intrare în vigoare prevăzut oferă operatorilor timpul necesar pentru adaptarea proceselor și a

			soluțiilor tehnice astfel încât impactul asupra utilizatorilor să fie minim, iar verificările să fie în mare parte automatizate. Referitor la riscurile de scurgeri de date, acestea nu reprezintă un argument pentru menținerea anonimatului structural, ci o obligație de conformare: prelucrarea datelor are temei legal, se supune principiilor de minimizare și securitate, iar operatorii au responsabilități clare (măsuri tehnice și organizatorice, control al accesului, jurnalizare/audit, termene de păstrare, răspundere contravențională/civilă, după caz), sub supravegherea autorităților competente. În concluzie, obiecția nu demonstrează lipsa de necesitate sau disproporționalitatea măsurii, iar soluțiile invocate (posibile eludări) nu infirmă utilitatea reglementării pentru piața națională.
ASOCIAȚIA NAȚIONALĂ A COMPANIILOR DIN DOMENIUL TIC Nr.757 din 18 februarie 2026	1.	**Observații privind eficiența măsurii** • Lipsa unei relații cauzale dovedite: Conform studiului GSMA[1] , nu există dovezi empirice publicate care să ateste o legătură directă între introducerea înregistrării obligatorii și reducerea activităților infracționale.	**Nu se acceptă.** Deși obiecția invocă studiul GSMA privind lipsa dovezilor empirice, datele demonstrează că eliminarea anonimatului are un impact de securitate direct și măsurabil: reduce volumul alertelor false de la un nivel sistemic (3.000-4.000/an) la (~200/an) și dublează rata de identificare a făptuitorilor de la 30%-40% la 60%-70%.
	2.	• Alternative: Există și metode mai puțin intruzive care pot contribui la atingerea acelorași scopuri în domeniul prevenirii și combaterii infracționalității.	**Nu se acceptă.** Metodele tehnice alternative (precum sistemele anti-fraudă, măsurile anti-spoofing sau cooperarea cu platformele digitale) sunt complementare și nu pot substitui necesitatea eliminării vulnerabilității fundamentale, accesul la numere naționale preplătite sub o identitate neasumată.
	3.	• Ocolirea măsurii prin cartele din alte țări: Infractorii pot utiliza în continuare cartele anonime emise în alte state, inclusiv din țările vecine; astfel de cartele pot fi achiziționate fizic sau online (eSIM). În contextul regimului „roaming ca acasă” cu Uniunea Europeană, cartelele emise în state membre UE utilizate în roaming în RM pot beneficia de aceleași tarife ca cele locale.	**Nu se acceptă.** Existența unor căi de eludare transfrontaliere (precum utilizarea cartelelor din state terțe în roaming) nu anulează utilitatea și necesitatea reglementării segmentului aflat sub competența națională. Scopul politicii publice nu este eliminarea absolută a oricărei forme de comunicare ilicită la nivel global, ci securizarea propriei infrastructuri prin tăierea accesului facil și ieftin la volume mari de numere locale anonime. Integrarea Republicii Moldova în regimul „roaming ca acasă” de la 1 ianuarie 2026 reprezintă un pas spre piața unică europeană, dar nu poate servi drept justificare pentru menținerea unui vid de securitate intern. Dimpotrivă, păstrarea anonimatului ar transforma statul nostru într-o sursă furnizoare de „turism SIM” pentru rețelele criminale regionale, fenomen recunoscut oficial de Consiliul

[1] GSMA — Digital Identity: Access to Mobile Services and Proof of Identity, 2021. — Digital-Identity-Access-toMobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf (gsma.com).

			UE drept „arbitraj infracțional”. Vulnerabilitățile generate de utilizarea cartelelor străine în roaming se combat prin instrumente de cooperare polițienească internațională (precum mecanismele europene EMPACT), nu prin abandonarea eforturilor de securizare a pieței naționale.
	4.	• Utilizarea cartelelor înregistrate pe alte persoane: Studiul GSMA citat arată că, în șapte țări cu venituri mici și medii în care s-au aplicat asemenea măsuri, circa 18% dintre deținătorii de cartele preplătite aveau cartela înregistrată pe numele unei alte persoane. Aceasta subliniază riscul ca infractorii să folosească cartele înregistrate pe terți.	**Nu se acceptă.** Riscul înregistrării cartelelor pe numele unor interpuși reprezintă un argument clar pentru instituirea unor mecanisme stricte de control, nu o justificare pentru menținerea anonimatului structural pe piața națională. Chiar și în condițiile unor posibile eludări, măsura reduce utilizarea anonimă și crește costul operațional, complexitatea logistică și riscurile pentru infractori. În plus, prin adoptarea versiunii agreate în urma ședințelor cu operatorii, care elimină colectarea fizică a actelor în mii de chioșcuri nespecializate și validează identitatea exclusiv digital și securizat (eKYC, interogarea registrelor de stat prin platforma MConnect), se diminuează direct posibilitatea înregistrărilor fictive în masă sau pe baza actelor sustrase.
	5.	• În practică, infractorii pot utiliza aplicații de tip Viber, Telegram, WhatsApp şi alte servicii „over-the-top” (OTT) pentru comunicare, precum şi aplicaţii sau servicii care permit substituirea (spoofing) identității liniei apelante. Aceste mijloace permit inițializarea şi derularea comunicațiilor fără a folosi direct o cartelă preplătită înregistrată în statul respectiv, reducând astfel eficiența măsurilor bazate exclusiv pe identificarea SIM. Prin urmare, o politică axată doar pe înregistrarea utilizatorilor de cartele preplătite riscă să nu acopere majoritatea canalelor efectiv folosite în anumite tipuri de infracționalitate.	**Nu se acceptă.** Deși infractorii pot utiliza servicii OTT (Viber, Telegram, WhatsApp), majoritatea acestor platforme necesită în mod obligatoriu un număr de telefon valid și activ pentru crearea și validarea conturilor. Prin urmare, eliminarea cartelelor preplătite anonime atinge direct în acest instrument logistic de bază, reducând capacitatea rețelelor infracționale de a genera și reseta masiv identități digitale false. În privința substituirii identității liniei apelante (spoofing), combaterea acesteia necesită într-adevăr măsuri tehnice complementare antifraudă, însă existența unor tehnici paralele de eludare nu justifică inacțiunea statului, menținerea unui vid de securitate pe piața națională și păstrarea anonimatului structural la achiziția și activarea cartelelor SIM/eSIM.
	6.	• Examenul internațional și decizii naționale: Conform studiul GSMA citat, state importante (SUA, Israel, Marea Britanie, Canada, Noua Zeelandă, Coreea de Sud și o serie de state membre UE — România, Țările Baltice, Finlanda, Suedia, Olanda, Islanda, Irlanda, Portugalia, Republica Cehă, Slovenia, Croația, Bosnia) au analizat politica de înregistrare și, ca urmare a proceselor de consultare, au respins impunerea unei obligații generale de înregistrare.	**Nu se acceptă.** Practica internațională invocată este neuniformă, iar enumerarea selectivă din studiul GSMA nu reflectă realitatea normativă actuală, unele state menționate ca respingând măsura (precum Suedia sau Croația) având de fapt deja implementată identificarea obligatorie. La nivelul Uniunii Europene, deși nu există o obligație generală armonizată, identificarea utilizatorilor preplătiți reprezintă standardul majoritar de securitate, fiind aplicată de 16 din cele 27 de state membre, care acoperă aproximativ 82% din populația UE. Prin urmare, decizia Republicii Moldova nu se poate baza pe exemple selective care

			mențin un vid de securitate, ci trebuie fundamentată pe evaluarea propriilor riscuri și pe alinierea la bunele practici internaționale pentru a preveni transformarea teritoriului național într-o sursă de „turism SIM” exploatată de rețelele transfrontaliere.
	7.	• Riscul limitării eficientei în situații de terorism: Țări europene în care s-au implementat astfel de măsuri (ex.: Franța, Germania, Spania, Belgia) s-au confruntat cu atacuri teroriste care nu au fost prevenite prin existența reglementării respective.	**Nu se acceptă.** Măsurile de securitate publică nu se evaluează prin criteriul nerealist de „zero incidente” sau prin garanția unei preveniri absolute a oricărui atac terorist. Obligația de identificare nu promite prevenirea în totalitate terorismului, ci reprezintă o măsură de reducere a riscurilor și un instrument esențial de sprijin pentru investigații (permite atribuirea certă a identității, reconstruirea rețelelor de comunicații și identificarea complicilor). Faptul că măsura nu poate preveni fiecare incident în parte nu îi anulează utilitatea operațională în destructurarea logisticii infracționale și în reducerea masivă a altor fenomene asociate, cum ar fi alertele false cu bombă, care au scăzut cu 93-95% în state care au implementat această reglementare, precum Polonia.
	8.	• Poziția instituțiilor UE: Comisia Europeană a refuzat să dea curs solicitărilor unor state membre privind impunerea înregistrării utilizatorilor cartelelor preplătite la nivel comunitar, constatând că eficiența măsurii la nivel național nu este dovedită, fapt pentru care nu s-a justificat o acțiune la nivelul UE[2].	**Nu se acceptă.** Referința la decizia Comisiei Europene de a nu reglementa acest domeniu (Raportul din 2011) este depășită de contextul actual. În realitate, poziția instituțiilor europene s-a modificat odată cu evoluția amenințărilor: prin Comunicarea COM(2016) 50, Comisia a recunoscut explicit că anonimatul instrumentelor preplătite reprezintă o vulnerabilitate de securitate. Faptul că obligația nu este impusă printr-un regulament unic la nivel comunitar nu demonstrează ineficiența ei, ci reflectă respectarea competenței naționale: Directiva (UE) 2018/1972 (Codul european al comunicațiilor electronice) stipulează expres că statele membre sunt libere să ia măsuri de restricționare a anonimatului pentru a asigura ordinea și siguranța publică. Mai mult, la nivelul Consiliului UE, prin documentul recent al Președinției Poloneze (ST-5556-2025-INIT), lipsa înregistrării unitare a cartelelor SIM a fost catalogată oficial drept o amenințare la adresa securității, generând un fenomen de „arbitraj infracțional” transfrontalier. Din acest motiv, necesitatea și legitimitatea măsurii la nivel național sunt incontestabile, fiind deja aplicată ca standard de securitate de 16 din cele 27 de state membre ale UE.

[2] Raportul Comisiei Europene COM(2011) 225 final din 18.04.2011 — https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=COM:2011:0225:FIN.

	9.	• Alternative: Există și metode mai puțin intruzive care pot contribui la atingerea acelorași scopuri în domeniul prevenirii și combaterii infracționalității.	**Nu se acceptă.** Măsurile alternative invocate (precum sistemele anti-fraudă, măsurile anti-spoofing, investigațiile digitale sau cooperarea cu platformele OTT) sunt instrumente complementare, nu substitutive, deoarece acestea nu înlătură vulnerabilitatea de bază: accesul direct la numere naționale preplătite sub o identitate neasumată. Menținerea status quo-ului și bazarea exclusiv pe alternative nu oferă un nivel adecvat de prevenție și nici un cadru predictibil pentru atribuirea identității în investigații.
	10.	**Costuri economice și sociale ale măsurii** Impact asupra incluziunii digitale și sociale: Introducerea înregistrării obligatorii va afecta în mod disproporționat utilizatorii de cartele preplătite, categoria incluzând în special persoane cu venituri mici, persoane în vârstă, tineri și șomeri; mulți locuiesc în mediul rural, unde punctele de vânzare pot lipsi.	**Nu se acceptă.** Proiectul nu introduce un mecanism restrictiv de acces la comunicații și previne în mod activ riscul excluziunii sociale sau digitale. Pentru a nu afecta categoriile vulnerabile (persoane în vârstă, cu venituri mici) și cetățenii din mediul rural, inițiativa a adoptat modelul „Digital First” (Opțiunea D), care decuplează comercializarea de activare. Astfel, cartelele preplătite vor putea fi cumpărate în continuare liber, ca produse neactivate, din orice punct de vânzare nespecializat existent (chioșcuri, magazine sătești, oficii poștale), fără nicio barieră birocratică la cumpărare. Procesul de identificare se va realiza exclusiv la momentul activării, oferindu-se metode flexibile și minim intruzive: la distanță (prin mijloace digitale, eKYC, identitate electronică) sau fizic, la punctele împuternicite ale operatorului, nefiind obligatorie deplasarea cetățenilor la un centru raional. Mai mult, legea nu are efect retroactiv se va aplica strict cartelelor noi (activate după intrarea în vigoare a legii), protejând astfel baza actuală de peste 1,59 milioane de utilizatori preplătiți existenți. Prin urmare, dreptul și accesul tuturor cetățenilor la serviciile de comunicații mobile rămân garantate, măsura fiind pe deplin proporțională.
	11.	• Barieră acces: Pentru utilizatorii din mediul rural, impunerea deplasărilor la centre raionale pentru înregistrare creează obstacole practice — unii nu se pot deplasa din motive de sănătate, vârstă sau lipsă de resurse. În plus, o parte semnificativă a persoanelor nu dețin acte de identitate valabile; GSMA indică că aproximativ 17% din locuitorii unor țări comparabile nu dispuneau de act de identitate valabil.	**Nu se acceptă.** Premisa conform căreia cetățenii din mediul rural vor fi obligați să se deplaseze la centrele raionale este eronată și nu derivă din textul proiectului. Adoptând modelul „Digital First” (Opțiunea D), legea flexibilizează procesul, permițând identificarea la distanță prin mijloace digitale și electronice, precum și identificarea fizică prin rețeaua de puncte de vânzare ale partenerilor împuterniciți, asigurând astfel o acoperire teritorială vastă, fără dependență exclusivă de magazinele proprii ale operatorilor.

			Referitor la persoanele fără acte valabile, regimul de securitate și ordine publică al comunicațiilor nu poate fi fundamentat pe menținerea anonimatului drept soluție la problema neidentificării populației. Proiectul oferă flexibilitate prin acceptarea diverselor documente (inclusiv acte emise de alte state), iar cazurile izolate de acte expirate trebuie rezolvate prin proceduri administrative standard de actualizare a documentelor, nu prin renunțarea la o măsură sistemică de securitate.
	12.	• Costuri logistice pentru operatori: Implementarea obligației ar necesita cheltuieli substanțiale pentru asigurarea logisticii procesului de înregistrare (echiparea punctelor de vânzare, procese operaționale, instruirea personalului etc.). Aceste costuri pot conduce la majorări ale tarifelor sau la reducerea disponibilității cartelelor preplătite.	**Nu se acceptă.** Costurile logistice invocate au fost deja luate în calcul prin structura proiectului, care a adoptat modelul „Digital First" (Opțiunea D). Prin decuplarea procesului de comercializare de cel de activare, se elimină complet necesitatea echipării tehnice și a instruirii personalului în cele peste 3.700 de puncte de vânzare nespecializate (chioșcuri, oficii poștale, stații PECO). Identificarea se va realiza preponderent prin mijloace digitale la distanță (eKYC, identitate electronică), ceea ce reduce drastic costurile operaționale de front-office și scade repetitivitatea înregistrărilor prin posibilitatea reutilizării datelor deja verificate de operator. Deși implementarea necesită investiții inițiale (CAPEX) pentru adaptarea sistemelor IT și de facturare (Billing/CRM) – estimate, conform datelor agregate furnizate de operatori, între 3,0 și 6,8 milioane MDL – aceste costuri sunt perfect gestionabile și justificate de interesul securității naționale.
	13.	• Efecte asupra distribuirii și accesului: Costurile ridicate și cererea redusă pot determina distribuitorii să renunțe la comercializarea cartelelor în multe localități rurale, reducând accesul populației la serviciile mobile.	**Nu se acceptă.** Afirmația potrivit căreia distribuitorii vor renunța la comercializare este incorectă, deoarece proiectul nu condiționează vânzarea cartelelor de existența infrastructurii de identificare la fața locului. Prin adoptarea versiunii agreate, legea decuplează în mod intenționat comercializarea de activare. Astfel, cartelele preplătite vor fi vândute în continuare liber, ca produse neactivate, scutind cei peste 3.700 de comercianți terți (inclusiv magazinele și oficiile poștale din mediul rural) de orice procedură birocratică, instruire sau costuri logistice suplimentare.
	14.	• Impact asupra investițiilor în rețea: Reducerea cererii pe piața rurală poate face nerentabile investițiile în dezvoltarea rețelelor în aceste zone, afectând progresul obiectivelor asumate prin Strategia de Transformare Digitală 2023–2030 și serviciul universal.	**Nu se acceptă.** Afirmația privind scăderea rentabilității investițiilor rurale este pur ipotetică și nu derivă din arhitectura proiectului. Dimpotrivă, prin implementarea modelului, inițiativa stimulează în mod direct migrarea populației către instrumente și procese digitale (identificare electronică și la distanță), fiind pe deplin unită cu obiectivele Strategiei de Transformare Digitală.

	15.	• Consecințe sociale: În final, un astfel de regim ar putea conduce la scăderea accesului la comunicații, amplificarea excluziunii sociale și scăderea standardelor de trai pentru segmente vulnerabile ale populației. Având în vedere: (i) lipsa dovezilor empirice care să susțină eficiența măsurii în reducerea criminalității; (ii) posibilitatea de ocolire a obligației prin utilizarea cartelor emise în alte jurisdicții sau cele înregistrate pe terți; (iii) deciziile și recomandările instituțiilor și statelor menționate; și (iv) costurile economice și sociale semnificative și riscul creșterii excluziunii digitale, considerăm că impunerea unei obligații generale de înregistrare a utilizatorilor cartelelor preplătite reprezintă un răspuns disproporționat la riscurile urmărite. În lumina celor de mai sus, solicităm ca inițiativa să fie reevaluată și, în absența unor dovezi clare privind eficiența sa, să nu i se dea curs. În același timp, recomandăm explorarea unor alternative mai puțin intruzive, cu un raport cost/beneficiu favorabil și cu impact minim asupra incluziunii digitale.	**Nu se acceptă.** Proiectul este calibrat pe principiul proporționalității, scopul său nefiind restrângerea accesului legitim la comunicații, ci eliminarea vulnerabilității fundamentale, accesul facil la numere naționale anonime. Riscul excluziunii sociale este prevenit direct prin aplicarea legii exclusiv pentru activările noi (protejând utilizatorii existenți), prin stabilirea unei perioade de tranziție de 12 luni și prin diversificarea canalelor de identificare (la distanță, online sau prin puncte împuternicite), asigurând accesul facil inclusiv pentru persoanele din mediul rural sau cu mobilitate redusă. Măsurile alternative propuse sunt doar complementare și nu pot substitui trasabilitatea necesară, iar menținerea status quo-ului nu oferă un nivel adecvat de prevenție pentru securitatea publică, motiv pentru care renunțarea la inițiativă nu este justificată.
CONSULTARE PUBLICĂ			
AGENȚIA NAȚIONALĂ PENTRU REGLEMENTARE ÎN COMUNICAȚII (Aviz nr.01-DRA/474 din 13 martie 2026)	1.	1. Pe întreg cuprinsul proiectului: 1) Cuvântul „abonat„ la orice formă gramaticală de substituit cu cuvântul „utilizator” la forma gramaticală corespunzătoare. Notă: Conform art. 2 pct. 1 din Legea comunicațiilor electronice nr. 72/2025, în continuare Legea nr. 72/2025, noțiunea de „abonat” semnifică „orice persoană fizică sau juridică care a încheiat un contract cu furnizorul de servicii de comunicații electronice accesibile publicului în vederea furnizării unor astfel de servicii”. Respectiv, toți abonații deja sunt identificați de către furnizori. Noțiunea de „utilizator”, conform pct. 93 art. 2 din Legea nr. 72/2025, semnifică „persoană fizică sau juridică ce utilizează sau solicită utilizarea unui serviciu de comunicații electronice accesibil publicului”.	**Se acceptă.**

	2.	La art. I, alin. (4) de expus în următoarea redacție: „(4) Furnizarea serviciilor de comunicații electronice, astfel încât să fie posibilă originarea sau terminarea apelurilor, prin intermediul unui număr asignat cartelei SIM/eSIM (activarea cartelei) comercializate unui utilizator se realiza după identificarea utilizatorului numărului. Până la identificarea utilizatorului, cartela SIM/eSIM poate fi utilizată doar pentru serviciile tehnice minime necesare stabilite de autoritatea de reglementare, dacă este fezabil. Notă: Modificarea dat are scopul clarificării prevederilor alin. (4).	**Se acceptă parțial.** Formularea propusă contravine direct art. 54 alin. (1) lit. a) din Legea nr. 100/2017 cu privire la actele normative. Norma trebuie să aibă un caracter strict dispozitiv, clar și concis. Detalierile tehnice excesive („*astfel încât să fie posibilă originarea sau terminarea apelurilor*”) și explicațiile introduse în paranteze „(*activarea cartelei*)” sunt inadmisibile în textul unei legi organice. Obiectivul vizat de autorul obiecției este deja acoperit integral în redacția finală: Este instituită imperativ la noul art. 125^1 alin. (1), care obligă identificarea „*cel târziu la momentul activării acestora*”. Este formulată exact la alin. (4) din proiectul agreat: „*Până la finalizarea procesului de identificare, cartelele SIM/eSIM pot fi utilizate doar pentru serviciile tehnice minime necesare, care urmează a fi stabilite de autoritatea de reglementare*”.
BIROUL POLITICI DE REINTEGRARE (Aviz nr. 04-78-1188 din 17 martie 2026)	1.	Ca urmare a examinării proiectului de lege pentru modificarea Legii nr.72/2025 comunicațiilor electronice (număr unic 196/MAI/2026), în limitele competențelor instituționale, comunicăm lipsa de obiecții și propuneri.	**Se acceptă.**
AGENȚIA SERVICII PUBLICE A REPUBLICII MOLDOVA (Aviz nr. 01/2266 din 16 martie 2026)	1.	Ca urmare a examinării proiectului de lege pentru modificarea Legii nr.72/2025 comunicațiilor electronice (număr unic 196/MAI/2026), comunicăm următoarele. La conținutul Articolului 125^1 propus pentru completarea Legii nr. 72/2025: 1. alin (2) pct. 1) – se propune substituirea sintagmei „interogarea gratuită a Sistemului informațional automatizat „Registrul de stat al populației”, în condițiile legii” prin sintagma „interogarea Sistemului informațional „Registrul de stat al populației”, prin intermediul platformei de interoperabilitate MConnect, în condițiile Legii nr.142/2018 cu privire la schimbul de date și interoperabilitate”.	**Se acceptă.**

	2.	2. alin (2) pct. 3) – se propune substituirea sintagmei „interogarea gratuită a Sistemului informațional „Registrul de stat al unităților de drept”, în condițiile legii” prin sintagma „interogarea Sistemului informațional „Registrul de stat al unităților de drept”, prin intermediul platformei de interoperabilitate MConnect, în condițiile Legii nr.142/2018 cu privire la schimbul de date și interoperabilitate”.	**Se acceptă.**
	3.	3. alin (3) pct. 3) lit. b) – se propune substituirea sintagmei „preluate gratuit din Sistemul informațional automatizat „Registrul de stat al populației”, utilizând mijloace digitale” prin sintagma „preluate din Sistemul informațional „Registrul de stat al populației”, prin intermediul platformei de interoperabilitate MConnect în condițiile Legii nr.142/2018 cu privire la schimbul de date și interoperabilitate”. Propunerile formulate sunt în concordanță cu cadrul normativ în vigoare privind schimbul de date și interoperabilitate, în special cu prevederile Legii nr.142/2018 cu privire la schimbul de date și interoperabilitate și Hotărârea Guvernului nr.211/2019 privind platforma de interoperabilitate MConnect. Astfel, potrivit art. 4 și art. 6 din Legea nr. 142/2018, în partea ce ține de „gratuitatea datelor” furnizate către participanții privați, se stabilește că punerea la Nr. 01/2266 din 16.03.2026 La nr. DGPSG-2055-18-69-841 din 11.03.2026 dispoziție a datelor deținute de participanții publici poate fi realizată cu titlu oneros în cazurile prevăzute de legislația în vigoare și conform mecanismului stabilit de Guvern. Totodată, schimbul de date cu participanții privați se realizează, exclusiv prin intermediul platformei de interoperabilitate. Contractul de schimb de date se încheie cu titlu oneros între deținătorul platformei de interoperabilitate și participantul privat, în modul și condițiile stabilite de Guvern.	**Se acceptă.**
CENTRUL NAȚIONAL PENTRU PROTECȚIA DATELOR CU	1.	Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova a examinat proiectul de lege pentru modificarea Legii comunicațiilor electronice nr. 72/2025 (număr unic 196/MAI/2026) și comunică următoarele:	**Se acceptă parțial.** Proiectul de lege este pe deplin aliniat la principiile de prelucrare a datelor cu caracter personal reglementate de Legea nr. 133/2011 (care urmează a fi abrogată la 23.08.2026), urmând ca în continuare

CARACTER PERSONAL (Aviz nr. 04-01/1001 din 19 martie 2026)		Proiectul de act normativ implică prelucrarea datelor cu caracter personal, întrucât instituie obligații puse în sarcina furnizorilor de servicii de comunicații electronice mobile accesibile publicului privind identificarea abonaților, precum și colectarea, verificarea, stocarea și păstrarea datelor de identificare ale acestora. În acest context, se impune asigurarea respectării principiilor fundamentale de prelucrare a datelor cu caracter personal, respectiv legalitatea, echitatea și transparența, limitarea scopului, minimizarea datelor, exactitatea, limitarea perioadei de stocare, integritatea și confidențialitatea. Totodată, este necesară instituirea unor garanții adecvate privind securitatea prelucrării datelor, inclusiv implementarea unor măsuri tehnice și organizatorice corespunzătoare, menite să prevină accesul neautorizat, pierderea, distrugerea sau divulgarea datelor. În acest sens, furnizorii urmează să adopte proceduri interne clare privind gestionarea datelor cu caracter personal și să asigure trasabilitatea operațiunilor de prelucrare.	aplicarea normelor să se raporteze direct la rigorile noii Legi nr. 195/2024 și ale Regulamentului (UE) 2016/679 (RGPD). Proiectul implementează direct principiul minimizării datelor, instituind o listă strictă și exhaustivă a datelor colectate la noul art. 125^1 alin. (2). Principiul limitării stocării este garantat prin art. 125^1 alin. (5), care restrânge retenția datelor strict pe durata utilizării și 12 luni de la încetarea utilizării numărului. Colectarea și stocarea datelor de identitate nu reprezintă o prelucrare nouă pentru operatori, procedurile fiind deja funcționale pentru abonații cu contract (postplătit). În calitatea lor de operatori de date, furnizorilor le revine obligația legală directă și imperativă (conform Legii nr. 195/2024) de a implementa măsurile tehnice și organizatorice pentru securitatea și trasabilitatea datelor colectate, fără a fi necesară dublarea acestor obligații orizontale în legea sectorială.
	2.	Redacția actuală a prevederii aferente art. 125^1 alin. (2) pct. (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, nu stabilește în mod clar dacă verificarea datelor personale și valabilității actului de identitate prin interogarea Sistemului informațional automatizat „Registrul de stat al populației” se realizează în toate cazurile sau doar în anumite situații. Or, lipsa unei astfel de precizări contravine exigențelor de claritate și previzibilitate a normei juridice, susceptibile de a genera interpretări divergente în procesul de aplicare. Mai mult, norma nu precizează în mod expres subiectul responsabil de efectuarea verificărilor în Sistemul informațional automatizat „Registrul de stat al populației”, respectiv dacă această obligație revine exclusiv furnizorului sau poate fi realizată și de către persoane împuternicite de acesta-punctele de vânzare.	**Nu se acceptă.** Conform art. 54 alin. (1) lit. a) din Legea nr. 100/2017 cu privire la actele normative, textul se expune clar și concis. O normă redactată la timpul prezent („*furnizorul verifică* ”) instituie o obligație imperativă, generală și permanentă. Adăugarea sintagmei „în toate cazurile” constituie o tautologie juridică ce încarcă inutil textul legii. Norma se interpretează, în coroborare cu întregul articol 125^1. Responsabilitatea legală este atribuită exclusiv furnizorilor, conform alin. (1). Concomitent, delegarea operațională a procesului de identificare (care include interogarea datelor) este reglementată exhaustiv la alin. (3) pct. 2), care permite expres identificarea „ *în punctele de vânzare ale persoanelor împuternicite de furnizor* ”. Repetarea acestui mecanism de delegare la alin. (2) este redundantă și contrară tehnicii legislative.

	3.	Cu titlu separat se va nota, că „Registrul de stat al populației” este un sistem unic integrat de evidență automatizată a cetățenilor Republicii Moldova, străinilor cu drept de ședere permanentă sau provizorie pe teritoriul Republicii Moldova, a refugiaților și a beneficiarilor de protecție umanitară, precum și a cetățenilor plecați peste hotare pentru a se stabili cu traiul permanent sau temporar pe o durată mai mare de trei luni. Având în vedere caracterul complex și volumul semnificativ de date cu caracter personal conținute în „Registrul de stat al populației”, oferirea accesului la acest sistem implică riscuri ridicate pentru drepturile și libertățile persoanelor vizate. În acest context, orice acces trebuie acordat cu maximă prudență, în baza unui temei legal clar, limitat strict la necesitatea realizării unui scop determinat și însoțit de garanții adecvate de securitate și control, pentru a preveni utilizarea abuzivă sau divulgarea neautorizată a datelor.	**Se acceptă.** **Precizare.** Noul art. 125[1] din Legea nr. 72/2025 constituie norma primară care mandatează schimbul de date, interogarea fiind strict limitată la un scop determinat: validarea identității la activarea serviciului. În conformitate cu Legea nr. 195/2024, se interoghează un set exhaustiv, strict și închis de informații (nume, prenume, IDNP, datele actului de identitate). Operatorii nu au acces direct și necontrolat la Registrul de stat. Schimbul de date se realizează exclusiv prin platforma guvernamentală MConnect (în condițiile Legii nr. 142/2018 și HG nr. 211/2019), infrastructură care asigură implicit criptarea, controlul accesului și jurnalizarea obligatorie a fiecărei interpelări. Furnizorii rămân operatori de date cu drepturi și obligații depline conform Legii nr. 195/2024, purtând răspunderea directă pentru implementarea măsurilor tehnice, organizatorice și de audit intern menite să prevină accesul abuziv sau divulgarea neautorizată a datelor preluate.
	4.	Cu referire la dispoziția „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” menționăm că, Legea privind protecția datelor cu caracter personal nu reglementează în mod expres condițiile în care poate fi reținută copia actului de identitate, ordine în care considerăm necesar excluderea referinței la legea vizată. Prin urmare, operatorul, fie autoritatea de reglementare este responsabil/ă de stabilirea condițiilor concrete în care poate fi reținută copia actului de identitate, a scopului prelucrării și a necesității acestei operațiuni. În alt context, în măsura în care sunt utilizate mijloace digitale de identificare ce implică tehnologii biometrice sau procese decizionale automatizate, se recomandă efectuarea unei evaluări a impactului asupra protecției datelor, în conformitate cu cadrul normativ aplicabil.	**Se acceptă parțial.** Reținerea copiei actului de identitate pentru cetățenii străini a fost agreată ca necesitate operațională în urma consultărilor cu ATIC. Menținerea sintagmei „ în condițiile legislației privind protecția datelor cu caracter personal ” este imperativă pentru a institui o garanție legală fermă. Aceasta obligă direct operatorul să aplice standardele de securitate, confidențialitate și limitare a stocării prevăzute de Legea nr. 195/2024, excluderea acestei referințe generând un vid de garanții. Obligația de a efectua DPIA în cazul utilizării noilor tehnologii (mijloace digitale, biometrice) derivă imperativ și direct din normele generale privind protecția datelor (art. 23 din Legea nr. 133/2011 și prevederile corespunzătoare din Legea nr. 195/2024). Conform normelor de tehnică legislativă (art. 54 din Legea nr. 100/2017), dublarea și repetarea dispozițiilor cadrului orizontal în legile sectoriale este inadmisibilă. Operatorii, în calitatea lor de operatori de date, sunt direct și nemijlocit responsabili de executarea acestei evaluări prealabile, fără a fi necesară o reglementare specială dublată în prezenta lege.
	5.	Cu titlu informativ, se reiterează că, potrivit art. 23–25 din Legea nr. 133/2011 privind protecția datelor cu caracter personal, operatorii au obligația de a efectua evaluarea	**Se acceptă.** Cerința evaluării prealabile în contextul adoptării actului normativ este deja îndeplinită. Nota de fundamentare (secțiunea 4.4.1) conține

		impactului asupra protecției datelor în situațiile în care prelucrarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, precum și obligația de a desemna o persoană responsabilă cu protecția datelor, în condițiile legii. Astfel, în conformitate cu art. 23 alin. (6) din Legea nr. 133/2011, în cazul în care tipurile de prelucrare reglementate prin proiectul de act normativ sunt susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, inclusiv prin raportare la prelucrarea datelor la scară largă, se impune realizarea evaluării impactului asupra protecției datelor în contextul adoptării actului normativ respectiv.	o evaluare exhaustivă a impactului asupra datelor cu caracter personal. Documentul demonstrează riguros temeiul legal, scopul legitim de securitate publică, proporționalitatea ingerinței, precum și respectarea strictă a principiului minimizării datelor și limitării stocării la 12 luni. Din perspectiva implementării practice a soluțiilor de identificare la distanță (eKYC, biometrie), obligația de a efectua Evaluarea Impactului asupra Protecției Datelor (DPIA) și de a desemna un responsabil cu protecția datelor datelor cu caracter personal revine exclusiv furnizorilor de servicii de comunicații electronice. Această sarcină derivă imperativ și direct din art. 23-25 ale Legii nr. 133/2011 (care urmează a fi abrogată la 23.08.2026) și, pe viitor, din dispozițiile corespunzătoare ale noii Legi nr. 195/2024. Operatorii de comunicații aplică aceste norme în mod direct, fiind responsabili de evaluarea riscurilor și de consultarea prealabilă a CNPDCP.
SERVICIUL DE INFORMAȚII ȘI SECURITATE (Aviz nr. IE/2879 din 25.03.2026)	1.	Ca urmare a examinării proiectului de lege pentru modificarea Legii nr.72/2025 comunicațiilor electronice (număr unic 196/MAI/2026), în limitele competenței funcționale, comunicăm lipsa de obiecții și propuneri.	**Se acceptă.**
MINISTERUL DEZVOLTĂRII ECONOMICE ȘI DIGITALIZĂRII AL REPUBLICII MOLDOVA (Aviz nr. 14-966 din 19.03.2026)	1.	Ministerul Dezvoltării Economice și Digitalizării a examinat proiectul de lege pentru modificarea Legii nr. 72/2025 comunicațiilor electronice (număr unic 196/MAI/2026), și în limita competențelor funcționale comunică următoarele. **Considerații de ordin general** 1) În anul 2025, prin adoptarea Legii comunicațiilor electronice nr. 72/2025, Republica Moldova a transpus Codul european al comunicațiilor electronice și 12 acte juridice ale Uniunii Europene relevante în domeniu, asigurând alinierea substanțială a cadrului normativ național la acquis-ul european în domeniul comunicațiilor electronice. Noua reglementare instituie un cadru juridic modern, coerent și competitiv pentru dezvoltarea rețelelor și serviciilor de comunicații electronice, creând premisele necesare pentru stimularea investițiilor, consolidarea concurenței și protecția utilizatorilor finali.	**Se acceptă parțial.** Instituirea noului art. 125^1 nu contravine Directivei (UE) 2018/1972 (Codul european al comunicațiilor electronice). Conform art. 1 alin. (3) lit. c) și Considerentului (6) din Directivă, normele europene nu aduc atingere acțiunilor și dreptului suveran al statelor membre de a adopta măsuri pentru asigurarea ordinii publice, siguranței publice și investigarea infracțiunilor. Mecanismele de acces la date ale organelor de drept (reglementate deja la art. 125) sunt ineficiente în lipsa unor date reale. Noul art. 125^1 completează acest vid de securitate printr-o măsură de identificarea prealabilă la activare. În urma ședinței interinstituționale din 08.12.2025, MDED a confirmat oficial (prin comunicarea din 19.12.2025) că modelul ales în proiect reprezintă *„cea mai optimă din perspectiva implementării ar fi Opțiunea D – Digital First”*, validând astfel proporționalitatea măsurii în raport cu obiectivele pieței unice.

		Totodată, legea stabilește baza normativă necesară pentru transpunerea și implementarea ulterioară a cadrului european aferent integrării Republicii Moldova în zona de „Roaming la tarife naționale” (Roam Like At Home) și pentru facilitarea integrării în piața unică digitală a Uniunii Europene. Ținem să menționăm că, anterior adoptării în plenul Parlamentului a noii Legi a comunicațiilor electronice, proiectul acesteia a fost supus unui proces de expertizare de către experții DG CONNECT din cadrul Comisiei Europene, care au confirmat compatibilitatea deplină a proiectului de lege cu cadrul juridic al Uniunii Europene în domeniul comunicațiilor electronice. În procesul de elaborare a proiectului de lege a fost constituit un grup de lucru interinstituțional, la care au participat și reprezentanți ai MAI. Cu suportul acestora și al Serviciului de Informații și Securitate, a fost definitivate mai multe articole esențiale din lege, inclusiv Articolul 125 - Regimul juridic al accesului autorităților competente la datele utilizatorilor de servicii de comunicații electronice și la comunicațiile acestora.	
	2.	2) Conform raportului Agenției Naționale pentru Reglementare în Comunicații (ARCOM) - Evoluția pieței de comunicații electronice în trimestrul III/2025, numărul utilizatorilor de cartele SIM prepaid (PrePay) în rețelele furnizorilor de comunicații electronice mobile din Republica Moldova este de circa 1,69 milioane, ce constituie 46,7% din numărul total de cartele SIM active la utilizatori. Aceste cartele sunt utilizate pentru servicii de voce sau Internet dedicat. Potrivit studiului „Access to Mobile Services and Proof of Identity 2021 elaborat de GSMA, la nivel mondial, cartelele SIM PrePay reprezintă aproximativ 72% din totalul conexiunilor mobile, ceea ce reflectă rolul esențial al acestora în extinderea accesului la servicii de comunicații mobile și în adoptarea pe scară largă a tehnologiilor mobile.	**Nu se acceptă.** Conform art. II din proiect, obligația de identificare se aplică exclusiv pe viitor (numerelor activate după intrarea în vigoare a legii). Baza curentă de aproximativ 1,6 milioane de utilizatori preplătiți nu este afectată, eliminând riscul deconectărilor în masă. Accesul fizic la cartele rămâne neschimbat și nerestricționat. Conform noului art. 125^1, cartelele preplătite se comercializează în continuare ca produse neactivate prin orice punct de vânzare (inclusiv chioșcuri și rețele terțe), fără obligația prezentării actului de identitate la momentul cumpărării. Pentru a preveni barierele de acces în zonele rurale sau pentru persoanele cu mobilitate redusă, art. 125^1 permite expres efectuarea identificării la distanță (prin mijloace de identificare electronică sau proceduri eKYC), garantând un proces de activare rapid, 100% digitalizat.
	3.	3) În același timp, cu referire la practica europeană, se constată că la nivelul Uniunii Europene nu există o reglementare armonizată privind identificarea obligatorie a utilizatorilor de cartele preplătite, acest domeniu fiind lăsat în	**Se acceptă parțial.** Referința la Raportul Comisiei din 2011 este depășită. Prin Comunicarea COM(2016)50 și, recent, prin documentul Consiliului UE (ST-5556-2025-INIT, elaborat de Președinția Poloneză),

		competența statelor membre, în aplicarea principiului subsidiarității. Practicile naționale sunt divergente, iar lipsa unei intervenții legislative la nivelul Uniunii reflectă absența unui consens privind necesitatea și eficacitatea unor asemenea măsuri. Totodată, la nivel european nu au fost prezentate dovezi empirice concludente care să demonstreze că obligativitatea identificării utilizatorilor de cartele preplătite contribuie efectiv la prevenirea sau combaterea criminalității. În acest sens, Comisia Europeană a constatat că eficacitatea acestor măsuri nu a fost dovedită și nu a identificat necesitatea unei intervenții legislative la nivelul Uniunii (Raportul Comisiei Europene COM(2011) 225 final). În aceste condiții, instituirea unor astfel de obligații trebuie analizată cu prudență, inclusiv din perspectiva proporționalității și a impactului asupra drepturilor fundamentale, în lipsa unor beneficii demonstrate. De exemplu, în anul 2014, Curtea Constituțională a României a declarat neconstituțională legea privind înregistrarea cartelelor preplătite, reținând că obligația de identificare a utilizatorilor nu era însoțită de garanții suficiente privind protecția datelor cu caracter personal și putea conduce la ingerințe nejustificate în drepturile fundamentale ale cetățenilor.	anonimatul cartelelor preplătite este catalogat drept o amenințare reală ce generează un „*arbitraj infracțional*” transfrontalier. În prezent, 16 din 27 de state membre UE (aprox. 82% din populația Uniunii) impun identificarea obligatorie. Legalitatea măsurii a fost tranșată definitiv de instanțele europene în favoarea securității statului. Curtea Europeană a Drepturilor Omului (cauza *Breyer c. Germaniei*, 2020) a decis clar că identificarea obligatorie a cartelelor SIM preplătite reprezintă o ingerință „limitată” și pe deplin proporțională, care NU încalcă dreptul la viață privată. Concomitent, Curtea de Justiție a UE (cauza *Ministerio Fiscal,* 2018) a statuat că accesul autorităților exclusiv la datele de identitate a persoanelor nu constituie o imixtiune „gravă”. Decizia Curții Constituționale a României (nr. 440/2014) a sancționat cu totul o altă arhitectură legală: aplicarea retroactivă și colectarea fizică, nesecurizată a datelor prin mii de comercianți nespecializați. Arhitectura proiectului Republicii Moldova elimină exact aceste neconcordanțe: măsura nu are efectul retroactiv și desparte comercializarea de activare, fiind identificarea în mediul digital securizat. Afirmația privind lipsa dovezilor este infirmată de Raportul de expertiză care a stat la baza proiectului. De exemplu, după introducerea obligativității în Polonia (2016), volumul alertelor false cu bombă a scăzut drastic cu 93-95% (de la cca. 4.000 la 200 anual), iar rata de depistare și reținere a făptuitorilor s-a dublat, crescând de la 30% la aproximativ 70%.
	4.	4) Ineficiența măsurilor de identificare a utilizatorilor cartelelor preplătite a fost recunoscută și de Dl Heinz KIEFER, președintele Confederației Europene a Poliției (EuroCop), care a declarat public, că criminalii și teroriștii pot evita această măsură de protecție prin metode relativ simple. Ca rezultat, va fi făcut un efort enorm, dar cu efect neînsemnat asupra infractorilor și teroriștilor. Astfel, asemenea activități restrictive nu sunt capabile să sporească încrederea cetățenilor în capacitatea autorităților de a asigura un grad înalt de protecție împotriva crimelor serioase și terorismului.	**Nu se acceptă.** Obiecția se fundamentează pe o opinie izolată, contrară poziției oficiale actuale a instituțiilor UE. Europol și Consiliul UE (Documentul Președinției Poloneze ST-5556-2025-INIT) definesc explicit anonimatul cartelelor SIM drept o vulnerabilitate critică ce generează un „arbitraj infracțional” transfrontalier, solicitând imperativ consolidarea procedurilor de identificare (KYC) în telecomunicații. Afirmația privind „efectul neînsemnat” este infirmată de datele din Raportul de expertiză care a stat la baza proiectului. În Polonia, implementarea măsurii a determinat o reducere drastică de 93-95% a alertelor false cu bombă și a dublat rata de identificare și reținere a făptuitorilor (de la 30-40% la 60-70%). Politicile de securitate publică se evaluează prin diminuarea vulnerabilităților sistemice, nu prin criteriul „zero incidente”; chiar dacă infractorii recurg la eludări

			(aplicații OTT, roaming), măsura crește costul operațional și le reduce capacitățile logistice. Critica privind efortul birocratic disproporționat nu este aplicabilă arhitecturii proiectului național. Proiectul elimină caracterul birocratic deoarece se aplică exclusiv cartelelor noi, conform Art. II din proiect și decuplează complet procesul de vânzare de cel de identificare.
	5.	5) Remarcăm că obligația de înregistrare a cartelelor PrePay va fi ineficientă în procesul de contracarare a criminalității, deoarece este puțin probabil că pentru comiterea infracțiunilor, infractorii vor utiliza cartele preplătite înregistrate pe numele propriu. Este evident că aceștia pot utiliza: - cartele SIM furate, înregistrate pe numele unor persoane terțe; - cartele SIM înregistrate pe numele unor persoane terțe, fără știrea și permisiunea acestora (inclusiv pe bază de acte de identitate furate sau copii de acte de identitate utilizate neautorizat); - cartele SIM înregistrate pe numele unor persoane din păturile social vulnerabile, inclusiv contra plată (persoane în etate, persoane cu dizabilități, persoane fără domiciliu, persoane cu venituri scăzute, etc.); - cartele SIM emise de furnizori din alte state, în care nu este obligația de înregistrare a utilizatorilor și utilizate în roaming în Republica Moldova.	**Nu se acceptă.** Riscul înregistrării abuzive pe baza unor acte furate/copii este neutralizat de mecanismele noului art. 125[1]. Identificarea se realizează exclusiv prin instrumente sigure: eKYC cu verificarea biometrică a prezenței fizice, semnătură electronică calificată sau interogarea Registrelor de stat prin intermediul platformei de interoperabilitate MConnect. Astfel, preluarea neautorizată a identității, fără participarea directă fizică sau digitală a titularului, este blocată tehnic. Eficiența unei politici de securitate se măsoară prin diminuarea vulnerabilităților sistemice, nu prin eliminarea absolută. Utilizarea persoanelor terțe complică major logistica grupărilor criminale, crește considerabil costurile și lasă urme (trasabilitate relațională și financiară), oferind organelor de drept puncte clare de pornire a anchetelor. Utilizarea cartelelor străine anonime în roaming este o problemă recunoscută la nivel european, cauzată de lipsa armonizării. Cu toate acestea, menținerea vidului legislativ național nu reprezintă o soluție, ci transformă direct Republica Moldova într-o sursă furnizoare de cartele anonime pentru rețelele criminale regionale și spionaj. Reglementarea pieței interne este o măsură necesară și proporțională pentru protejarea ordinii publice.
	6.	6) Odată cu comercializarea în masă a terminalelor inteligente (smartphone, tablete, etc.) care au încorporate module Wi-Fi, au devenit foarte populare serviciile alternative de comunicații, bazate pe aplicațiile sau serviciile „de conținut”, denumite generic OTT (Over The Top - conținut, servicii sau aplicații furnizate în mediul online prin Internetul deschis, cum ar fi diferite tipuri de mesagerii, inclusiv cu voce/video). Exemple de aplicații OTT sunt aplicațiile pentru rețele sociale, pentru hărți, pentru mesagerie instantanee sau e-mail, comunicare audiovideo, etc. Astfel infractorii pentru comunicare pot utiliza aplicații alternative (Viber, WatsApp, Telegram, Skype, Messenger) prin intermediul rețelelor Wi-Fi	**Nu se acceptă.** Argumentul ignoră funcționarea tehnică a aplicațiilor OTT (WhatsApp, Telegram, Viber), care necesită obligatoriu un număr de telefon mobil valid pentru crearea și activarea contului. Cartelele preplătite anonime reprezintă exact instrumentul logistic de bază prin care infractorii generează aceste conturi netrasabile. Eliminarea anonimatului SIM blochează direct validarea conturilor OTT false (aspect confirmat în Raportul de expertiză). Existența unor metode alternative de comunicare (Wi-Fi public) nu justifică menținerea unui vid legislativ structural pe piața comunicațiilor naționale. Limitarea anonimatului forțează infractorii să recurgă la metode logistice mult mai complexe, costisitoare și riscante lăsând urme.

		publice sau private, ori utilizând alte echipamente moderne de radiocomunicații.	
	7.	7) Introducerea condiției de identificare a cartelelor PrePay va avea ca efect direct scăderea vânzărilor furnizorilor de comunicații mobile și în consecință contribuțiile acestora la bugetul statului, în special TVA. În condițiile actuale, când veniturile de la furnizarea serviciilor de telefonie mobilă înregistrează o scădere continuă pentru al treilea an consecutiv, impunerea unor obligații suplimentare furnizorilor de comunicații mobile poate avea un efect negativ considerabil asupra acestui segment al pieței comunicațiilor electronice, precum și asupra segmentelor conexe - acces la Internet în bandă largă și servicii TV cu plată prin intermediul rețelelor de comunicații electronice mobile. Pe lângă costurile iminente este necesară estimarea pierderilor generate de dezicerea unor utilizatori de serviciile furnizate prin intermediul cartelelor PrePay sau de limitarea accesului la procurarea cartelelor respective. Analiza preliminară a inițiativei denotă creșterea nejustificată a costurilor pentru furnizorii de comunicații mobile, creșterea prețurilor pentru utilizatorii finali, cât și pierderi substanțiale pentru bugetul de stat urmare a micșorării vânzărilor de servicii. Astfel, reglementarea va avea un efect negativ economic și social disproporțional, care va afecta industria TIC în Republica Moldova.	**Nu se acceptă.** Reglementarea produce efecte exclusiv pe viitor. Conform Art. II din proiect, noile reguli se aplică doar numerelor activate după intrarea în vigoare a legii. Baza curentă de ~1,6 milioane de clienți, care generează veniturile actuale, rămâne neafectată. Conform noului art. 125^1 alin. (3), comercializarea cartelelor preplătite în rețelele terțe de distribuție rămâne complet nerestricționată, acestea fiind vândute ca produse neactivate, fără solicitarea actelor de identitate la cumpărare. Astfel, se anulează riscul reducerii accesibilității și al scăderii vânzărilor. Costurile de conformare (estimate agregat la 3,0 - 6,8 mln. MDL) sunt justificate de interesul superior al securității naționale și atenuate prin termenul de tranziție extins de 12 luni. Practica europeană confirmă că, în implementarea normelor de securitate publică și combatere a terorismului, obiectivele de securitate națională primează imperativ în fața criteriilor de cost-eficiență comercială.
	8.	8) Introducerea unor norme cu astfel de efect economic și social major necesită elaborarea unui studiu de fundamentare/fezabilitate, care să prezinte costurile de conformare, riscurile și impactul cost/beneficiu și intervenției statului prin implementarea normei de reglementare.	**Se acceptă.** Impactul intervenției statului a fost evaluat exhaustiv în Capitolul 4 din Nota de fundamentare, în strictă conformitate cu rigorile Legii nr. 100/2017 și ale Metodologiei de analiză a impactului de reglementare. Documentul analizează opțiunile alternative și detaliază impactul asupra mediului de afaceri, a sectorului public și a societății. Costurile de conformare pentru sectorul privat au fost calculate în baza datelor furnizate de operatori. Conform Notei de fundamentare, investițiile inițiale necesare pentru adaptarea sistemelor de Billing/CRM și integrarea soluțiilor de identificare digitală (eKYC) sunt estimate, la nivel agregat, între 3,0 și 6,8 mln. MDL. Impactul operațional și financiar asupra operatorilor este diminuat direct prin instituirea perioadei de tranziție de 12 luni. Această perioadă este tehnic suficientă pentru a asigura planificarea bugetară, derularea procedurilor de achiziție și implementarea

			etapizată a noilor soluții digitale, fără a perturba activitatea comercială curentă a furnizorilor de comunicații.
	9.	Nota de fundamentare nu conține suficiente informații pentru a justifica oportunitatea intervenției și proporționalitatea soluțiilor propuse. Totodată, lipsește o analiză completă a impactului, care să demonstreze beneficiile măsurilor și capacitatea acestora de a atinge obiectivele urmărite, motiv pentru care documentul nu corespunde cerințelor Metodologiei de analiză a impactului de reglementare, aprobate prin Hotărârea Guvernului nr. 574/2024. Totodată, deși Nota de fundamentare face referire la existența unor practici în statele membre ale Uniunii Europene, aceste referințe sunt generale și nu sunt însoțite de o analiză concretă a modelelor de reglementare aplicate, a eficienței acestora sau de trimitere la acte normative relevante. În lipsa unor exemple detaliate și a indicării surselor verificabile (inclusiv acte normative sau politici publice), nu poate fi realizată o evaluare comparativă reală a soluției propuse, ceea ce afectează fundamentarea acesteia în sensul cerințelor Metodologiei AIR. Cu referire la pct. 4.2 „Impactul financiar și argumentarea costurilor estimative”, se constată că analiza prezentată este incompletă și nu corespunde cerințelor Metodologiei de analiză a impactului de reglementare, aprobate prin Hotărârea Guvernului nr. 574/2024. Astfel, Nota de fundamentare nu conține o estimare clară și fundamentată a costurilor necesare pentru implementarea măsurii de înregistrare a utilizatorilor de cartele preplătite, nefiind prezentate calcule detaliate, ipotezele utilizate sau sursele de date care au stat la baza estimărilor. În mod particular, nu este clar de unde provine estimarea costurilor în cuantum agregat de 3,0 - 6,8 mil. MDL, nefiind indicată metodologia de calcul și nici dacă aceasta se bazează pe surse externe, studii relevante sau pe informații furnizate de operatorii de comunicații electronice vizați de implementarea măsurii. În aceste condiții, se impune completarea substanțială a Notei de fundamentare, inclusiv prin clarificarea originii estimărilor, prezentarea calculelor detaliate și a ipotezelor	**Se acceptă parțial.** Nota de fundamentare va fi completată exhaustiv pentru a evidenția temeiul european al intervenției: „clauza de salvgardare” din Directiva (UE) 2018/1972 (art. 1 alin. (3) lit. c) și Considerentul 6), care recunoaște prioritatea statelor membre de a deroga de la normele pieței unice pentru asigurarea ordinii publice, a securității și investigarea infracțiunilor. Modelele de referință incluse vor fi: Germania (Legea Telecomunicațiilor - TKG, validare eID/VideoID), Spania (Legea Generală a Telecomunicațiilor) și Franța (Codul Poștei și Comunicațiilor Electronice - CPCE). Proporționalitatea măsurii este validată de jurisprudența supremă europeană. Curtea Europeană a Drepturilor Omului (cauza *Breyer c. Germaniei*, 2020) și Curtea de Justiție a Uniunii Europene (cauza *Ministerio Fiscal*, 2018) au statuat definitiv că obligația de identificare, limitată strict la datele de identitate, reprezintă o ingerință „limitată” și pe deplin proporțională cu scopul asigurării securității publice. Analiza impactului financiar nu este ipotetică. Suma agregată de 3,0 - 6,8 mil. MDL indicată la compartimentul 4.2 derivă exclusiv și direct din datele oficiale furnizate de operatorii de comunicații mobile în cadrul consultărilor tehnice din noiembrie 2025 (scrisorile nr. 01-07/9974 din 19.11.2025 și nr. 19504-11/25 din 21.11.2025). Acestea au fost prezentate agregat strict pentru protejarea secretului comercial. Beneficiile de securitate publică depășesc costurile de conformare, eficiența fiind dovedită empiric (ex: scăderea cu 93-95% a alertelor false cu bombă în Polonia). Impactul asupra operatorilor a fost minimizat direct în proiect, care exclude necesitatea identificării fizice în cele peste 3.700 de puncte de distribuție și transferă procesul exclusiv în mediul digital, la momentul activării.

		utilizate, precum și prin evaluarea costurilor pentru toate categoriile de actori vizați, inclusiv în baza consultării operatorilor de comunicații electronice. În absența acestor elemente, nu poate fi apreciată proporționalitatea măsurii propuse în raport cu obiectivele urmărite.	
	10.	**Concluzii și recomandări** Orice modificare sau completare a Legii comunicațiilor electronice nr. 72/2025, prin introducerea unor norme noi, necesită supunerea proiectului de lege procesului de expertizare al Comisiei Europene, în vederea asigurării compatibilității depline cu cadrul juridic al Uniunii Europene. De asemenea, se recomandă analizarea atentă a obiecțiilor și îngrijorărilor formulate de asociația patronală Asociația Națională a Companiilor din sectorul TIC (ATIC), expuse în demersul nr.757 din 18 februarie 2026, în vederea evaluării impactului asupra mediului investițional, a securității juridice și a funcționării pieței comunicațiilor electronice.	**Nu se acceptă.** Derogările în materie de securitate publică introduse de noul art. 125[1] sunt în deplină concordanță cu „clauza de salvgardare" a Directivei (UE) 2018/1972 (art. 1 alin. (3) lit. c) și Considerentul 6) și cu rigorile Regulamentului (UE) 2016/679 (RGPD). Expertiza de compatibilitate a proiectului cu legislația europeană este asigurată instituțional, în conformitate cu Legea nr. 100/2017, de către Centrul de Armonizare a Legislației. Îngrijorările industriei formulate prin demersul nr. 757 din 18.02.2026 au fost soluționate direct prin versiunea finală a proiectului. Care decuplează vânzarea de identificare, transferând sarcina exclusiv în mediul digital la momentul activării și evitând astfel blocajele logistice în cele peste 3.700 de puncte de distribuție terțe. Impactul asupra mediului de afaceri TIC este prevenit prin două garanții legale exprese, rezultate din consensul tehnic agreat cu operatorii în ședința din 24.12.2025: Conform Art. II din proiect, măsura se aplică exclusiv activărilor noi, eliminând riscul de pierdere a bazei actuale de clienți și de scădere a veniturilor curente ale operatorilor. Termenul de intrare în vigoare este stabilit la **12 luni**, oferind predictibilitatea și timpul necesar pentru adaptarea și testarea fără riscuri operaționale a sistemelor IT (eKYC, Billing).
INSPECTORAT DE STAT PENTRU SUPRAVEGHERE A PRODUSELOR NEALIMENTARE ȘI PROTECȚIA CONSUMATORILOR (Aviz nr. 27/12-1685 din 26 martie 2026)	1.	Inspectoratul de Stat pentru Supravegherea Produselor Nealimentare și Protecția Consumatorilor în limita competențelor atribuite prin lege, a examinat proiectul de lege pentru modificarea Legii nr. 72/2025 comunicațiilor electronice (număr unic 196/MAI/2026, autor – Ministerul Afacerilor Interne), și Vă transmite avizul fără propuneri și obiecții.	**Se acceptă.**
GRUPUL DE LUCRU AL COMISIEI DE	1.	Formularea de la alin.(4), care prevede că „până la finalizarea procesului de identificare" cartela poate fi utilizată	**Se acceptă parțial.**

STAT PENTRU REGLEMENTA A ACTIVITĂȚII DE ÎNTREPRINZĂTOR (Aviz nr. 38-78-3178 din 19 martie 2026)		doar pentru „servicii tehnice minime” (dacă este fezabil), este incertă și aplicabilitatea acesteia poate fi imprevizibilă. Cel puțin nu este clarificat ce presupune „servicii tehnice minime”. Dacă se instituie unele limitări, atunci acestea trebuie să fie clare și înțelese în mod cert, fără ambiguități și posibilități de interpretări discreționare. Obligația prevăzută la alin.(5), de a păstra datele de identificare a utilizatorului, este reglementată în mod ambiguu, odată ce se limitează la 12 luni de la „încetarea utilizării numărului”, ori în multe cazuri este complicat de a stabili exact când persoană a încetat să mai folosească un număr. Pentru un spor de precizie se recomandă completarea alineatului pentru a identifica „momentul încetării utilizării”, spre exemplu un eveniment mult mai cert ar fi încetarea contractului sau efectuarea ultimului apel, fie trimiterea ultimului mesaj SMS (sau de alt tip).	Pentru a oferi certitudinea solicitată, proiectul instituie un mecanism clar la Articolul II alin. (2), care obligă autoritatea de reglementare în domeniul comunicațiilor electronice să aprobe reglementările privind stabilirea acestor servicii necesare până la intrarea în vigoare a legii. Prin delegarea acestei competențe se asigură claritatea normei fără a supraîncărca textul de bază. Referitor la propunerea de a defini momentul încetării utilizării numărului prin acțiuni specifice precum ultimul apel sau SMS, sintagma actuală este menținută intenționat generică pentru a acoperi diversitatea raporturilor juridice, inclusiv serviciile de tip Machine-to-Machine (M2M) sau Internet of Things (IoT). În astfel de cazuri, încetarea utilizării este marcată de închiderea fluxului de date automatizat, iar o definire prea îngustă ar lăsa în afara legii categorii importante de servicii noi. Momentul exact al încetării utilizării este deja determinat și reglementat în practică prin condițiile generale de furnizare a serviciilor și prin contractele de abonament ale operatorilor.
	2.	Luând în calcul că obligația de identificare a utilizatorului se propune să fie plasată pe umerii operatorilor, la analiza situației existente lipsesc date despre modalitățile de vânzare din prezent, volumul vânzărilor și, în special, rata de cartele SIM preplătite sau volumul de utilizatori neidentificați, raportat la cei care se identifică la procurare sau în scurt timp după, optând pentru un abonament. În argumentarea necesității intervenției sunt prezentate unele raționamente de ordin general, mai mult ipotetic, fără statistici și date concrete. Fiind ilustrat un caz despre utilizarea abuzivă a cartelelor preplătite în unele state din UE (operațiunea Simcartel), fără a demonstra legătura cu Republica Moldova sau că în Moldova ar avea loc un fenomen similar. Pentru a estima la comp.4 beneficiile pentru societate, este important de a examina, demonstra și estima care este impactul real al utilizării anonime a cartelelor SIM. Dacă lipsa anonimatului ar putea duce la scăderea timpului de identificare a infractorilor, atunci poate fi estimat cu câte puncte procentuale ar putea crește nivelul de contracarare a infracțiunilor (și găsirea făptașilor), corespunzător cu câte puncte procentuale ar putea scădea prejudiciul pentru victime, dacă infractorul nu ar ajunge să comită mai multe infracțiuni. Însă, din analiza și practica altor state, aceste beneficii în realitate nu pot fi demonstrate. Așa	**Se acceptă parțial.** Nota de fundamentare va fi completată cu datele statistice care justifică ferm necesitatea intervenției: în Republica Moldova există în prezent 1.595.986 de cartele preplătite active, ceea ce reprezintă 42,7% din piața totală. Structura rețelei de distribuție arată că doar 12% din vânzări se realizează prin canale directe, restul de 88% bazându-se pe peste 3.700 de puncte terțe nespecializate, precum chioșcuri sau stații PECO. Acest volum masiv de conexiuni anonime constituie o vulnerabilitate sistemică critică, exploatată direct inclusiv în schemele recente de finanțare ilegală a campaniilor electorale, unde organele de drept au depistat zeci de mii de astfel de cartele. Chiar dacă operațiunea „Simcartel” vizează state membre UE, mecanismele și vulnerabilitățile descrise sunt direct aplicabile Republicii Moldova. Menținerea vidului de reglementare național transformă țara într-o sursă furnizoare de „turism SIM” pentru rețelele transfrontaliere, risc confirmat expres de documentele de securitate ale Consiliului UE din 2025. Pe plan intern, impactul lipsei anonimatului este documentat clar prin creșterea exponențială a criminalității informatice și a escrocheriilor bancare (phishing), infractorii utilizând exclusiv numere naționale anonime pentru a devaliza cetățenii.

		cum consemnează și o serie de organizații internaționale, precum Statewatch și Privacy International, nu există dovezi empirice că înregistrarea obligatorie a SIM-urilor duce la reducerea criminalității, ba din contra unele astfel de politici s-au dovedit ineficiente sau chiar contraproductive.	
	3.	Pe de o parte se impune gestionarea cu un volum mare de date care necesită un efort considerabil pentru a-l colecta, administra și proteja (cu riscuri înalte ca aceste date să fie sustrase sau vândute în mod ilegal), pe de altă parte există multe posibilități pentru infractori, cum ar fi utilizarea identității false sau de interpuși, SIM-uri cumpărate din alte țări, metode alternative de comunicare, un volum foarte mare de cartele care sunt deja activate și motivează la crearea unei piețe negre a acestora. O serie de state dezvoltate au examinat posibilitatea impunerii identificării utilizatorilor, cum ar fi Regatul Unit, Canada, Cehia, Noua Zeelandă, însă au renunțat la această reglementare odată ce au concluzionat că efectul asupra criminalității este limitat, riscurile însă sunt prea mari. Un exemplu elocvent este cel al Mexicului. În 2009, Mexicul a creat un registru național al utilizatorilor de telefonie mobilă. Toate cartelele SIM trebuiau înregistrate cu date personale. În 2012, legea a fost abrogată, din cauză că baza de date a fost spartă și vândută pe piața neagră, dar și s-a constatat că pe perioada funcționării legii, criminalitatea nu a scăzut, odată ce foarte multe SIM-uri folosite în infracțiuni erau înregistrate pe identități false. După abrogare, autoritățile au decis chiar ștergerea bazei de date cu utilizatori pentru a evita abuzurile. La analiza impactului este obligatoriu de a estima întregul spectru de costuri, în special pentru operatori și vânzătorii de cartele SIM, dar și cum aceste costuri se vor răsfrânge asupra prețului serviciilor de telefonie. Marea majoritate costurilor apar datorită obligației de a respecta legislația cu privire la protecția datelor cu caracter personal. Inclusiv este important de a estima scăderii volumului de vânzări, nu doar din cauza că obligația de identificare ar putea descuraja persoanele să procure o cartela SIM, dar și din cauză ca efortul și costul suplimentar pentru identificarea cumpărătorului și stocarea datelor presupune inevitabil scăderea accesibilității cartelelor. La fel, obligativitatea identificării poate deveni o piedică insurmontabilă pentru dezvoltarea noului segment de	**Se acceptă parțial.** Obiecțiile vizând securitatea datelor și posibilitățile de eludare a normei sunt soluționate prin varianta finală agreată a proiectului. Spre deosebire de modelele centralizate depășite, noile reglementări exclud colectarea fizică și stocarea nesigură a datelor în cele peste 3.700 de puncte de vânzare nespecializate. Identificarea se va realiza exclusiv prin instrumente controlate și securizate (eKYC, biometrie facială, interogare în timp real prin platforma MConnect), aplicând standarde de tip eIDAS care previn tehnic utilizarea actelor false sau furate. Deși nicio măsură nu elimină absolut riscul de eludare (prin roaming sau aplicații OTT), limitarea anonimatului pe piața internă crește exponențial costurile și riscurile operaționale pentru rețelele infracționale. Utilitatea este demonstrată empiric de practica altor state (precum Polonia), unde s-a înregistrat o reducere de 93-95% a alertelor false și o dublare a ratei de identificare a făptuitorilor, înregistrarea cartelelor fiind la momentul actual standardul de securitate aplicabil pentru peste 80% din populația Uniunii Europene. Impactul economic asupra operatorilor este atenuat strategic și direct prin două mecanisme juridice. În primul rând, se aplică principiul neretroactivității, legea vizând exclusiv activările viitoare și protejând astfel veniturile generate de baza curentă de aproximativ 1,59 milioane de utilizatori preplătiți. În al doilea rând, abordarea „Digital First” nu reprezintă o piedică, ci instrumentul care facilitează activarea online a tehnologiei eSIM prin identitate digitală (EVO/eID). Costurile de conformare inițială (CAPEX), estimate transparent între 3,0 și 6,8 milioane MDL în baza datelor oficiale comunicate de industrie, sunt proporționale cu interesul public major de reducere a fraudelor bancare și de salvare a bugetelor operaționale de urgență (serviciul 112). Acest efort financiar este eșalonat sustenabil prin instituirea perioadei de tranziție de 12 luni, care oferă operatorilor timpul necesar pentru adaptarea sistemelor de facturare și eKYC.

		tehnologie eSIM. Deci, pe lângă costurile directe pe care le vor suporta operatorii, este important de a estima și pierderile potențiale, care trebuie adăugate la costurile totale. Într-un final, este necesar de a contrapune costurile cu beneficiile pentru societate și a demonstra care sunt beneficiile nete, dacă acestea sunt demonstrate și estimate. Nu în ultimul rând, este important de a clarifica care sunt mecanismele care asigură că aceste date nu vor ajunge să fie furate sau cumpărate pe piața neagră, inclusiv ce asigurări sunt că datele vor fi colectate fără abuzuri și fără falsuri.	
CONSILIULUI CONCURENȚEI (Aviz nr. DJ-06/207-480 din 27.03.2026)	1.	Plenul Consiliului Concurenței, în cadrul ședinței din 27 martie 2026, a examinat, în temeiul prevederilor art. 39 lit. c) și art. 41 alin. (1) lit. d) ale Legii concurenței nr. 183/2012, proiectul de lege pentru modificarea Legii nr. 72/2025 comunicațiilor electronice (număr unic 196/MAI/2026) și, în limitele competenței sale, comunică lipsa de obiecții și propuneri.	**Se acceptă.**
CENTRUL DE ARMONIZARE A LEGISLAȚIEI (Aviz nr. 31/02-69 3392 din 27.03.2026)	1.	Centrul de armonizare a legislației a examinat proiectul de lege pentru modificarea Legii nr. 72/2025 comunicațiilor electronice, promovat suplimentar Programului național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029, aprobat prin Hotărârea Guvernului nr. 306/2025 și, comunică următoarele. Proiectul prenotat are drept scop completarea Legii nr. 72/2025 comunicațiilor electronice cu un nou articol 125¹, prin care se instituie obligația furnizorilor de servicii de comunicații electronice mobile accesibile publicului de a identifica abonații, indiferent dacă este vorba despre abonamente sau cartele preplătite. Textul reglementează categoriile de date ce urmează a fi colectate, metodele de identificare, inclusiv la distanță, utilizarea mijloacelor de identificare electronică și a biometriei faciale, precum și păstrarea datelor de identificare pe durata utilizării serviciului și încă 12 luni după încetarea utilizării numărului. Menționăm că, Legea nr. 72/2025 este un act normativ național armonizat, care a asigurat transpunerea parțială a prevederilor Directivei (UE) 2018/1972, Regulamentului delegat (UE) 2021/654, Directivei 2002/58/CE, Directivei 2008/63/CE, Directivei 98/84/CE, Regulamentului (UE) 2015/2120, Regulamentului delegat (UE) 2023/444, precum și transpunerea Regulamentului (UE)	**Se acceptă.**

		2021/1232 și Directivei 2002/77/CE. Din perspectiva proiectului examinat, prezintă relevanță: Carta drepturilor fundamentale a Uniunii Europene, Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice (reformare), Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) și Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).	
	2.	La nivel de drepturi fundamentale, art. 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene protejează viața privată și datele cu caracter personal, iar articolul 52 (1) din aceasta impune ca orice restrângere să fie prevăzută de lege, să respecte substanța drepturilor și să fie proporțională în raport cu un obiectiv de interes general.	**Se acceptă.** Aceste norme constituie fundamentul juridic pe care a fost elaborată întreaga arhitectură a proiectului de lege. Modificarea actului normativ propus prin introducerea art. 125[1] în Legea nr. 72/2025 a fost minuțios analizat pentru a respecta proporționalității și necesității, fiind concepută ca o derogare strict limitată în scopul protejării securității naționale și ordinii publice, în deplină concordanță cu art. 23 din Regulamentul (UE) 2016/679 (GDPR) și art. 15 din Directiva ePrivacy.
	3.	În context, art. 100 din Directiva 2018/1972 statuează că măsurile luate la nivel național cu privire la accesul și folosirea de către utilizatorii finali a serviciilor și aplicațiilor prin intermediul rețelelor de comunicații electronice trebuie să respecte Carta drepturilor fundamentale a Uniunii și principiile generale ale dreptului Uniunii, iar orice restrângere a drepturilor poate fi impusă numai dacă este prevăzută de lege și respectă respectivele drepturi și libertăți, este proporțională, necesară și răspunde efectiv obiectivelor de interes general recunoscute de dreptul Uniunii sau necesității de a proteja drepturile și libertățile celorlalți în conformitate cu articolul 52 alineatul (1) din Cartă și cu principiile generale ale dreptului Uniunii, inclusiv dreptul la o cale de atac eficientă și la un proces echitabil.	**Se acceptă parțial.** Măsura răspunde necesității imperative de a proteja securitatea națională și ordinea publică, prin eliminarea anonimatului structural care facilitează criminalitatea. Ingerința este strict limitată la colectarea datelor de identitate (nume, prenume, IDNP) necesare pentru atribuirea numărului, fără a viza conținutul comunicațiilor sau datele de trafic, fapt ce încadrează măsura în categoria „ingerințelor limitate”, conform reglementărilor CJUE (cauza Ministerio Fiscal) și CEDO (cauza Breyer c. Germaniei). Mecanismul propus nu doar că respectă, dar și implementează garanțiile cerute de art. 100 din Directiva (UE) 2018/1972, asigurând un echilibru corect între securitatea colectivă și libertățile individuale.

		Totodată, și art. 15 din Directiva 2002/58/CE permite statelor să adopte măsuri legislative care restrâng anumite drepturi în materia comunicațiilor electronice doar dacă acestea sunt adecvate, strict proporționale, necesare într-o societate democratică și însoțite de garanții corespunzătoare pentru a proteja securitatea națională (de exemplu siguranța statului), apărarea, siguranța publică sau pentru prevenirea, investigarea, detectarea și urmărirea penală a unor fapte penale sau a folosirii neautorizate a sistemelor de comunicații electronice, în conformitate cu articolul 13 alineatul (1) al Directivei 95/46/CE.	
	4.	În context, instituirea, prin proiectul național, a unei obligații de identificare a utilizatorilor serviciilor mobile, inclusiv, pentru cartelele preplătite, reprezintă o măsură de restrângere a drepturilor în materia comunicațiilor electronice, dar care, nu este, per se, interzisă de dreptul UE. Curtea de Justiție a Uniunii Europene, în Hotărârea Curții (Marea Cameră) din 5 aprilie 2022. G.D. împotriva Commissioner of the Garda Síochána și alții., a constatat expres că, dreptul UE nu se opune unei legislații naționale care, în scopul combaterii criminalității grave și al prevenirii amenințărilor grave împotriva siguranței publice, stabilește o ”păstrare generalizată și nediferențiată a datelor referitoare la identitatea civilă a utilizatorilor de mijloace de comunicații electronice” (condiționează cumpărarea unui mijloc de comunicație electronică, precum o cartelă SIM preplătită, de verificarea identității cumpărătorului și de înregistrarea datelor relevante de către vânzător). Cu toate acestea, proiectul național nu enunță expres care este scopul legitim (”în scopul combaterii criminalității grave și al prevenirii amenințărilor grave împotriva siguranței publice”) pentru care se instituie identificarea generalizată a abonaților. Din perspectiva legislației UE, aceasta este o omisiune relevantă, deoarece ingerințele în drepturile consacrate de art. 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene trebuie să fie nu doar utile autorităților publice, ci și clar justificate printr-un obiectiv determinat și redactate într-o manieră suficient de precisă.	**Nu se acceptă.** Potrivit normelor de tehnică legislativă prevăzute la art. 54 alin. (1) lit. a) din Legea nr. 100/2017, textul articolelor trebuie să aibă un caracter strict dispozitiv, prezentând norma instituită fără explicații sau justificări, motiv pentru care inserarea unor norme penale în structura legii ar altera actul normativ. Funcția de explicitare a scopului legitim este exercitată exclusiv de Nota de fundamentare, care, conform art. 71 alin. (4) din Legea nr. 100/2017, reprezintă instrumentul prin care se identifică voința autorității și ghidează interpretarea normei, satisfăcând astfel pe deplin exigențele CJUE privind justificarea ingerinței. Din perspectiva dreptului Uniunii Europene, proiectul instituie o obligație de colectare exclusivă a datelor de identitate, acțiune calificată de jurisprudența CJUE (cauza *Ministerio Fiscal*, 2018) și CEDO (cauza *Breyer c. Germaniei*, 2020) drept o ingerință limitată, care nu permite crearea unui profil al vieții private. În consecință, standardul de justificare este unul general, axat pe prevenirea infracțiunilor, nefiind condiționat de pragul „criminalității grave” aplicabil doar retenției metadatelor de trafic și localizare. Măsura valorifică „clauza de salvgardare” din Considerentul (6) al Directivei (UE) 2018/1972, care recunoaște prioritatea acțiunilor statelor membre pentru asigurarea ordinii și siguranței publice.
	5.	De asemenea, art. 125^1 , alin. (2) din proiect, care stabilește colectarea a ”cel puțin a următoarelor date”, ridică	**Se acceptă.**

		aspecte de compatibilitate cu Regulamentul (UE) 2016/679, în speță, cu art. 5, care consacră principiile limitării scopului, reducerii la minimum a datelor și limitării stocării, ceea ce presupune că datele trebuie să fie adecvate, relevante și limitate la ceea ce este necesar pentru scopul urmărit. Astfel, se consideră necesară enumerarea exhaustivă a datelor care sunt colectate și eliminarea formulării extensibile. Art. 125^1 , alin. (5) din proiect, care stabilește păstrarea datelor de identificare pe durata utilizării serviciului și încă 12 luni după încetarea utilizării numărului, urmează a fi reexaminat prin prisma principiului limitării stocării la ”o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele” din art. 5 din Regulamentul (UE) 2016/679. În context, se impune justificarea suplimentară și explicită a necesității stocării acestor date peste durata utilizării serviciului. În concluzie, se impune reexaminarea proiectului de Lege prin prisma observațiilor expuse mai sus. Facem mențiunea că analiza Centrului de armonizare a legislației nu are în vedere elementele de oportunitate ale soluțiilor juridice incluse în proiectul de act normativ, ci se referă strict la conformitatea acestora cu Dreptul UE aplicabil, obligațiile juridice asumate în lumina Acordului de Asociere RM – UE și Cadrului de negociere cu Uniunea Europeană.	
PROCURATURA GENERALĂ (Aviz nr. 31/02-69 3392 din 27.03.2026)	1.	Procuratura Generală a examinat proiectul de lege pentru modificarea Legii nr. 72/2025 comunicațiilor electronice (număr unic 196/MAI/2026), expediat spre avizare. Apreciind conținutul proiectului prin prisma principiilor activității de legiferare prevăzute la art. 3 din Legea nr. 100/2017 cu privire la actele normative, precum și în limita competențelor funcționale, se formulează următoarele constatări și propuneri: Proiectul de lege propune instituirea obligației de identificare a utilizatorilor serviciilor de comunicații electronice mobile, inclusiv în cazul cartelelor preplătite, prin introducerea art. 125^1.Se apreciază că inițiativa legislativă urmărește un scop legitim, orientat spre reducerea riscurilor de criminalitate asociate utilizării anonime a serviciilor de comunicații electronice, fiind, în principiu, oportună. Totodată, se constată că utilizarea metodelor de identificare la distanță, inclusiv prin mijloace biometrice sau alte	**Nu se acceptă.** **Precizare.** Constatările sunt pertinente, însă reglementarea specifică a standardelor minime de securitate și a garanțiilor privind prelucrarea datelor biometrice la distanță, direct în textul Legii comunicațiilor electronice nr. 72/2025, nu este necesară și ar genera un paralelism legislativ, contrar rigorilor de tehnică legislativă prevăzute de art. 54 din Legea nr. 100/2017 cu privire la actele normative. Cadrul juridic pentru protecția și securitatea datelor este deja complet configurat, iar furnizorii au obligația să i se conformeze în mod direct: Obligația de a institui măsuri tehnice și organizatorice de securitate, criptare, control al accesului, trasabilitate și prevenire a fraudelor derivă imperativ din cadrul normativ general privind protecția datelor cu caracter personal, în speță **Legea nr. 133/2011** și **noua Lege nr. 195/2024** (care transpune Regulamentul (UE) 2016/679 - GDPR). Din perspectiva utilizării noilor tehnologii (soluții

		tehnologii electronice, nu este însoțită de instituirea unor standarde minime de securitate și a unor garanții adecvate privind protecția datelor cu caracter personal, ceea ce poate genera riscuri în aplicare. În acest context, proiectul nu reglementează cerințe minime privind securitatea prelucrării datelor utilizate în cadrul procesului de identificare la distanță, în special în cazul datelor biometrice, precum: standarde de autentificare, măsuri de prevenire a utilizării frauduloase, cerințe de criptare, precum și reguli privind stocarea și accesul la aceste date. Deși prevederile art. 115-125 din Legea nr. 72/2025 privind comunicațiile electronice instituie un cadru general în materia securității prelucrării datelor și a confidențialității comunicațiilor, acestea nu reglementează în mod specific particularitățile și riscurile aferente utilizării datelor biometrice.	biometrice sau eKYC la distanță), operatorii sunt obligați direct de legile menționate să efectueze o Evaluare a Impactului asupra Protecției Datelor (DPIA) înaintea implementării. Utilizarea mijloacelor de identificare la distanță și validarea tehnologiilor (inclusiv autentificarea biometrică) urmează a fi realizată cu respectarea strictă a rigorilor și standardelor tehnice de securitate din **Legea nr. 124/2022** privind identificarea electronică și serviciile de încredere. Așa cum s-a stabilit și în urma consultărilor cu Centrul Național pentru Protecția Datelor cu Caracter Personal (CNPDCP), operatorii rămân titularii unici ai obligațiilor de colectare și securizare, iar competențele de verificare și sancționare aparțin direct autorității de supraveghere pe domeniul datelor personale, fără a fi necesară crearea unor regimuri ori proceduri paralele în legea sectorială. Prin urmare, nu se impune dublarea normelor privind protecția datelor biometrice sau a cerințelor de criptare și securitate informațională în Legea nr. 72/2025, operatorii fiind direct ținuți să respecte acquis-ul orizontal în materie de securitate a datelor.
	2.	De asemenea, formularea relativ generală referitoare la „alte mijloace electronice oferite de furnizor” din conținutul art. 125^1 alin. (3) pct. 3 lit. d) poate genera incertitudine juridică și practici neuniforme, fiind recomandabilă fie definirea acestor mijloace, fie stabilirea unor criterii minime obligatorii. În considerarea celor expuse, se avizează pozitiv proiectul de lege, cu recomandarea valorificării observațiilor și propunerilor formulate.	**Nu se acceptă.** Formularea referitoare la „alte mijloace electronice oferite de către furnizor” nu instituie o categorie arbitrară sau deschisă de identificare care ar genera practici neuniforme, ci este condiționată expres și limitativ în textul legii. Conform art. 125^1 alin. (3), aceste mijloace pot fi utilizate exclusiv „în cazul în care datele de identificare ale abonatului au fost anterior verificate în legătură cu un alt număr” prin una dintre metodele principale, cu grad înalt de securitate (identificare fizică, prin semnătură electronică calificată conform Legii nr. 124/2022 sau prin identificare digitală/biometrică cu interogarea Registrului de stat al populației). Prin urmare, s-a stabilit deja criteriul minim obligatoriu: „alte mijloace electronice” (cum ar fi autentificarea în aplicația mobilă a operatorului sau confirmarea prin cod OTP) reprezintă doar un mecanism de reutilizare a validării KYC (Know Your Customer) pentru clienții existenți a căror identitate certă este deja stabilită și stocată de operator.

SERVICIUL TEHNOLOGIA INFORMAȚIEI ȘI SECURITATE CIBERNETICĂ (Aviz nr. 1.4/638/26 din 25.03.2026)	1.	Cu referire la art. I din proiect, prin care se propune completarea Legii nr. 72/2025 comunicațiilor electronice cu art. 125[1] alin. (3) pct. 3): - litera a) cuvintele „sau avansată” se vor exclude întrucât potrivit art. 21 alin. (2) din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere, semnătura electronică calificată este singura care are aceeași valoare juridică precum semnătura olografă. În acest context, includerea alăturată a două instrumente care nu beneficiază de același regim juridic poate genera neclarități de aplicare. Prin urmare, excluderea cuvintelor menționate este necesară pentru a evita eventuale interpretări cu privire la valoarea juridică a mijlocului de identificare utilizat.	**Se acceptă.**
	2.	Totodată, se propune excluderea textului „sau alte mijloace electronice oferite de către un prestator de servicii de încredere calificat” întrucât formularea utilizată are un caracter general și nu permite identificarea suficient de clară a mijloacelor electronice avute în vedere. În redactarea actuală, aceasta poate crea dificultăți de aplicare.	**Nu se acceptă.** Conform Legii nr. 124/2022, un „prestator de servicii de încredere calificat” este o entitate supusă unui regim juridic extrem de riguros. Pentru a obține și menține acest statut, prestatorul este obligat să parcurgă proceduri de auditare a conformității și să implementeze sisteme tehnice de cel mai înalt nivel de securitate, fiind monitorizat constant de organul de supraveghere a statului. Excluderea acestei sintagme ar restrânge identificarea la distanță doar la „semnătura electronică calificată”, limitând artificial capacitatea operatorilor de a utiliza alte instrumente moderne și sigure. Conform art. 10 alin. (2) pct. 4) lit. d) din Legea nr. 124/2022, identitatea persoanelor poate fi verificată de prestatori și „ prin utilizarea altor metode de identificare recunoscute la nivel național, care oferă un nivel de asigurare echivalent, din perspectiva fiabilității, cu prezența fizică ”. Astfel, textul proiectului trebuie să lase deschise soluțiile eKYC (Know Your Customer electronic) la distanță sau viitoarele Portofele Europene pentru Identitate Digitală (EUDIW / eIDAS 2.0) oferite de acești prestatori calificați. Orice „alt mijloc electronic” va putea fi aplicat în practică doar dacă este recunoscut și reglementat prin actele normative subsecvente Legii nr. 124/2022, eliminându-se astfel riscul de practici neuniforme.

	3.	- litera c) se va exclude. Se constată că proiectul utilizează sintagma „sistemul guvernamental de identitate digitală (EVO)” ca și cum aceasta ar reprezenta un sistem existent în cadrul normativ în vigoare. Or, STISC nu a identificat un act normativ care să reglementeze EVO sub această denumire și cu această funcționalitate. În conformitate cu art. 76 din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, toate sistemele și resursele informaționale de stat urmează să fie documentate în mod corespunzător. Prin urmare, dacă un „sistem guvernamental de identitate digitală (EVO)” ar exista în sensul utilizat în proiect, acesta ar trebui să fie prevăzut și documentat expres în cadrul normativ.	**Se acceptă.**
	4.	Totodată, potrivit Hotărârii Guvernului nr. 5/2024 cu privire la aplicația guvernamentală integrată a serviciilor electronice EVO, soluția EVO reprezintă o soluție bazată pe aplicații mobile, care permite persoanelor fizice și juridice să acceseze servicii electronice, date din registrele de stat și să dețină versiuni digitale ale actelor de identitate și ale altor documente-cheie. De asemenea, aceasta reprezintă un ansamblu de resurse și tehnologii informaționale, mijloace tehnice de program și metodologii, aflate în interconexiune, având drept scop oferirea unui punct unic de acces la resurse, aplicații și servicii electronice.	**Se acceptă.**
	5.	Totodată, din conținutul actului normativ nu rezultă în mod expres că aceasta ar avea ca scop sau ar include funcționalități de identificare la distanță a persoanei. În aceste condiții, formularea utilizată în proiect nu rezultă din cadrul normativ existent, fiind de natură să creeze neclarități sub aspectul regimului juridic și al funcționalităților avute în vedere.	**Se acceptă.**

AGENȚIA DE GUVERNARE ELECTRONICĂ (Aviz nr. 3007-073 din 25.03.2026)	1.	La alin. (2) utilizarea sintagmei „cel puțin a următoarelor date” nu este conformă principiilor protecției datelor cu caracter personal în contextul colectării unor astfel de date. Această formulare poate permite colectarea nejustificată și a unor alte date cu caracter personal, fapt care contravine principiului minimizării datelor, reglementat în art. 5 lit. c) din Legea nr. 195/2024 privind protecția datelor cu caracter personal (care va intra în vigoare la data de 23.08.2026). Astfel, conform principiului menționat, căruia datele cu caracter personal sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate. În caz contrar, operatorii pot interpreta norma într-un mod în care le-ar permite să colecteze categorii suplimentare de date care nu sunt neapărat potrivite scopului urmărit și fără o justificare legală clară.	**Se acceptă.**
	2.	La alin.(2) pct.2) și 4), sub aspectul reținerii copiilor actelor de identitate sau a copiilor documentelor care atestă înregistrarea persoanelor juridice, recomandăm excluderea necesității colectării acestor copii, în contextul în care la prezentarea originalelor actelor respective, datele necesare de identificare sunt colectate.	**Nu se acceptă.** Proiectul de lege exclude deja obligația reținerii copiilor actelor de identitate pentru cetățenii și persoanele juridice din Republica Moldova, deoarece identificarea și validarea acestora se realizează direct, automatizat și sigur prin interogarea Registrului de stat, prin intermediul platformei guvernamentale MConnect. În cazul persoanelor fizice și juridice străine, reglementate la art. 125^1 alin. (2) pct. 2) și 4), statul nu deține acces la registrele din alte state pentru a le verifica datele. În lipsa posibilității de validare electronică a acestor documente, reținerea copiei actului de identitate sau a documentului de înregistrare pentru nerezidenți reprezintă singura modalitate tehnică și juridică viabilă de a asigura trasabilitatea reală a utilizatorului, condiție imperativă solicitată de organele de drept. Excluderea acestei cerințe ar genera o lacună majoră de securitate, permițând eludarea identificării prin utilizarea actelor străine imposibil de verificat ulterior.
	3.	Cu referire la alin. (2) pct.1) și 3) și alin.(3) pct.3) lit.b) care prevede gratuitatea interogării Registrului de stat al populației și a Registrului de stat al unităților de drept de către furnizorii de servicii de comunicații electronice mobile, atragem atenția că potrivit art. 6 alin.(6) din Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate, schimbul de date pentru participanții privați are loc exclusiv prin intermediul platformei de interoperabilitate (MConnect). Contractul de schimb de date este cu titlu oneros și se încheie	**Se acceptă.**

		între deținătorul platformei de interoperabilitate (AGE) și participantul privat în modul și condițiile stabilite de Guvern. Costul serviciilor de schimb de date se achită de participantul privat conform facturilor emise de autoritatea competentă și se distribuie în modul următor: 75% din taxa aplicată – către furnizorii de date, 25% din taxa aplicată – către deținătorul platformei de interoperabilitate. Subsecvent, din proiectul de lege se vor exclude referințele la gratuitatea datelor puse la dispoziție furnizorilor de servicii de comunicații electronice mobile.	
	4.	În concordanță cu noțiunile reglementate de Legea nr.124/2022 privind identificarea electronică și serviciile de încredere, Hotărârea Guvernului nr.5/2024 cu privire la aplicația guvernamentală integrată a serviciilor electronice EVO, Procedura de identificare a persoanei fizice de la distanță utilizând mijloace digitale, aprobată prin Hotărârea Guvernului nr. 977/2023, dar și a acțiunilor care urmează a fi întreprinse în contextul transpunerii totale a Regulamentului (UE) nr.910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, alin.(3) al art.125[1] . „(3) La alegerea furnizorilor, identificarea și verificarea identității abonaților serviciilor de comunicații electronice mobile accesibile publicului se realizează prin una sau mai multe dintre următoarele metode: 1) prin prezența fizică a persoanei fizice sau a reprezentantului autorizat al persoanei juridice la punctele de vânzare proprii ale furnizorului; 2) prin prezența fizică la punctele de vânzare ale persoanelor împuternicite de furnizor în baza unui raport juridic de reprezentare; 3) la distanță, prin: a) utilizarea unui portofel pentru identitatea digitală, furnizat sau recunoscut de stat, care permite utilizatorului stocarea și furnizarea în condiții de siguranță a datelor de identificare personală; b) utilizarea unor mijloace de identificare electronică emise în cadrul unui sistem de identificare electronică (semnătură electronică sau sigiliu electronic calificate sau avansate) ori prin alte servicii de încredere prestate de un prestator de servicii de încredere calificat, în condițiile cadrului normativ care reglementează identificarea electronică și serviciile de încredere; c) proceduri	**Se acceptă parțial.** Așa cum s-a stabilit în urma examinării avizului Serviciului Tehnologia Informației și Securitate Cibernetică (STISC), conform art. 21 alin. (2) din Legea nr. 124/2022, doar semnătura electronică calificată are o valoare juridică echivalentă cu semnătura olografă la încheierea contractelor. Păstrarea semnăturii „*avansate*” ar genera incertitudine juridică. Totodată, textul propus utilizează termenul de „*abonat*”, deși s-a agreat deja utilizarea noțiunii mai largi și corecte de „utilizator”. Formularea propusă conține detalii tehnice excesive (precum referințele la „*portofelul digital*” sau la datele biometrice). Conform normelor de tehnică legislativă art. 54 din Legea nr. 100/2017 cu privire la actele normative, o lege-cadru trebuie să rămână neutră din punct de vedere tehnologic pentru a-și păstra aplicabilitatea în timp. Astfel, detaliile tehnice specifice și modul de funcționare a acestor instrumente urmează a fi reglementate separat, prin acte normative secundare.

		de identificare de la distanță ce asigură un nivel de încredere ridicat, bazate pe utilizarea datelor de identificare personală și a factorilor de inerență (date biometrice), prin procesarea imaginilor și a informațiilor verificate prin raportare la o resursă informațională de stat (sursă autentică); d) procesul de corelare a identității abonatului cu date de identificare personală ce au fost verificate anterior în raport cu un alt număr de abonat, utilizând metodele prevăzute la subpunctele 1) - 3).”	
SERVICIUL TEHNOLOGIA INFORMAȚIEI ȘI SECURITATE CIBERNETICĂ (Aviz nr. 1.4/693/26 din 03.04.2026)	1.	În spiritul bunei colaborări instituționale și cu deosebit respect față de eforturile depuse de Ministerul Afacerilor Interne, I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică” (în continuare IP STISC) îndrăznește să apeleze la deschiderea și susținerea Dumneavoastră în vederea examinării posibilității de a completa proiectul de lege pentru modificarea Legii nr. 72/2025 a comunicațiilor electronice (număr unic 196/MAI/2026) cu unele prevederi esențiale, dar care nu au fost prevăzute la etapa de elaborare a noii legi a comunicațiilor electronice. Astfel, se propune completarea Articolului I cu următoarele prevederi care au drept scop modificarea art. 3 alin. (5) din Legea nr. 72/2025: 1. lit. b), se va expune în redacție nouă după cum urmează: „b) atribuie, înregistrează, reînregistrează, blochează, revocă, retrage nume din domeniul național de nivel superior „.md”, modifică datele de contact ale Registrantului, după caz suspendă modificarea datelor de contact ale Registrantului;”;	**Nu se acceptă.** Propunerea formulată de I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică” (STISC), deși este pertinentă pentru clarificarea atribuțiilor instituției în gestionarea domeniului de nivel superior „.md”, excedează obiectului de reglementare al prezentului proiect de lege. Conform normelor de tehnică legislativă prevăzute de Legea nr. 100/2017 cu privire la actele normative, modificările aduse unui act trebuie să asigure caracterul unitar al reglementării și să corespundă strict scopului intervenției legislative. Prezentul proiect de lege are un scop exhaustiv și fundamentat pe rațiuni de securitate și ordine publică: instituirea obligației de identificare a utilizatorilor de cartele SIM preplătite la momentul activării. Totodată, subliniem că, în conformitate cu prevederile art. 23 alin. (1) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, Ministerul Dezvoltării Economice și Digitalizării (MDED) este organul central de specialitate competent să elaboreze documentele de politici și actele normative în domeniul informatizării, al sistemelor și resurselor informaționale de stat. Prin urmare, inițiativa legislativă de extindere sau clarificare a atribuțiilor STISC privind administrarea resurselor de internet urmează a fi înaintată conform competenței către MDED, pentru a fi examinată și promovată separat, în cadrul unui proiect de act normativ distinct și relevant domeniului vizat.
	2.	Se va completa cu lit. f) cu următorul cuprins „f) și alte atribuții stabilite conform art. 7 alin. (2) pct. 26).”. Subliniem că gestionarea domeniului național de nivel superior .md este	**Nu se acceptă.** **Argumentarea la pct. 1.**

		reglementată de către Agenția Națională pentru Reglementare în Comunicații, iar atribuțiile IP STISC în calitate de registrator național, conform pct. 8 sbp. 35) din Statutul IP STISC aprobat prin Anexa nr. 1 la Hotărârea Guvernului nr. 414/2018, implică mult mai multe activități decât cele reglementate expres și limitativ de Legea nr. 72/2025. Or, redacția actuală a art. 3 alin. (5) împiedică gestionarea corespunzătoare a domeniului național de nivel superior .md prin restricționarea exercitării altor atribuții imperative. Fără aceste modificări, respectiv fără determinarea atribuțiilor într-un cadru F01-IL-1.2.01 V.R 1.0 Pagina 2 din 2 mai general la art. 3 alin. (5) din Legea nr. 72/2025, IP STISC s-ar putea ciocni cu litigii pentru îndeplinirii neîntemeiată și abuzivă a altor atribuții decât cele prevăzute expres de legea primară. În această ordine de idei, Vă rămânem profund recunoscători pentru analizarea acestor completări esențiale și, în speranța unei decizii favorabile, Vă exprimăm înalta considerație și deplina deschidere spre colaborare.	
MINISTERUL FINANŢELOR AL REPUBLICII MOLDOVA (Aviz nr. 09/2-03/201/468 din 02.04.2026)	1.	La demersul Cancelariei de Stat nr. DGPȘG-2055-18-69-841 din 10.03.2026, Ministerul Finanțelor a examinat proiectul de lege pentru modificarea Legii nr. 72/2025 comunicațiilor electronice (număr unic 196/MAI/2026), autor – Ministerul Afacerilor Interne și, în limita domeniilor de competență, comunică următoarele. 1) La Articolul I, în cuprinsul Articolului 125[1] , alin. (1) va avea următorul cuprins: „(1) Furnizorii de servicii de comunicații electronice mobile accesibile publicului sunt obligați să identifice utilizatorii finali, persoane fizice sau juridice, care contractează ori activează serviciile 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.”. Această propunere este dictată de necesitatea respectării prevederilor art. 2 din Legea comunicațiilor electronice nr. 72/2025, unde noțiunea de „abonat” presupune deja existența unui contract prealabil. În cazul cartelelor preplătite, raportul juridic de abonament se cristalizează abia post-identificare. Utilizarea termenului de „utilizator final” corelat cu acțiunea de „contractare sau activare” asigură conformitatea cu Directiva (UE) 2018/1972 și elimină riscul ca operatorii să invoce lipsa calității de	**Se acceptă parțial.** Conform art. 2 din Legea nr. 72/2025, noțiunea de „utilizator” semnifică deja expres o „persoană fizică sau juridică ce utilizează sau solicită utilizarea unui serviciu de comunicații electronice”. Prin urmare, adăugarea sintagmei explicative „ persoane fizice sau juridice ” constituie o tautologie juridică și încarcă inutil textul actului normativ. În al doilea rând, precizarea acțiunilor „ *care contractează ori activează serviciile* ” este redundantă și descriptivă, având în vedere că momentul aplicării obligației este deja reglementat clar și imperativ în textul proiectului: „ *la momentul încheierii contractului de abonament sau, în cazul cartelelor preplătite, cel târziu la momentul activării acestora* ”. Subliniem că riscul invocat de Ministerul Finanțelor a fost deja înlăturat prin proiectul definitivat, unde s-a acceptat (inclusiv la propunerea ARCOM) substituirea integrală a termenului de „abonat” cu cel de „utilizator”, asigurând astfel un cadru corect și acoperitor pentru ambele tipuri de oferte (abonament și cartelă preplătită), cu respectarea regulilor de redactare a actelor normative.

		„abonat” a posesorilor de cartele preplătite pentru a evita procedura de identificare. Totodată, precizarea expresă a persoanelor juridice asigură trasabilitatea în schemele de distribuție complexe (B2B2C), închizând astfel orice „portiță” de interpretare restrictivă.	
	2.	2) Proiectul legii se va completa prin includerea unui Articol III pentru modificarea Codului Contravențional nr. 218/2008, prin introducerea sancțiunilor pentru furnizorii care activează servicii fără identificarea prealabilă. Modificarea este motivată prin faptul că, în absența unei sancțiuni, obligația instituită la Art. 125^1 rămâne o declarație de intenție. Prin urmare, pentru eficiența normei, este necesară corelarea cu regimul sancționator contravențional.	**Nu se acceptă.** Afirmația conform căreia norma ar rămâne o simplă „declarație de intenție” nu este reținută. Odată cu introducerea noului art.125^1 în Legea comunicațiilor electronice nr. 72/2025, identificarea utilizatorilor devine o obligație legală expresă și o condiție de furnizare a serviciilor. Prin urmare, nerespectarea acestei norme atrage direct incidența regimului sancționator general deja existent în Codul Contravențional pentru încălcarea legislației în domeniul comunicațiilor electronice. Autoritatea de reglementare (ARCOM) dispune deja de mecanisme de control și sancționare (inclusiv suspendarea activității sau sancțiuni financiare) pentru furnizorii care nu respectă obligațiile legale. Implementarea și eficiența art. 125^1 sunt asigurate de mecanismele de supraveghere și sancționare existente, urmând ca, în cazul în care practica de aplicare o va impune, individualizarea unei contravenții specifice să fie promovată ulterior, printr-un proiect distinct de modificare a Codului Contravențional.
EXPERTIZARE			
BIROUL POLITICI DE REINTEGRARE (comentariu în e-Legiferare)	1.	Biroul politici de reintegrare comunică lipsa de obiecții și propuneri.	**Se acceptă.**
MINISTERUL FINANȚELOR (comentariu în e-Legiferare)	1.	Lipsa obiecțiilor	**Se acceptă.**
PROCURATURA GENERALĂ (comentariu în e-Legiferare)	1.	Procuratura Generală informează lipsa de obiecții/propuneri	**Se acceptă.**

MINISTERUL DEZVOLTĂRII ECONOMICE ȘI DIGITALIZĂRII (comentariu în e-Legiferare)	1.	Prin adoptarea Legii comunicațiilor electronice nr. 72/2025, Republica Moldova a asigurat transpunerea Codului european al comunicațiilor electronice și a actelor relevante ale Uniunii Europene, instituind un cadru juridic aliniat la acquis-ul european. Proiectul legii a fost supus, anterior adoptării, expertizării de către experții DG CONNECT din cadrul Comisiei Europene, fiind confirmată compatibilitatea deplină cu cadrul juridic al Uniunii Europene. În acest context, în cazul promovării unor modificări sau completări ale Legii comunicațiilor electronice nr. 72/2025, prin introducerea unor norme noi, se recomandă supunerea proiectului de lege procesului de expertizare al Comisiei Europene, în vederea asigurării și menținerii compatibilității cu cadrul juridic al Uniunii Europene.	**Nu se acceptă.** Derogările în materie de securitate publică introduse prin noul art. 125[1] sunt în deplină concordanță cu „clauza de salvgardare" a Directivei (UE) 2018/1972 (art. 1 alin. (3) lit. c) și Considerentul 6) și cu rigorile Regulamentului (UE) 2016/679 (GDPR). Expertiza de compatibilitate a proiectului de lege cu legislația Uniunii Europene este deja asigurată la nivel instituțional, în conformitate cu prevederile Legii nr. 100/2017 cu privire la actele normative, de către Centrul de Armonizare a Legislației. Prin urmare, menținerea compatibilității cu cadrul juridic al UE este verificată și garantată prin mecanismele naționale de expertizare, având în vedere că măsura propusă constituie o derogare legitimă care ține de asigurarea securității și ordinii publice. Mai mult, propunerile de completare a Legii comunicațiilor electronice nr. 72/2025, nu creează careva neconcordanțe cu Codul european al comunicațiilor electronice și a actelor relevante ale Uniunii Europene și nu afectează transpunerea actului UE în legislația națională.
CENTRUL NAȚIONAL ANTICORUPȚIE (Aviz nr. ELO26/11429 din 06.05.2026)	1.	Prin proiect se propune reglementarea modalității de identificare a utilizatorilor serviciilor de comunicații electronice mobile accesibile publicului. Astfel, în condițiile normei legale, furnizorii de servicii de comunicații electronice mobile accesibile publicului sunt obligați să identifice utilizatorii 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. În nota de fundamentare autorul menționează că: „Proiectul actului normativ a fost elaborat din proprie inițiativă de către Ministerul Afacerilor Interne, cu scopul de a soluționa un vid legislativ (o lacună normativă) critic pentru securitatea statului. Intervenția a fost impusă de necesitatea curmării accesului neîngrădit și anonim la cartelele SIM preplătite, care, în perioada anilor 2020-2025, s-a transformat dintr-o vulnerabilitate administrativă într-un instrument logistic de bază exploatat pe scară largă pentru crima organizată transfrontalieră, fraude informatice, escrocherii, alerte false cu bombă la infrastructuri critice și coordonarea de la distanță a echipamentelor cu dublă destinație (ex: drone implicate în contrabandă). Totodată, proiectul aliniază	**Se acceptă.**

		standardele de siguranță națională la eforturile generale de integrare a Republicii Moldova în Piața Unică Digitală a Uniunii Europene". Cu referire la „Impactul financiar și argumentarea costurilor estimative" autorul descrie informații detaliate în acest sens în nota de fundamentare. În final, menționăm că, în redacția propusă, proiectul nu conține factori și riscuri de corupție	
MINISTERUL JUSTIȚIEI (Aviz nr. 04/2-5654 din 22.05.2026)	1.	Ministerul Justiției a examinat proiectul de lege pentru modificarea Legii comunicațiilor electronice nr. 72/2025 (număr unic 196/MAI/2026) și comunică următoarele. Proiectul de act normativ propune completarea Legii comunicațiilor electronice nr. 72/2025 (în continuare – Legea nr. 72/2025), cu art. 125^1 , care instituie obligația identificării utilizatorilor de servicii mobile accesibile publicului. Potrivit notei de fundamentare, temeiul legal al intervenției rezidă în obligația statului de a asigura ordinea și securitatea publică. Astfel, la nivelul drepturilor fundamentale și protecției datelor cu caracter personal, intervenția se fundamentează pe art. 6 alin. (1) lit. c) și art. 23 alin. (1) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), precum și pe dispozițiile specifice ale Directivei ePrivacy. Aferent redacției proiectului se expun următoarele observații și propuneri. Cu titlu general, proiectul legii instituie obligații generale de identificare a tuturor utilizatorilor serviciilor mobile accesibile publicului, inclusiv a cartelelor preplătite. Astfel, se prevăd colectări de nume, prenume, acte de identitate, IDNP, ș.a. Această abordare reprezintă o ingerință semnificativă în dreptul la viața privată și protecția datelor cu caracter personal, deoarece transformă accesul la un serviciu de comunicații într-un proces de comunicare sistematică și obligatorie. Din această perspectivă, se consideră necesare stabilirea unor norme explicite, clare și previzibile, care să nu	**Se acceptă parțial.** Proiectul de lege a fost elaborat pentru a asigura un echilibru între asigurarea securității publice și protecția drepturilor fundamentale (*viața privată și protecția datelor cu caracter personal*), integrând deja normele explicite, garanțiile și limitările solicitate, în deplină corespundere cu art. 23 și art. 54 din Constituția Republicii Moldova, precum și cu Legii nr. 195/2024 privind protecția datelor cu caracter personal (*în vigoare din 23.08.2026*). Obligația de identificare instituită, fiind limitată strict la colectarea datelor de identitate la momentul activării (*fără a reține date de trafic, conținut sau localizare a comunicațiilor*), constituie o ingerință „*limitată*". Legalitatea și proporționalitatea acestui regim de identificare au fost validate definitiv în favoarea securității statului de Curtea de Justiție a Uniunii Europene (*cauza Ministerio Fiscal, 2018*) și de Curtea Europeană a Drepturilor Omului (*cauza Breyer c. Germaniei, 2020*), instanțele statuând că aceasta este o măsură necesară într-o societate democratică, proporțională cu scopul combaterii criminalității și care nu constituie o imixtiune „gravă" în viața privată. Această abordare corespunde pe deplin criteriilor prevăzute de art. 54 alin. (2) din Constituția Republicii Moldova, care admite restrângerea drepturilor în interesele securității naționale, ordinii publice și prevenirii infracțiunilor. Proiectul integrează norme clare și predictibile care limitează prelucrarea datelor cu caracter personal la minimul absolut necesar: Proiectul definește o listă exhaustivă, strictă și limitativă a datelor prelucrate (*nume, prenume, IDNP / datele actului de identitate*), fără a permite extinderea nejustificată a acestora, respectând astfel cerințele Legii nr. 195/2024. Obligația de stocare este strict și clar limitată în timp. Datele sunt păstrate doar pe durata utilizării serviciului și o perioadă de exact 12 luni de la încetarea utilizării numărului de telefon (*noul art. 125^1*

		aducă atingere Legii nr. 195/2024 privind protecția datelor cu caracter personal (în vigoare din 23.08.2026), precum și art. 23 și 54 din Constituție. Or, normele se vor stabili astfel încât să se asigure proporționalitatea între necesitatea includerii obligației de identificare a tuturor utilizatorilor serviciilor mobile accesibile publicului și asigurarea protecției datelor cu caracter personal. Totodată, asemenea măsuri trebuie să mențină un just echilibru între interesul public și drepturile fundamentale ale persoanei. În lipsa unor garanții suficiente, limitări clare, stabilirea unor mecanisme de control, reguli precise de păstrare și acces, normele prevăzute în proiectul de lege riscă să fie percepute ca instituind un regim de identificare generalizată incompatibil cu protecția datelor cu caracter personal și al vieții private.	*alin. (5)*). Acesta este un prag minim necesar pentru a asigura trasabilitatea investigației infracțiunilor. Pentru a evita riscul creării unui „*regim de identificare generalizată incompatibil cu protecția datelor*”, proiectul adoptă arhitectura „*Digital First*” (*Opțiunea D*). Aceasta elimină complet vulnerabilitatea colectării și copierii fizice a actelor de identitate în cele peste 3.700 de puncte de vânzare terțe nespecializate (*stații PECO, chioșcuri, oficii poștale*) de către personal neinstruit. Identificarea cetățenilor rezidenți se va realiza strict automatizat și digital, prin interogarea Sistemului informațional „Registrul de stat al populației”, intermediată de platforma securizată MConnect, care asigură criptarea transmisiunilor și jurnalizarea (MLog) fiecărei accesări, prevenind tehnic accesul neautorizat și furtul de identitate. Furnizorii de comunicații electronice rămân, în sensul deplin al Legii nr. 195/2024, operatori de date. Introducerea soluțiilor tehnologice de identificare la distanță (eKYC, biometrie) nu creează un regim derogatoriu, ci le impune acestora obligația legală imperativă de a implementa măsuri tehnice și organizatorice adecvate pentru securitatea informației, de a efectua o Evaluare a Impactului asupra Protecției Datelor (DPIA) și de a consulta în prealabil autoritatea de supraveghere (CNPDCP) pentru prevenirea oricăror riscuri, obligații ce derivă nemijlocit din cadrul normativ general privind protecția datelor datelor cu caracter personal.
	2.	În continuare, se expun cele mai relevante observații asupra proiectului de lege, atât din punct de vedere conceptual, cât și din punct de vedere al tehnicii legislative, întru îmbunătățirea calității acestuia. Având în vedere faptul că prin proiect se propune completarea Legii nr. 72/2025 doar cu art. 125^1 , denumirea proiectului de lege va prevedea nemijlocit acest fapt. Potrivit proiectului, art. 125^1 – „Identificarea utilizatorilor serviciilor de comunicații electronice mobile accesibile publicului” se propune a fi inclus în capitolul XVIII - „Protecția confidențialității în domeniul comunicațiilor electronice”. În acest context, se atestă că obiectul de reglementare a art. 125^1 nu se circumscrie obiectului de reglementare a capitolului XVIII. Or, acestea au conotații diametral opuse.	**Se acceptă.** Totodată, urmare a consensului atins cu Ministerul Justiției privind încadrarea normei în obiectul de reglementare al Capitolului XVIII, s-au operat următoarele ajustări conceptuale: Denumirea articolului a fost modificată în: „***Articolul 125¹.*** *Identificarea utilizatorilor serviciilor de comunicații electronice mobile accesibile publicului și protecția confidențialității datelor.*” Aceste ajustări demonstrează esența normei ca fiind un proces de prelucrare a datelor cu caracter personal. Coroborat cu norma-cadru a art. 114 alin. (1) și (2) din lege (care vizează expres „prelucrarea datelor cu caracter personal în domeniul comunicațiilor”), noul articol se integrează organic în Capitolul XVIII, nefiind necesară divizarea sau mutarea sa într-un capitol distinct.

	3.	În textul art. 125[1] se atestă utilizarea cuvintelor „cartelă preplătită”. Astfel, pentru înțelegerea justă a reglementărilor, se va analiza oportunitatea definirii acestui termen.	**Nu se acceptă.** Conform normelor și recomandărilor privind tehnica legislativă, actul normativ nu este un dicționar juridic. Definirea noțiunilor se justifică doar în cazul în care, la momentul adoptării actului, se știe cu certitudine că un anumit termen este pasibil de mai multe interpretări sau dacă i se atribuie un sens juridic specific, diferit de cel uzual. Sintagma „*cartelă preplătită*” este un termen cu un sens clar, de largă circulație și general înțeles atât de publicul larg, cât și în limbajul de specialitate al comunicațiilor electronice (desemnând instrumentul prin care plata pentru servicii se face în avans). Această noțiune nu este susceptibilă de a fi interpretată echivoc în contextul aplicării legii. Din aceste considerente, introducerea unei definiții suplimentare ar încărca inutil textul actului normativ.
	4.	În alin. (2) pct. 1), se va analiza necesitatea textului „ , datele actului de identitate (denumirea, seria, numărul)”, în măsura în care se solicită inclusiv prezentarea IDNP-ului. Or, funcția de identificare este deja realizată prin IDNP. Menționăm că IDNP-ul reprezintă un identificator unic, permanent și individual atribuit fiecărei persoane fizice. Spre deosebire de seria și numărul actului de identitate, care se pot modifica odată cu expirarea sau înlocuirea documentului, IDNP-ul rămâne neschimbat pe toată durata vieții persoanei. Prin urmare, solicitarea numelui, prenumelui și IDNP-ul persoanei permite identificarea exactă și neechivocă a persoanei, fără a mai fi necesară indicarea altor elemente identificabile din actul de identitate. Totodată, constatăm că Legea nr. 72/2025, în art. 125 alin. (2) pct. 3) lit. b), stabilește deja identificarea abonaților doar prin numele, prenumele, IDNP și adresa abonatului.	**Nu se acceptă.** Solicitarea datelor actului de identitate (denumirea, seria, numărul) alături de IDNP nu este o cerință redundantă, ci o garanție tehnică și juridică indispensabilă pentru verificarea autenticității persoanei și prevenirea furtului de identitate. Conform noului art. 125[1] alin. (2) pct. 1) din proiect, obligația furnizorului nu se rezumă la simpla colectare declarativă a datelor, ci impune ca acesta să verifice „*datele și valabilitatea acestuia (actului de identitate) cu interogarea Sistemului informațional (Registrul de stat al populației)*”. Simpla cunoaștere a unui IDNP nu permite sistemelor să confirme dacă documentul efectiv prezentat fizic sau digital la momentul activării este valid, dacă este expirat, anulat sau declarat pierdut/furat. Fără preluarea datelor actului (seria/numărul), interogarea privind starea documentului este imposibilă. IDNP-ul, deși este unic și permanent pe durata vieții, este o informație care poate fi compromisă sau aflată relativ ușor de către terți. Dacă identificarea s-ar limita exclusiv la nume și IDNP, orice persoană rău-intenționată ar putea activa cartele SIM pe numele altor cetățeni, generând baze de date cu identități false. Solicitarea datelor actului de identitate și confruntarea lor (*inclusiv prin mijloace eKYC la distanță, care prevăd expres „verificarea identității persoanei fizice în baza actelor de identitate prezentate”*) reprezintă un filtru de securitate ce neutralizează posibilitatea înregistrărilor abuzive fără știrea persoanei vizate. Articolul 125 reglementează exclusiv datele de trasabilitate care trebuie reținute și prezentate organelor de drept la solicitare (unde

			numele, IDNP-ul și adresa sunt suficiente pentru a indica subiectul vizat). În schimb, noul art. 125[1] reglementează procesul activ de cunoaștere și validare a clientului (KYC - Know Your Customer) în momentul încheierii contractului sau activării cartelei. La această etapă prealabilă, verificarea elementelor identificabile ale unui document emis de stat este singura cale de a stabili cu certitudine că persoana care solicită serviciul este cu adevărat titularul de drept.
	5.	Cu referire la alin. (2) pct. 2), care prevede reținerea copiei actului de identitate pentru persoanele fizice care se identifică cu acte de identitate emise de alte state, menționăm că legislația în vigoare, în special Legea privind protecția datelor cu caracter personal nr. 195/2024, nu reglementează condițiile în care poate fi reținută copia actului de identitate. Mai mult, dispoziția acestui punct se va revedea și prin prisma principiului nediscriminării, prevăzut în art. 97 al Legii nr. 72/2025, care prevede că furnizorii de rețele sau de servicii de comunicații electronice nu pot aplica utilizatorilor finali din Republica Moldova și din statele membre ale Uniunii Europene cerințe sau condiții generale diferite în ceea ce privește accesul la rețele sau servicii ori utilizarea acestora din motive legate de cetățenia, statul de reședință sau de amplasarea sediului utilizatorului final, cu excepția cazurilor în care un astfel de tratament diferit este justificat în mod obiectiv. Totodată, potrivit art. 98 alin. (2) al aceleiași legi, orice măsuri privind accesul utilizatorilor finali la servicii și la aplicații sau privind utilizarea acestor servicii și aplicații de către utilizatorii finali prin intermediul rețelelor de comunicații electronice, care ar putea restrânge exercitarea drepturilor sau libertăților recunoscute de Convenția europeană pentru apărarea a drepturilor omului și a libertăților fundamentale și de Constituția Republicii Moldova, sunt impuse numai dacă sunt prevăzute de lege și respectă drepturile sau libertățile în cauză, sunt proporționale, necesare și răspund efectiv unor obiective de interes general, recunoscute de lege sau necesității de a proteja drepturile și libertățile celorlalți în conformitate cu art. 18 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale și cu art. 54 din Constituția Republicii Moldova (observație similară valabilă și pentru alin. (2) pct. 4)).	**Nu se acceptă.** Privind principiul nediscriminării (art. 97 din Legea nr. 72/2025) și al proporționalității (art. 98 alin. (2) și art. 54 din Constituție), tratamentul diferențiat aplicat persoanelor rezidente comparativ cu cele nerezidente este justificat în mod obiectiv de posibilitățile tehnice de validare a identității. Proiectul de lege interzice și exclude obligația reținerii copiilor actelor de identitate pentru cetățenii și persoanele juridice din Republica Moldova, deoarece identificarea și validarea acestora se realizează direct, automatizat și sigur prin interogarea Registrului de stat, prin intermediul platformei guvernamentale MConnect. În schimb, în cazul persoanelor fizice și juridice din alte state (reglementate la alin. (2) lit. b și d), statul nu deține acces la registrele altor țări pentru a le verifica datele electronic. În lipsa posibilității de validare electronică la distanță, reținerea copiei actului de identitate sau a documentului de înregistrare pentru nerezidenți reprezintă singura modalitate tehnică și juridică viabilă de a asigura trasabilitatea reală a utilizatorului, aceasta fiind o condiție cerută de organele de drept. Excluderea acestei cerințe ar genera o lacună de securitate, permițând eludarea obligației de identificare prin utilizarea unor acte străine ce ar fi imposibil de verificat ulterior. Astfel, măsura constituie un mijloc strict necesar, limitat și proporțional cu obiectivul de asigurare a ordinii și securității publice. Faptul că proiectul de lege menționează că reținerea copiei actului de identitate se face „*în condițiile legislației privind protecția datelor cu caracter personal*” este intenționat și constituie o garanție legală fermă. Această trimitere obligă direct operatorul ca, în procesul de păstrare a acestor copii, să aplice toate standardele stricte de securitate, confidențialitate și limitare a stocării (*strict pe durata utilizării numărului și 12 luni după dezactivare*) impuse de Legea nr. 195/2024. Excluderea acestei precizări tocmai că ar genera un vid de garanții juridice.

			Mai mult, reținerea copiei actului exclusiv pentru cetățenii străini a fost agreată ca o necesitate operațională în urma consultărilor cu mediul de afaceri, în speță Asociația Națională a Companiilor din Domeniul TIC (ATIC), fiind asumată ca un compromis optim pentru a face legea aplicabilă și utilă procesului de investigare a infracțiunilor transfrontaliere.
	6.	Subsecvent, în alin. (2) pct. 4): - cuvântul „furnizorul” se va substitui cu cuvintele „furnizorul de servicii de comunicații electronice mobile accesibile publicului”, iar după cuvântul „înregistrarea” se va completa cu cuvintele „persoanei juridice în registrul comercial al statului străin”, în vederea clarității normei, precum și a utilizării unei terminologii uniforme în tot textul legii (observații valabile în tot textul proiectului, cu referire la termenul „furnizor”);	**Se acceptă.**
	7.	- aferent solicitării traducerii legalizate în limba română a documentului care atestă înregistrarea persoanei juridice în registrul comercial al statului străin, acest aspect poate constitui din punct de vedere juridic un impediment disproporționat și nejustificat pentru obținerea unei cartele de telefonie mobilă. Or, orice condiție administrativă impusă pentru accesul la un serviciu trebuie să fie adecvată scopului urmărit, necesară și proporțională. În acest sens, dacă scopul operatorului este doar identificarea persoanei juridice, existența documentului oficial emis de registrul comercial străin este, în sine, aptă să confirme existența juridică a societății, denumirea, numărul de înregistrare, ș.a. Impunerea suplimentară a unei traduceri legalizate ar complica excesiv procedura, ar genera costuri suplimentare, precum și ar prelungi termenul de acces la serviciu. De asemenea, aceasta poate contraveni principiilor promovate de Uniunea Europeană în materia libertății prestării de servicii și a libertății de a furniza servicii. Astfel, sub aspect comparativ, Legea nr. 282/2024 privind libertatea de stabilire a prestatorilor de servicii și libertatea de a furniza servicii (în vigoare din 1 ianuarie 2030, care a transpus Directiva 2006/123/CE a Parlamentului European și a Consiliului din 12 decembrie 2006 privind serviciile în cadrul pieței interne), prevede în art. 5 alin. (3) că „În cazul în care o autoritate competentă solicită ca prestatorul ori beneficiarul să prezinte un certificat, o atestare sau un alt document pentru a dovedi că	**Se acceptă.**

		o anumită cerință a fost îndeplinită, aceasta acceptă orice document dintr-un stat membru întocmit într-un scop echivalent sau din care reiese clar că cerința respectivă este îndeplinită. Autoritățile competente nu pot solicita prezentarea unui document emis într-un stat membru în original, în copie certificată pentru conformitate sau traducere certificată, cu excepția cazurilor prevăzute de alte acte normative care transpun acte ale UE ori creează cadrul pentru aplicarea directă a regulamentelor sau a cazurilor în care o astfel de cerință este justificată printr-un motiv imperativ de interes general.”. Mai mult, nota de fundamentare nu conține argumentele care să justifice necesitatea unei traduceri legalizate în limba română a documentului ce atestă înregistrarea persoanei juridice în registrul comercial al statului străin.	
	8.	În alin. (3) pct. 2), nu este clar ce semnifică cuvintele „persoanelor împuternicite de furnizor”, or, în forma expusă, lasă loc de interpretare și aplicare necorespunzătoare a normei. Astfel, această formulare lasă furnizorului o marjă excesivă de apreciere, ceea ce contravine principiului previzibilității normei, derivat din dispozițiile art. 23 din Constituție. Astfel, din conținutul normei propuse se poate înțelege că furnizorul de servicii de comunicații electronice mobile accesibile publicului poate împuternici prin contract orice persoană, inclusiv orice vânzător din puncte comerciale terțe nespecializate (chioșcuri, stații PECO) de a efectua identificarea utilizatorilor la momentul comercializării cartelelor de telefonie mobile. În acest context, pentru evitarea unor împuterniciri abuzive se vor stabili ce persoane pot fi împuternicite de furnizor (statutul lor, cerințe de calificare profesională, deținerea unor competențe specifice activității prelucrării datelor cu caracter personal) și condițiile acestor împuterniciri (standarde de securitate, obligații de confidențialitate, mecanisme de control a acestor persoane). De asemenea, sintagma „alt temei juridic corespunzător” este imprecisă și generală. Or, norma nu indică, ce fel de act juridic poate constitui un asemenea temei, cine îl emite și care sunt condițiile minime de validitate a unui asemenea act. Mai mult, se va reține că, reglementările primare se stabilesc în legi.	**Se acceptă.** Pentru a exclude riscul unor delegări abuzive, propunerea a fost acceptată prin completarea proiectului cu o trimitere expresă la legea-cadru, alin. (3) pct. 2) se expune în următoarea redacție: „*2) în punctele de vânzare ale persoanelor împuternicite de operator, astfel cum sunt definite în art. 4 al Legii nr. 195/2024 privind protecția datelor cu caracter personal, în baza unui contract sau a unui alt temei juridic corespunzător;*” La detalierea cerințelor de securitate și control, aceste exigențe derivă deja imperativ din legislația privind protecția datelor. Conform acesteia, delegarea sarcinii nu eliberează operatorul de răspundere, iar orice eroare sau utilizare ilicită a datelor de către persoana împuternicită atrage răspunderea directă a furnizorului de comunicații. Suplimentar, trecerea la modelul „*Digital First*” exclude din start colectarea datelor de către personal neinstruit în cele peste 3.700 de puncte comerciale nespecializate. Vânzarea cartelelor este decuplată de activare, iar identificarea se va realiza exclusiv într-un mediu securizat (digital sau în magazinele oficiale ale furnizorului și ale persoanelor împuternicite de acesta).

		Mai mult, extinderea cercului persoanelor care pot efectua identificarea utilizatorului, inclusiv, în baza unui „alt temei juridic corespunzător”, amplifică riscul scurgerii datelor, riscul furtului de identitate și accesului neautorizat la date personale. Or, potrivit principiilor de protecție a datelor cu caracter personal, accesul la asemenea operațiuni trebuie limitat și strict reglementat de lege. De asemenea, norma nu delimitează clar răspunderea furnizorului de răspunderea persoanei împuternicite în cazul unor identificări eronate de către persoana împuternicită sau a utilizării frauduloase a datelor de către aceasta. În lipsa unor asemenea garanții, norma riscă să permită delegarea excesivă a unei activități sensibile ce presupune identificarea datelor cu caracter personal ale utilizatorilor de telefonie mobilă.	
	9.	La alin. (3) pct. 3): Menționăm că utilizarea Sistemului informațional „Registrul de Stat al populației” la identificarea persoanei fizice este aplicabilă doar în cazul persoanelor fizice rezidente, nu și în cazul persoanelor străine. Prin urmare, norma stabilită la lit. b) se va reformula. În dispoziția lit. c), textul „subpunctele 1)-3)” sugerăm a fi substituit cu textul „subpct. 1) și 2), precum și la lit. a) și b)”.	**Se acceptă.**
	10.	În alin. (4): - cuvintele „care urmează a fi” se vor exclude, ca fiind inutile;	**Se acceptă.**
	11.	- se va stabili concret la ce „autoritate de reglementare” se face referire. Astfel, aceste cuvinte urmează a fi substituite cu cuvintele „autoritatea națională de reglementare în domeniul comunicațiilor electronice” sau cu cuvântul „Agenție”. Totodată, considerăm oportun a se prevedea denumirea concretă a actului prin care se vor stabili serviciile tehnice minime necesare utilizate până la finalizarea procesului de identificare a cartelelor SIM/eSIM”, astfel încât norma dată să constituie temei juridic pentru adoptarea actului normativ în cauză. De asemenea, denumirea concretă a actului se va indica și în art. II alin. (2) al proiectului de lege.	**Se acceptă.**

	12.	Dispoziția alin. (5) se recomandă a fi exclusă, deoarece face trimitere la norme deja existente și este lipsit de densitate normativă. Or, norma prevăzută la art. 125 alin. (3) al Legii nr. 72/2027 este aplicabilă inclusiv pentru furnizorii de servicii de comunicații electronice mobile accesibile publicului.	**Nu se acceptă.** Norma invocată din art. 125 al Legii nr. 72/2025 reglementează obligațiile de reținere pentru datele tehnice de trasabilitate (date de trafic, de localizare, echipament) generate pe parcursul prestării serviciului. În contrast, noul art. 125[1] alin. (5) are ca obiect de reglementare exclusiv datele de identitate prelucrate la momentul identificării prealabile a utilizatorului (procedura KYC) și protecția confidențialității datelor. Orice prelucrare de date cu caracter personal trebuie să respecte principiul „*reducerii la minimum a datelor*” (Regulamentul (UE) 2016/679 și art. 5 alin. (1) lit. c) Legea nr. 195/2024). Fixarea prin alin. (5) a perioadei de retenție (*pe întreaga durată de utilizare a serviciului și exact 12 luni de la încetarea utilizării numărului*) oferă o garanție juridică fundamentală, reprezentând pragul minim proporțional necesar pentru a asigura trasabilitatea în cazul investigațiilor. Excluderea alin. (5) ar lăsa neacoperit termenul legal de păstrare a datelor prelucrate exclusiv în contextul înregistrării și identificării utilizatorilor de cartele preplătite. Trimiterea de la finalul alin. (5) la art. 125 alin. (3) are rolul de a corela și de a uniformiza regimul de stocare a identității cu termenele de retenție a datelor tehnice existente în lege, asigurând coerența actului normativ.
	13.	Suplimentar la art. I, diviziunile alin. (2) recomandăm a fi însemnate prin litere, în corespundere cu art. 51 alin. (6) al Legii nr. 100/2017 cu privire la actele normative.	**Se acceptă.**
	14.	La art. II: Dispozițiile alin. (1), ce vizează intrarea în vigoare a actului normativ se recomandă a fi divizate de cele ce prevăd aplicabilitatea actului normativ, fiind expuse în alineate distincte.	**Se acceptă.**
	15.	În alin. (2): - după cuvântul „Autoritatea” se va include cuvântul „națională”, în scopul asigurării utilizării unei terminologii uniforme în tot textul legii;	**Se acceptă.** Pentru a respecta cu strictețe terminologia legii de bază, în loc de a adăuga cuvântul „*națională*”, textul de la art. II alin. (2) va fi ajustat prin substituirea sintagmei „*Autoritatea de reglementare în domeniul comunicațiilor electronice*” direct cu cuvântul „*Agenția*”. În conformitate cu dispozițiile art. 7 alin. (1) din Legea nr. 72/2025, autoritatea învestită cu competențe de reglementare, monitorizare și control al activităților din domeniu este definită expres ca fiind „*Agenția*”.

	16.	- textul „menționate la art. 125[1] alin. (4)” se vor substitui cu textul „menționate la art. I, în partea ce vizează redacția art. 125[1] alin. (4) al Legii comunicațiilor electronice nr. 72/2025”;	**Se acceptă.**
	17.	- se recomandă completarea acestui alineat cu dispoziția care ar prevedea aducerea actelor normative ale autorității naționale de reglementare în domeniul comunicațiilor electronice în conformitate cu respectiva lege.	**Se acceptă.**

Ministru **Daniella MISAIL-NICHITIN**