

NOTA DE FUNDAMENTARE
la proiectul de lege pentru completarea cu
articolul 125¹ a Legii comunicațiilor electronice nr. 72/2025

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ
<i>Autorul proiectului:</i> 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 salvagardare” 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. 125¹), 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 (chioscuri, 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 intenționate 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 ilicite.

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 125¹, 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 salvagardare” 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 permissive 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 – 125¹ – 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 (chioscuri, 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 electronice, 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 inefficientă, 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 agreeat „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 intenționate 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 ținut.

Alertele false la adresa infrastructurilor critice (ex: Aeroportul Internațional „Eugen Doga”) paralizază 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 interelare. 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 (chioscuri, 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 pereclitează 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 salvagardare” 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 suspectilor. 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 (CNPDPCP) 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 agreeat 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. 125¹), 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