



AmCham Moldova
fighting for your business



Către: Daniella MISAIL-NICHITIN
Ministra Afacerilor Interne

Copie: Eugen OSMOCHESCU
Viceprim-ministru, Ministrul Dezvoltării Economice și Digitalizării

Nr. 12 din 10 februarie 2026

Ref.: Proiectul de lege pentru modificarea Legii comunicațiilor electronice nr. 72/2025

Stimată Doamnă Ministră,

Vă salutăm din numele Asociației Patronale „Camera de Comerț Americană din Moldova” (AmCham Moldova) și Asociației Naționale a Companiilor din sectorul TIC (ATIC), organizații reprezentative pentru furnizorii de servicii de comunicații electronice.

Prin prezenta, asociațiile își exprimă profunda preocupare în legătură cu intenția Ministerului Afacerilor Interne de a impune furnizorii să îi acorde acces direct la datele de localizare ale abonaților de comunicații mobile.

Recent, pe pagina www.particip.gov.md a fost publicat anunțul de inițiere a procesului de elaborare a proiectului de lege pentru modificarea Legii comunicațiilor electronice nr. 72/2025¹. Scopul anunțat al proiectului este modernizarea cadrului legal privind accesul autorităților competente la datele de localizare în cazurile de infracțiuni grave și dispariții de persoane, inclusiv ale minorilor, prin instituirea unui mecanism securizat, standardizat și supus controlului judiciar. Proiectul ar urmări facilitarea intervenției rapide a autorităților, **prin acces direct** și autorizat **la datele de localizare**, cu respectarea drepturilor fundamentale și alinierea la bunele practici internaționale.

Această inițiativă reprezintă o măsură disproporționată, care ar încălca dreptul la viața privată a cetățenilor.

Conform art. 28 din Constituție, statul respectă și ocrotește viața intimă, familială și privată. Articolul 54 alin. (2) și (4) din Constituție stabilește că exercițiul drepturilor și libertăților nu poate fi supus altor restrângeri decât celor prevăzute de lege, care corespund normelor unanim recunoscute ale dreptului internațional și sunt necesare în interesele securității naționale, integrității teritoriale, bunăstării economice a țării, ordinii publice, în scopul prevenirii tulburărilor în masă și infracțiunilor, protejării drepturilor, libertăților și demnității altor persoane, împiedicării divulgării informațiilor confidențiale sau

¹ <https://particip.gov.md/ro/document/stages/proiectul-de-lege-pentru-modificarea-legii-comunicatiilor-electronice-nr722025/15981>

garantării autorității și imparțialității justiției. Restrângerea trebuie să fie proporțională cu situația care a determinat-o și nu poate atinge existența dreptului sau a libertății.

Articolul 8 din Convenția pentru apărarea Drepturilor Omului și a Libertăților fundamentale, de asemenea, prevede că orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului său și a corespondenței sale. Nu este admis amestecul unei autorități publice în exercitarea acestui drept decât în măsura în care acesta este prevăzut de lege și constituie, într-o societate democratică, o măsură necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protecția sănătății, a moralei, a drepturilor și a libertăților altora.

Acordarea posibilității ca MAI să acceseze de sine stătător metadatele stocate la furnizori generează riscul accesului neautorizat și utilizării abuzive a informațiilor cetățenilor care nu au vreo legătură cu activități criminale. Faptul că, formal, accesul va fi supus controlului judiciar² nu împiedică MAI să acceseze asemenea informații pe ascuns, fără autorizarea judecătorului.

În hotărârile sale pe dosarele Digital Rights Ireland³ și Tele2 Sverige⁴, Curtea de Justiție a Uniunii Europene a reținut că o gamă nelimitată de subiecți ai reținerii datelor echivalează cu o încălcare a principiilor strictei necesități și proporționalității. Instanța a subliniat că, deși nu dezvăluie conținutul comunicărilor, metadatele permit să se tragă concluzii precise și intime despre viața unei persoane, iar obiectivul combaterii infracțiunilor grave nu poate justifica o intervenție atât de intruzivă în viața privată a cetățenilor care nu au vreo legătură cu activități criminale. Curtea a precizat fără ambiguitate că, pe lângă faptul că trebuie să vizeze subiecți selectați pe baza unor criterii rezonabile și a unor probe obiective, un regim proporțional de reținere și acces al datelor trebuie să ofere garanții suficiente împotriva utilizării abuzive a datelor⁵.

² Este de menționat faptul că, informația aferentă la „locația echipamentului de comunicații mobile de la începutul comunicației” potrivit art. 1384 alin. (1) lit. h) din Codul de Procedură Penală, , se atribuie măsurii speciale de investigație colectarea informației, care se realizează cu autorizarea judecătorului de instrucție în conformitate cu prevederile art. 134 alin. (1), pct. 1) lit. f) al CPP.

³ [C-0293-12-00000000RP-01-P-01 ARRET 150642-RO-1](#)

⁴ [C-0203-15-00000000RP-01-P-01 ARR COMM 188001-RO-1](#)

⁵ Hotărârea CJUE în cauza Ireland Digital Rights:

54. Astfel, reglementarea Uniunii în cauză trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună o serie de cerințe minime astfel încât persoanele ale căror date au fost păstrate să dispună de garanții suficiente care să permită protejarea în mod eficient a datelor lor cu caracter personal împotriva riscurilor de abuz, precum și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date (a se vedea prin analogie, în ceea ce privește articolul 8 din CEDO, Hotărârea Curții EDO din 1 iulie 2008, Liberty și alții împotriva Regatului Unit, nr. 58243/00, § 62 și 63, Hotărârea Rotaru împotriva României, citată anterior, § 57-59, precum și Hotărârea S și Marper împotriva Regatului Unit, citată anterior, § 99).

59. Pe de altă parte, deși urmărește să contribuie la combaterea criminalității grave, directiva menționată nu impune existența unei relații între datele a căror păstrare este prevăzută și o amenințare pentru siguranța publică și în special aceasta nu se limitează la păstrarea fie a unor date aferente unei perioade temporale și/sau unei zone geografice determinate și/sau unui cerc de persoane determinate care ar putea fi implicate, într-un mod sau altul, în săvârșirea unei infracțiuni grave, fie a unor date referitoare la persoane care ar putea contribui, pentru alte motive, prin păstrarea datelor lor, la prevenirea, la detectarea sau la urmărirea penală a infracțiunilor grave.

Observăm că o inițiativă similară de a acorda SIS acces direct la metadatele stocate la furnizori a fost respinsă de Parlament ca urmare a opiniei negative a Comisiei de la Veneția⁶:

„54. În ceea ce privește culegerea de informații de la furnizorii de comunicații electronice, prevederea permite o putere nelimitată de a accesa tot felul de comunicații electronice, cu sau fără asistența operatorului. De asemenea, SIS nu numai că își stabilește propriile sisteme informatice, ci are și dreptul de a accesa în general, în mod gratuit, sistemele informaționale, rețelele de comunicații electronice, resursele informaționale și bazele de date ale organelor de drept, autorităților publice, întreprinderilor, instituțiilor și organizațiilor, indiferent de proprietatea acestora. Este de remarcat faptul că, deși această măsura necesită un mandat judiciar, dacă SIS ar fi în poziția de a o efectua fără asistența unui operator, nu ar exista absolut nicio entitate care să constate existența reală a mandatului judiciar. În plus, nu există nicio prevedere ca furnizorii particulari de servicii să conteste sau să atace ordinul de predare a datelor abonaților. Aceste prevederi par a fi în mod clar disproporționate. În comentariile lor, autoritățile au informat că intenționează să precizeze în proiectul de prevedere că accesul se referă doar la sistemele informaționale și bazele de date create și gestionate de stat, astfel încât să excludă sistemele informaționale private ale companiilor [...]”

În afară de cele expuse mai sus, menționăm că sistemele furnizorilor în care sunt stocate metadatele sunt dimensionate pentru un număr foarte limitat de căutări simultane. Supraîncărcarea acestor sisteme prin efectuarea de către MAI a unui număr mare de căutări extensive simultane ar putea face inoperabile aceste sisteme critice și vitale pentru furnizori, perturbând serviciile furnizate.

În acest context, îndemnăm autoritățile să renunțe la această inițiativă, în vederea garantării reale a drepturilor cetățenilor la viața privată. Vă mulțumim.

Cu respect,

Mila Malairău
Director Executiv
AmCham Moldova

Irina Oriol
Director Executiv
ATIC

62. În special, Directiva 2006/24 nu prevede niciun criteriu obiectiv care să permită limitarea numărului de persoane ce dispun de autorizația de acces și de utilizare ulterioară a datelor păstrate la strictul necesar în lumina obiectivului urmărit. Mai ales, accesul la datele păstrate de autoritățile naționale competente nu este condiționat de un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă prin a căror decizie se urmărește limitarea accesului la date și a utilizării lor la ceea ce este strict necesar în vederea atingerii obiectivului urmărit și care este adoptată în urma unei cereri motivate a acestor autorități formulate în cadrul procedurilor de prevenire, de detectare sau de urmărire penală. În directivă nu s-a prevăzut nici o obligație precisă a statelor membre privind stabilirea unor astfel de limitări.

⁶ [Republic of Moldova - Opinion on the draft law on the Intelligence and Security Service, as well as on the draft law on counterintelligence and external intelligence activity - Venice Commission of the Council of Europe](#)