

Nr. 12  
Din 15 februarie 2023

**Domnului Igor GROSU,**  
**Președinte al Parlamentului RM**

**Domnului Lilian CARP,**  
**Președinte al Comisiei parlamentare securitate națională,**  
**apărare și ordine publică**

**Subiect:** Comentarii pe marginea pachetului de Legii nr. 420 privind Serviciul de Informații și Securitate al Republicii Moldova și nr. 422 privind activitatea contrainformativă și activitatea informativă externă

**Stimate Domnule Grosu,**  
**Stimate Domnule Carp,**

Vă salutăm din numele Asociației Naționale a Companiilor din Domeniul TIC ("ATIC") și Asociației Investitorilor Străini („FIA”).

Înțelegem și apreciem eforturile autorilor proiectelor de Legi menționate mai sus îndreptate spre minimizarea riscurilor și amenințărilor la adresa securității naționale a Republicii Moldova, prin reglementarea detaliată a atribuțiilor, obligațiilor și drepturilor SIS.

Totodată, dorim să atragem atenția dumneavoastră asupra unor prevederi din proiectele de Legi care trezesc îngrijorarea comunității de afaceri. Comentariile, propunerile și arumentele corespunzătoare le găsiți în anexa la prezenta adresare.

Remarcăm că aceste comentarii/propuneri și argumente au fost comunicate și către experții Comisiei de la Veneția, care au solicitat opinia mediului de afaceri cu privire la aceste proiecte. Mizăm pe faptul că autoritățile RM vor lua în considerare aceste comentarii și argumente la definitivarea proiectelor de legi în cauză.

De asemenea, Vă atragem atenția că unele prevederi contestate din proiectele de legi respective sunt dublate în proiectul de lege pentru modificarea Codului de Procedură Penală și Legii privind activitatea specială de investigații, aprobat recent de Parlament în primă lectură în regim prioritar: <https://justice.gov.md/ro/content/proiectul-de-lege-pentru-modificarea-unor-acte-normative-privind-activitatea-speciala-de-1>. (Avizul la Proiect se anexează). Astfel, acest proiect de lege ar trebui la rândul său să fie ajustat în mod corespunzător.

Vă mulțumim anticipat și rămânem la dispoziția DVS pentru orice întrebări legate de acest subiect.

**Cu deosebite considerațiuni,**

---

Marina Bzovii, Director Executiv, ATIC

---

Ana Groza, Director Executiv, FIA

**Anexă la Avizul nr. 12**  
**Din 15 februarie 2023**

Legea 420

Articol din proiect	Comentariu
<p><b>Articolul 8. Drepturile Serviciului</b></p> <p>(1) Serviciul are dreptul:</p> <p>4) să utilizeze următoarele bunuri, cu excepția celor ce aparțin misiunilor diplomatice și persoanelor cu imunitate diplomatică:</p> <p>a) în bază de contract <u>sau înțelegere verbală</u>, în limitele necesare pentru realizarea atribuțiilor ce-i revin, încăperile de serviciu, alte bunuri ale persoanelor juridice, ale formațiunilor militare, precum și încăperile și alte bunuri ale persoanelor fizice;</p> <p>d) în situații excepționale, precum și în cazul aplicațiilor planificate la nivel național sau de către Serviciu, în bază de contract <u>sau înțelegere verbală</u>, <u>pe gratis</u>, rețelele și serviciile de comunicații electronice ale furnizorilor, indiferent de tipul de proprietate al acestora. <u>La cererea furnizorilor, Serviciul le compensează, în modul stabilit de legislația civilă, cheltuielile sau prejudiciile cauzate;</u></p> <p>7) să solicite și să primească, <u>pe gratis</u>, de la autoritățile publice, alte persoane juridice, indiferent de tipul de proprietate, informații necesare pentru exercitarea atribuțiilor ce revin Serviciului. <u>Prezentarea informațiilor solicitate de Serviciu nu poate fi refuzată pe motiv că acestea constituie informații cu accesibilitate limitată;</u></p>	<p>La art. 8 alin. (1) pct. 4) lit. a), nu este definit clar cine stabilește dacă încăperile sau bunurile se oferă în bază de contract sau înțelegere verbală. Norma ar trebui să prevadă că încăperile sau bunurile <u>se oferă în bază de contract, dacă părțile nu au convenit altfel.</u></p> <p>La art. 8 alin. (1) pct. 4) lit. d), există o contradicție între textul care prevede că rețelele și serviciile de comunicații electronice ale furnizorilor sunt puse la dispoziția SIS pe gratis și textul care prevede dreptul furnizorilor de a cere compensarea cheltuielilor sau prejudiciului. De asemenea, nu este definit clar cine stabilește dacă rețelele se utilizează în bază de contract sau înțelegere verbală. Norma ar trebui să prevadă că <u>rețelele se utilizează în bază de contract, dacă părțile nu au convenit altfel, iar mențiunea “pe gratis” trebuie exclusă</u>, păstrând dreptul furnizorilor de a cere compensarea cheltuielilor sau prejudiciului.</p> <p>La art. 8 alin. (1) pct. 7), nu se face referință la necesitatea respectării procedurii de autorizare a obținerii informațiilor cu accesibilitate limitată, stabilite de lege. Or, art. 12 din prezenta lege stabilește că anumite informații, cum ar fi informația financiară sau identitatea abonatului, informația ce se află sau se prelucrează într-un sistem informațional, informația colectată de la furnizorii de servicii de comunicații electronice, se prezintă numai în baza autorizației directorului sau directorului adjunct special împuternicit al SIS sau în baza mandatului judecătoresc. Norma ar trebui să</p>

	<p>prevadă că prezentarea informațiilor solicitate de Serviciu nu poate fi refuzată pe motiv că acestea constituie informații cu accesibilitate limitată, <u>dacă a fost respectată procedura de autorizare a măsurii respective, stabilită de lege.</u></p>
<p><b>Articolul 11.</b> Cooperarea Serviciului cu instituții din țară și din străinătate</p> <p>4) Autoritățile publice, precum și alte <u>persoane juridice indiferent de tipul de proprietate, sînt obligate să acorde Serviciului, în limita posibilităților, asistență operațională, informațională, tehnică și de altă natură în vederea îndeplinirii atribuțiilor ce îi revin, inclusiv să ofere, funcții pentru detașarea ofițerilor de informații în vederea îndeplinirii unor atribuții în interesul securității naționale.</u></p>	<p>Această normă contravine art. 7 alin. (3), potrivit căruia <u>doar organele administrației publice centrale, subdiviziunile și instituțiile subordonate acestora</u> sunt obligate, la solicitare, să pună la dispoziție Serviciului funcții în care vor fi detașați ofițeri de informații în scopul realizării activității informative/contrainformative.</p> <p>În ceea ce privește obligația de a acorda asistență operațională, informațională, tehnică și de altă natură, această normă este foarte vagă, creând premise pentru solicitări abuzive din partea SIS (furnizorii s-au ciocnit anterior cu asemenea solicitări).</p> <p>Norma ar trebui să limiteze obligațiile respective la <u>organele administrației publice centrale, subdiviziunile și instituțiile subordonate acestora</u>, nu și la alte persoane juridice.</p>
<p><b>Articolul 27.</b> Asigurarea informațională a Serviciului</p> <p>(2) În interesul asigurării securității naționale, Serviciul, în modul stabilit de legislație, <u>are drept de acces, gratuit, la sistemele informaționale, rețelele de comunicații electronice, la resursele informaționale și bazele de date ale organelor de ocrotire a normelor de drept, autorităților publice, întreprinderilor, instituțiilor și organizațiilor, indiferent de tipul de proprietate.</u></p>	<p>Obligația de a acorda <u>acces, gratuit, în modul stabilit de legislație, la sistemele informaționale, rețelele de comunicații electronice, la resursele informaționale și bazele de date ale întreprinderilor, instituțiilor și organizațiilor, indiferent de tipul de proprietate</u> este foarte vagă, creând premise pentru solicitări abuzive din partea SIS. Pentru reducerea acestui risc, norma ar trebui să prevadă că accesul se acordă <u>în cazurile și în modul stabilit de prezenta lege.</u></p>

## Legea 422

<p><b>Articolul 7. Asistența acordată la efectuarea activității informative/contrainformative</b></p> <p>(1) Persoanele fizice și juridice, indiferent de forma de proprietate, <u>sînt obligate, în condițiile prezentei legi, să acorde asistența necesară Serviciului, să pună imediat, gratis la dispoziția acestuia informațiile solicitate, precum și, în măsura posibilității, bunuri mobile și imobile, alte obiecte și documente necesare pentru realizarea activității informative/contrainformative.</u></p> <p>(2) Prestatorii de servicii poștale și furnizorii de rețele și/sau servicii de comunicații electronice, indiferent de tipul de proprietate sunt obligați:</p> <p>1) să pună la dispoziție <u>spații, echipamente și condiții tehnice necesare pentru înfăptuirea de către Serviciu a măsurilor contrainformative sau informative externe și să prezinte, în acest scop, datele tehnice necesare;</u></p> <p>4) să asigure accesul liber și operativ al subdiviziunii specializate a Serviciului <u>la toate interfețele echipamentelor furnizorilor, la propriile rețele de comunicații electronice,</u> să asigure condițiile tehnice și datele necesare pentru conectarea mijloacelor tehnice speciale predestinate înfăptuirii măsurilor contrainformative sau informative externe;</p> <p>5) să asigure permanent și continuu condițiile tehnice necesare pentru conectarea și funcționarea mijloacelor tehnice speciale predestinate înfăptuirii măsurilor contrainformative sau informative externe în regim de timp real și în volum deplin, în special în ceea ce privește:</p> <p>a) <u>corespunderea specificației echipamentului furnizorului cu formatul acceptat de mijloacele tehnice speciale;</u></p>	<p>La art. 7 alin. (1), trebuie exclus termenul „gratis”, iar sintagma „în condițiile prezentei legi” trebuie înlocuită cu sintagma „în cazurile și în modul prevăzut de lege”.</p> <p>Termenul „gratis” face ca prezenta normă să fie în contradicție cu art. 8 alin. (1) pct. 4) din Legea nr. 420, potrivit căruia SIS are dreptul să utilizeze bunurile altor persoane în bază de contract, dacă nu există o înțelegere verbală între părți, precum și că, la cererea persoanelor, Serviciul le compensează, în modul stabilit de legislația civilă, cheltuielile sau prejudiciile cauzate.</p> <p>Deoarece condițiile în care SIS are dreptul să utilizeze bunurile altor persoane sunt stabilite nu în prezenta lege, dar în Legea nr. 420, sintagma „în condițiile prezentei legi” ar trebui înlocuită cu sintagma „în cazurile și în modul prevăzut de lege”.</p> <p>La art. 7 alin. (2) pct. 1), după termenul “spații” este necesar de a adăuga sintagma “în bază de contract”, pentru a respecta norma generală, stabilită la art. 8 alin. (1) pct. 4) din Legea nr. 420, citat mai sus. De asemenea, termenul „echipamente” trebuie exclus, deoarece procurarea echipamentelor necesare pentru înfăptuirea de către Serviciu a măsurilor contrainformative sau informative externe se face din bugetul de stat. Prestatorii de servicii poștale și furnizorii de rețele și/sau servicii de comunicații electronice achită impozite și taxe în bugetul de stat și nu pot fi obligați să finanțeze suplimentar procurarea echipamentelor necesare pentru activitatea SIS.</p>
--	---

<p>b) disponibilitatea furnizorului de a conecta mijloacele tehnice speciale via conexiuni fixe sau prin comutator;</p> <p>9) <u>să asigure accesul continuu a Serviciului la bazele de date ale abonaților (ce vor conține obligatoriu identificatorii tehnice și datele de identitate ale abonaților, dacă acestea se cunosc), prin conectarea mijloacelor tehnice ale Serviciului la echipamentul furnizorilor de rețele și/sau servicii de comunicații electronice, sau prin alte metode stabilite de comun acord, în scopul înlăturării măsurilor contrainformative în conformitate cu legea;</u></p> <p>11) <u>să-și modernizeze și/sau extindă rețelele de comunicații electronice și infrastructura asociată astfel încât să nu afecteze continuitatea efectuării măsurilor contrainformative sau informative externe în rețelele de comunicații electronice. În cazul în care modernizarea și/sau extinderea rețelei de comunicații electronice sau a infrastructurii asociate poate împiedica efectuarea măsurilor contrainformative sau informative externe, darea în exploatare a acestora va avea loc <b>concomitent cu instalarea, din contul furnizorului, a echipamentului suplimentar necesar conectării mijloacelor tehnice speciale și ajustării formatului pentru transmiterea informațiilor cu formatul acceptat de mijloacele tehnice speciale.</b></u></p>	<p>La art. 7 alin. (2) pct. 4), sintagma „la toate interfețele echipamentelor furnizorilor, la propriile rețele de comunicații electronice” ar trebui înlocuită cu sintagma „la toate interfețele propriilor rețele de comunicații electronice ale furnizorilor”. SIS nu ar trebui să aibă dreptul de a se conecta la echipamente ale furnizorilor care nu sunt parte a rețelor de comunicații electronice.</p> <p>La art. 7 alin. (2) pct. 5) lit. a), furnizorii ar trebui obligați să asigure corespunderea specificației echipamentului furnizorului cu formatul standard pentru conectarea mijloacelor tehnice speciale (de exemplu, standardele ETSI). Furnizorii nu ar trebui să fie obligați să investească în echipamente non-standard, lucru care face echipamentul mult mai costisitor și poate întârzia punerea în funcțiune a acestuia. Orice soluții speciale solicitate de SIS trebuie să fie finanțate din contul bugetului de stat.</p> <p>La art. 7 alin. (2) pct. 9), obligația de a asigura accesul continuu a Serviciului la bazele de date ale abonaților, prin conectarea mijloacelor tehnice ale Serviciului la echipamentul furnizorilor de rețele și/sau servicii de comunicații electronice, ar trebui exclusă, deoarece generează riscul accesului neautorizat și divulgării neautorizate a informațiilor privind posesorii numerelor de telefon sau numerele de telefon care aparțin anumitor persoane, inclusiv copierea neautorizată și comercializarea bazelor de date ale abonaților. Mai mult ca atât, art. 12 din Legea nr. 420 prevede că informația privind identitatea abonaților se oferă în baza ordonanței directorului sau directorului adjunct special împuternicit al SIS, iar informația privind posesorii numerelor de telefon sau numerele de telefon care aparțin anumitor persoane se oferă în baza mandatului judecătoresc.</p>
---	---

	<p>La art. 7 alin. (2) pct. 11), furnizorii trebuie să poată să-și modernizeze și/sau extindă rețelele de comunicații electronice și infrastructura asociată fără nicio restricție, fiind obligați doar să asigure interfețele necesare pentru conectarea mijloacelor tehnice speciale și corespunderea specificației echipamentului furnizorului cu formatul standard pentru conectarea mijloacelor tehnice speciale (de exemplu, standardele ETSI). Furnizorii de rețele și/sau servicii de comunicații electronice nu ar trebui obligați să amâne modernizarea și/sau extinderea rețelelor de comunicații electronice (chiar dacă aceasta este o evoluție standard al tehnologiei, cum ar fi implementarea tehnologiei 5G sau 6G) sau să procure echipamentele necesare pentru îndeplinirea de către Serviciu a măsurilor contrainformative sau informative externe. Furnizorii achită impozite și taxe în bugetul de stat și nu pot fi obligați să finanțeze suplimentar procurarea echipamentelor necesare pentru activitatea SIS.</p>
<p>Articolul 25. Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice ori a unui punct de acces la un sistem informatic cu sau fără aportul furnizorilor de servicii de comunicații electronice</p> <p>(1) Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice ori a unui punct de acces la un sistem informatic constă în stabilirea, cu sau fără aportul unui furnizor de servicii electronice, a identității abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice, unui mijloc de comunicații electronice ori a unui punct de acces la un sistem informatic, sau stabilirea dacă un anumit mijloc de comunicații sau punct de acces la un sistem informatic este utilizat sau activ, ori a fost utilizat sau activ la o anumită dată, ori stabilirea mijloacelor de</p>	<p>La art. 25 alin. (1), nu este clar ce se înțelege prin “sistem de comunicații electronice”, “mijloc de comunicații electronice” și “punct de acces la un sistem informatic” (număr de telefon, adresă IP, dispozitiv mobil identificat prin cod IMEI).</p> <p>Pe de altă parte, prezentarea informațiilor privind posesorii numerelor de telefon, posesorii IP adreselor statice și dinamice sau a informației ce identifică echipamentul de comunicații electronice (codurile IMEI) este expres prevăzută la art. 41.</p> <p><u>Această neclaritate face imposibilă determinarea modului corect de autorizare a prezentării anumitor informații de către furnizorii de comunicații</u></p>

comunicații electronice prezente la un moment dat la o persoană.

(3) În cazul în care măsura contrainformativă se realizează cu aportul unui furnizor de servicii electronice, acesta după recepționarea extrasului din ordonanța directorului Serviciului sau directorului adjunct special împuternicit privind autorizarea măsurii, prezintă informațiile solicitate fără păstrarea copiei (inclusiv în format electronic) a răspunsului și datelor remise, în cel mai scurt timp posibil, dar nu mai târziu de 24 de ore din momentul primirii autorizației.

electronice. Or, conform art. 12, informațiile prevăzute la art. 25 se oferă în baza ordonanței directorului sau directorului adjunct special împuternicit al SIS, iar informațiile prevăzute la art. 41 se oferă în baza mandatului judecătoresc.

Prezenta normă ar trebui să se limiteze la identificarea titularilor numerelor de telefon sau adreșelor IP statice, care sunt ușor accesibile și nu cer o analiză a traficului.

Adresa IP dinamică este alocată utilizatorului doar pe durata sesiunii de Internet. Astfel, adresele IP dinamice ajung să fie utilizate de sute de mii de utilizatori. Posesorul unei adrese IP dinamice se determină numai în raport cu o comunicație (sesiune de Internet) specifică, a cărei dată și oră se cunoaște exact. Obținând informația privind posesorul adresei IP dinamice, SIS obține efectiv date privind sursa unei comunicații, care face obiectul art. 41 și ar trebui să fie autorizată prin mandat judecătoresc.

În mod similar, stabilirea mijloacelor de comunicații electronice (cod IMEI, adresă IP) prezente la un moment dat la o persoană se face numai în raport cu o comunicație specifică, a cărei dată și oră se cunoaște exact. Informația privind echipamentul utilizat pentru comunicație, de asemenea, face obiectul art. 41 și ar trebui să fie autorizată prin mandat judecătoresc.

La art. 25 alin. (3), stabilirea termenului maxim de 24 ore pentru prezentarea informațiilor privind identitatea abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice ori a unui punct de acces la un sistem informatic ar

	<p>obliga furnizorii să asigure prezența la serviciu a personalului responsabil pentru furnizarea unor asemenea informații în regim de <u>24/24 ore, 7/7 zile pe săptămână, inclusiv în zilele de sărbătoare.</u></p> <p>Asemenea cerință este abuzivă, mai ales în contextul în care art. 7 alin. (1) stabilește că asemenea informații se prezintă gratis. În țările democratice dezvoltate, furnizorii oferă asemenea servicii contra plată.</p>
<p>Articolul 38. Interceptarea comunicărilor cu sau fără înregistrarea acestora</p>	<p>Măsura cu privire la interceptarea comunicărilor în acest proiect prevede posibilitatea de înregistrare a comunicărilor voce, text și transfer de date/internet, pe când acestea sunt reglementate distinct în redacția actuală a CPP, fiindcă sunt categorii diferite de date și se realizează în mod diferențiat din punct de vedere tehnologic. Reglementările UE de asemenea le tratează diferit. Respectiv, considerăm că art. 12 trebuie să prevadă ca măsură separată monitorizarea transferului de date.</p> <p>Totodată, reieșind din faptul că interceptarea comunicărilor este o măsură intruzivă în viața privată credem că Legea ar trebui să prevadă în mod expres infracțiunile pentru care poate fi dispusă această măsură, similar redacției actuale din CPPRM.</p>
<p><b>Articolul 41. Colectarea informației de la furnizorii de servicii de comunicații electronice</b></p> <p>(1) Colectarea informației de la furnizorii de servicii de comunicații electronice constă în <u>colectarea, cu sau fără aportul furnizorilor de servicii de comunicații electronice, a informațiilor transmise prin canalele tehnice de comunicații electronice, fixarea secretă a informațiilor, transmise sau primite prin intermediul liniilor tehnice de legături de</u></p>	<p>La art. 41 alin. (1), textul “colectarea, cu sau fără aportul furnizorilor de servicii de comunicații electronice, a informațiilor transmise prin canalele tehnice de comunicații electronice, fixarea secretă a informațiilor, transmise sau primite prin intermediul liniilor tehnice de legături de comunicații electronice de către persoanele supuse măsurii contrainformative” ține de interceptarea comunicărilor, dar nu de colectarea informației de la furnizorii de servicii de comunicații electronice, și ar</p>

<p><u>comunicații electronice de către persoanele supuse măsurii contrainformative</u>, precum și obținerea de la operatori a informației disponibile, generate sau procesate în cadrul furnizării propriilor servicii de comunicații electronice, inclusiv de roaming, necesare pentru identificarea și urmărirea sursei de comunicații electronice, identificarea destinației, tipului, datei, orei și duratei comunicației electronice, identificarea echipamentului de comunicații electronice al utilizatorului sau al altui dispozitiv utilizat pentru comunicație, identificarea coordonatelor echipamentului terminal de comunicații mobile, și în special despre:</p> <ol style="list-style-type: none"><li>1) <u>posesorii numerelor de telefon (numele, prenumele, domiciliul)</u>;</li><li>2) numerele de telefon înregistrate pe numele unei persoane;</li><li>3) serviciile de comunicații electronice prestate utilizatorului;</li><li>4) sursa de comunicații electronice (<u>datele de identificare tehnice</u>; numele, prenumele și domiciliul abonatului sau utilizatorului înregistrat);</li><li>5) destinația comunicației electronice (<u>datele de identificare tehnice al apelatului</u>; <u>datele de identificare tehnice ale punctului de acces redirectionat</u>, după caz; numele, prenumele și domiciliul abonatului sau utilizatorului înregistrat);</li><li>6) tipul, data, ora și durata comunicației electronice, inclusiv ale tentativelor de apel eșuate. Prin tentativă de apel eșuată se înțelege comunicarea în care apelul a fost conectat cu succes, dar nu a fost răspuns sau a avut loc o intervenție legată de gestionarea rețelei;</li><li>7) echipamentul de comunicații electronice al utilizatorului sau un alt dispozitiv utilizat pentru comunicație {codurile <u>IMSI</u> și <u>IMEI</u> ale telefoanelor mobile ale apelantului și apelatului; în cazul serviciilor preplătite anonime - data și ora la care a</li></ol>	<p>trebui exclus sau mutat la articolul ce reglementează interceptarea.</p> <p>Așa cum am remarcat mai sus, art. 41 alin. (1) pct. 1), 7) și 9) din prezentul articol sunt în contradicție cu art. 25. Pentru a evita această contradicție și a stabili exact modul de autorizare a prezentării informațiilor respective, art. 25 ar trebui să se limiteze la identificarea posesorilor numerelor de telefon sau adreselor IP statice, iar identificarea posesorilor adreselor IP dinamice și stabilirea mijlocului de comunicații ar trebui să facă obiectul art. 41.</p> <p>La art. 41 alin. (1) pct. 4) și 5), este necesar de a defini clar ce se înțelege prin “date de identificare tehnice”.</p> <p>La art. 41 alin. (1) pct. 7), este necesar de a exclude referința la codurile “IMSI” ale telefoanelor mobile, deoarece telefoanele mobile sunt identificate prin cod IMEI (International Mobile Equipment Identity), iar IMSI (International Mobile Subscriber Identity), compus din prefixul de țară, prefixul rețelei și numărul de telefon mobil, identifică abonații.</p> <p>La art. 41 alin. (1) pct. 9), este necesar de a defini clar ce se înțelege prin “informația ce identifică echipamentul comunicațional” al posesorilor IP adreselor statice și dinamice. Adresa IP însăși definește un echipament terminal.</p> <p>La art. 41 alin. (2), lit. b), care permite colectarea informației de la furnizorii de servicii de comunicații electronice de sine stătător, cu utilizarea produselor de program sau mijloacelor tehnice speciale</p>
---	---

<p>fost inițial activat serviciul și denumirea locației (Cell ID) din care a fost activat serviciul, <u>precum și orice date care pot servi pentru identificarea utilizatorului serviciului</u>};</p> <p>8) locul echipamentului de comunicații mobile {denumirea locației (Cell ID) de la începutul comunicației; locația geografică a celulei prin referință la denumirea locației, în perioada în care datele sunt reținute};</p> <p>9) <u>posesorii IP adreselor statice și dinamice (numele, prenumele, domiciliul, denumirea firmei, adresa juridică etc.), precum și informația ce identifică echipamentul comunicațional al acestora</u>;</p> <p>registrele de evidență, generate sau procesate în procesul furnizării utilizatorilor a serviciilor de comunicații electronice, necesare pentru identificarea și urmărirea sursei de comunicații electronice, precum și alta date referitoare la traficul informațional.</p> <p>(2) Colectarea informației de la furnizorii de servicii de comunicații electronice se realizează:</p> <p>a) prin prezentarea nemijlocită către furnizorii de servicii de comunicații electronice a extrasului din mandatul judecătoresc, eliberat de către judecător concomitent cu mandatul judecătoresc, în care se va indica doar categoria de informații ce urmează a fi prezentată;</p> <p>b) prin intermediul subunității specializate a Serviciului, <u>cu utilizarea produselor de program sau mijloacelor tehnice speciale conectate, în caz de necesitate, la echipamentul furnizorilor.</u></p>	<p>conectate la echipamentul furnizorilor, ar trebui exclusă.</p> <p>În hotărârile sale pe dosarele Digital Rights Ireland și Tele2 Sverige, Curtea de Justiție a Uniunii Europene a reținut că <u>o gamă nelimitată de subiecți ai reținerii datelor echivalează cu o încălcare a principiilor strictei necesități și proporționalității</u>. 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.</p> <p>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 îndeplinească următoarele condiții:</p> <ul style="list-style-type: none"><li>• să fie clar și precis;</li><li>• să definească categoriile de date păstrate, perioadele de păstrare și mijloacele de comunicare și persoanele afectate și să le limiteze la ceea ce este strict necesar;</li><li>• să ofere garanții suficiente împotriva utilizării <u>abuzive a datelor</u>, inclusiv obligația de a păstra datele în UE și de a distruge ireversibil datele la sfârșitul perioadei de păstrare;</li><li>• să permită accesul exclusiv în interesul combaterii criminalității grave;</li><li>• să stabilească <u>procedura de accesare a datelor reținute</u>; și</li></ul>
--	---

	<ul style="list-style-type: none"><li>• <u>să stabilească un sistem de revizuire independentă ex ante și ex post a cererilor de acces<sup>1</sup>.</u></li></ul> <p>Acordarea posibilității ca SIS să acceseze de sine stătător la metadatele generează riscul accesului neautorizat și divulgării neautorizate a informațiilor protejate prin secretul corespondenței. Faptul că art. 12 din Legea nr. 420 prevede că asemenea informații se oferă în baza mandatului judecătoresc nu împiedică SIS să acceseze asemenea date pe ascuns, fără mandat judecătoresc.</p> <p>În afară de cele expuse mai sus, merită de menționat 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 SIS a unui număr mare de căutări extensive simultane ar putea face aceste sisteme inoperabile. În cazul în care SIS ar obține accesul direct la asemenea sisteme,</p>
--	---

<sup>1</sup> 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.

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.

	<p>investițiile suplimentare în creșterea capacității lor pentru a face față necesităților SIS ar trebui să fie eventual acoperite din contul bugetului public.</p>
<p><b>Articolul 44. Blocarea unui punct de acces conectat la un sistem informatic sau la rețele de comunicații electronice</b></p> <p>(1) Blocarea unui punct de acces conectat la un sistem informatic sau la rețele de comunicații electronice presupune deconectarea forțată de la un sistem informatic sau de la o rețea de comunicații electronice <u>a unui mijloc de comunicații</u> cu, sau fără, stabilirea interdicției de reconectare.</p> <p>(2) Blocarea unui punct de acces conectat la un sistem informatic sau la rețele de comunicații electronice se efectuează de către Serviciu cu utilizarea produselor de program, mijloacelor tehnice speciale <u>sau de către furnizorii de servicii de comunicații electronice, la prezentarea extrasului din mandatul judecătoresc.</u></p>	<p>La art. 44, norma respectivă ar trebuie exclusă, deoarece este ineficientă.</p> <p>În primul rând, nu este clar ce se înțelege prin termenul “mijloc de comunicații”. Dacă prin mijloc de comunicații se înțelege un telefon mobil, modem, tabletă (identificate prin IMEI), acest lucru nu va împiedica persoana vizată să utilizeze orice alt telefon mobil, modem sau tabletă pentru accesul la servicii. Astfel, investițiile furnizorilor în crearea “listei negre” a dispozitivelor mobile ar fi irosite.</p> <p>Dacă prin mijloc de comunicații se înțelege un calculator, nu există posibilitatea de a bloca un calculator anume.</p> <p>Norma respectivă ar putea fi reformulată astfel ca să prevadă suspendarea contractului cu anumită persoană și/sau pentru o anumită adresă, însă asemenea interdicție nu ar împiedica persoana să acceseze serviciile prin intermediul cartelelor emise de operatori străini sau cartelelor anonime, sau prin intermediul rețelelor Wi-Fi publice, sau să utilizeze serviciile contractate de persoane terțe sau la adrese terțe.</p>
<p>Capitolul VI</p> <p>Controlul activității informative și contrainformative</p> <p>Articolul 57. Controlul parlamentar</p> <p>(1) Controlul parlamentar asupra activității</p>	<p>Luând în considerație că în obiectivul controlului este și respectarea drepturilor omului, în special dreptul la viața privată, credem că, controlul parlamentar trebuie să se exercite minim de 2 ori pe an, iar raportul trebuie să conțină informații destul de detaliate pentru a permite o apreciere obiectivă</p>

<p>informative/contrainformative este exercitat de către Comisia securitate națională, apărare și ordine publică, prin intermediul Subcomisiei pentru exercitarea controlului parlamentar asupra activității Serviciului de Informații și Securitate al Republicii Moldova (în continuare – Subcomisia parlamentară).</p> <p>(2) Directorul Serviciului prezintă anual, în ședință închisă, Subcomisiei parlamentare un raport general cu privire la activitatea informativă/contrainformativă, care va cuprinde, în mod obligatoriu, informații despre numărul total al măsurilor contrainformative efectuate, numărul măsurilor contrainformative, stabilite la art. 12 alin. (1), efectuate, pe fiecare măsură în parte.</p> <p>(3) Subcomisia parlamentară poate solicita de la Președintele Judecătoriei Chișinău și Curții de Apel Chișinău informații privind numărul măsurilor contrainformative pentru care s-a eliberat mandat judecătoresc și numărul celor refuzate de a fi autorizate.</p> <p>(4) După prezentarea raportului, membrii Subcomisiei parlamentare pot înainta întrebări cu privire la activitatea informativă/contrainformativă înfăptuită de către Serviciu în anul precedent. În cadrul ședinței pot fi</p>	<p>asupra faptului dacă sunt comise abuzuri sau nu la acest subiect.</p> <p>În special, raportul trebuie să reflecte următoarea informație: în baza la ce articole din CP au fost efectuate măsurile, durata de efectuare a unor așa măsuri ca cercetarea domiciliului sau interceptarea comunicărilor, numărul de cetățeni care au fost supuși la fiecare măsură în parte, cum au fost întreprinse măsurile de informare a cetățenilor supuși acestor măsuri, câte contestații au fost depuse și examinate în privința obiectivității măsurilor dispuse și informația cu privire la distrugerea informațiilor obținute în cadrul măsurilor contrainformative.</p> <p>La moment, proiectul prevede că raportul Comisiei "poate fi făcut public". Credem că sintagma "poate" trebuie înlocuită cu "trebuie", fiindcă informarea societății cu privire la măsurile efectuate și care pot afecta viața privată este un control indirect a societății și un exercițiu de democrație.</p>
--	--



**ASOCIAȚIA NAȚIONALĂ**  
A COMPANIILOR DIN  
DOMENIUL TIC



<p>prezentate informații despre operațiunile finalizate realizate de către Serviciu, dacă divulgarea lor nu va prejudicia securitatea statului. Informații despre operațiunile în derulare nu se prezintă.</p> <p>(5) În baza raportului prezentat, Subcomisia parlamentară poate înainta recomandări privind activitatea Serviciului.</p> <p>Raportul prezentat Subcomisiei parlamentare poate fi făcut public, excluzându-se din acesta informațiile atribuite la secret de stat.</p>	
---	--