ASOCIAȚIA NAȚIONALĂ
A COMPANIILOR DIN
DOMENIUL TIC

FOREIGN INVESTORS ASSOCIATION
Investing in Moldova's Future

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 Asociaţiei Naţionale a Companiilor din Domeniul TIC (”ATIC) și Asociației Investitorilor Străini („FIA”).

Înţelegem şi apreciem eforturile autorilor proiectelor de Legi menţionate mai sus îndreptate spre minimizarea riscurilor şi ameninţărilor la adresa securităţii naţionale a Republicii Moldova, prin reglementarea detaliată a atribuţiilor, obligaţiilor şi 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 şi argumente au fost comunicate şi către experții Comisiei de la Veneția, care au solicitat opinia mediului de afaceri cu privire la aceste proiecte. Mizăm pe faptul că autorităţile RM vor lua în considerare aceste comentarii şi argumente la definitivarea proiectelor de legi în cauză.

De asemenea, Vă atragem atenţia 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,

Digitally signed by Bzovii Marina
Date: 2023.02.15 16:28:43 EET
Reason: MoldSign Signature
Location: Moldova

Marina Bzovii, Director Executiv, ATIC

Ana Groza, Director Executiv, FIA

ASOCIAŢIA NAŢIONALĂ
A COMPANIILOR DIN
DOMENIUL TIC

FOREIGN INVESTORS ASSOCIATION
Investing in Moldova's Future

Anexă la Avizul nr. 12
Din 15 februarie 2023

Legea 420

Articol din proiect	**Comentariu**
Articolul 8. Drepturile Serviciului (1) Serviciul are dreptul: 4) să utilizeze următoarele bunuri, cu excepţia celor ce aparţin misiunilor diplomatice şi persoanelor cu imunitate diplomatică: a) în bază de contract sau înţelegere verbală, în limitele necesare pentru realizarea atribuţiilor ce-i revin, încăperile de serviciu, alte bunuri ale persoanelor juridice, ale formaţiunilor militare, precum şi încăperile şi alte bunuri ale persoanelor fizice; d) în situaţii excepţionale, precum şi în cazul aplicaţiilor planificate la nivel naţional sau de către Serviciu, în bază de contract sau înţelegere verbală, pe gratis, reţelele şi serviciile de comunicaţii electronice ale furnizorilor, indiferent de tipul de proprietate al acestora. La cererea furnizorilor, Serviciul le compensează, în modul stabilit de legislaţia civilă, cheltuielile sau prejudiciile cauzate; 7) să solicite şi să primească, pe gratis, de la autorităţile publice, alte persoane juridice, indiferent de tipul de proprietate, informaţii necesare pentru exercitarea atribuţiilor ce revin Serviciului. Prezentarea informaţiilor solicitate de Serviciu nu poate fi refuzată pe motiv că acestea constituie informaţii cu accesibilitate limitată;	La art. 8 alin. (1) pct. 4) lit. a), nu este definit clar cine stabileşte dacă încăperile sau bunurile se oferă în bază de contract sau înţelegere verbală. Norma ar trebui să prevadă că încăperile sau bunurile se oferă în bază de contract, dacă părţile nu au convenit altfel. La art. 8 alin. (1) pct. 4) lit. d), există o contradicţie între textul care prevede că reţelele şi serviciile de comunicaţii electronice ale furnizorilor sunt puse la dispoziţia SIS pe gratis şi textul care prevede dreptul furnizorilor de a cere compensarea cheltuielilor sau prejudiciului. De asemenea, nu este definit clar cine stabileşte dacă reţelele se utilizează în bază de contract sau înţelegere verbală. Norma ar trebui să prevadă că reţelele se utilizează în bază de contract, dacă părţile nu au convenit altfel, iar menţiunea "pe gratis" trebuie exclusă, păstrând dreptul furnizorilor de a cere compensarea cheltuielilor sau prejudiciului. La art. 8 alin. (1) pct. 7), nu se face referinţă la necesitatea respectării procedurii de autorizare a obţinerii informaţiilor cu accesibilitate limitată, stabilite de lege. Or, art. 12 din prezenta lege stabileşte că anumite informaţii, cum ar fi informaţia financiară sau identitatea abonatului, informaţia ce se află sau se prelucrează într-un sistem informational, informaţia colectată de la furnizorii de servicii de comunicaţii electronice, se prezintă numai în baza autorizaţiei directorului sau directorului adjunct special împuternicit al SIS sau în baza mandatului judecătoresc. Norma ar trebui să

	prevadă că prezentarea informaţiilor solicitate de Serviciu nu poate fi refuzată pe motiv că acestea constituie informaţii cu accesibilitate limitată, dacă a fost respectată procedura de autorizare a măsurii respective, stabilită de lege.
Articolul 11. Cooperarea Serviciului cu instituţii din ţară şi din străinătate 4) Autorităţile publice, precum şi alte persoane juridice indiferent de tipul de proprietate, sînt obligate să acorde Serviciului, în limita posibilităţilor, asistenţă operaţională, informaţională, tehnică şi de altă natură în vederea îndeplinirii atribuţiilor ce îi revin, inclusiv să ofere, funcţii pentru detaşarea ofiţerilor de informaţii în vederea îndeplinirii unor atribuţii în interesul securităţii naţionale.	Această normă contravine art. 7 alin. (3), potrivit căruia doar organele administraţiei publice centrale, subdiviziunile şi instituţiile subordonate acestora sunt obligate, la solicitare, să pună la dispoziţie Serviciului funcţii în care vor fi detaşaţi ofiţeri de informaţii în scopul realizării activităţii informative/contrainformative. În ceea ce priveşte obligaţia de a acorda asistenţă operaţională, informaţională, tehnică şi de altă natură, această normă este foarte vagă, creând premise pentru solicitări abuzive din partea SIS (furnizorii s-au ciocnit anterior cu asemenea solicitări). Norma ar trebui să limiteze obligaţiile respective la organele administraţiei publice centrale, subdiviziunile şi instituţiile subordonate acestora, nu şi la alte persoane juridice.
Articolul 27. Asigurarea informaţională a Serviciului (2) În interesul asigurării securităţii naţionale, Serviciul, în modul stabilit de legislaţie, are drept de acces, gratuit, la sistemele informaţionale, reţelele de comunicaţii electronice, la resursele informaţionale şi bazele de date ale organelor de ocrotire a normelor de drept, autorităţilor publice, întreprinderilor, instituţiilor şi organizaţiilor, indiferent de tipul de proprietate.	Obligaţia de a acorda acces, gratuit, în modul stabilit de legislaţie, la sistemele informaţionale, reţelele de comunicaţii electronice, la resursele informaţionale şi bazele de date ale întreprinderilor, instituţiilor şi organizaţiilor, indiferent de tipul de proprietate este foarte vagă, creând premise pentru solicitări abuzive din partea SIS. Pentru reducerea acestui risc, norma ar trebui să prevadă că accesul se acordă în cazurile şi în modul stabilit de prezenta lege.

Legea 422

Articolul 7. Asistenţa acordată la efectuarea activităţii informative/contrainformative (1) Persoanele fizice şi juridice, indiferent de forma de proprietate, sînt obligate, în condiţiile **prezentei legi**, să acorde asistenţa necesară Serviciului, să pună imediat, **gratis** la dispoziţia acestuia informaţiile solicitate, precum şi, în măsura posibilităţii, bunuri mobile şi imobile, alte obiecte şi documente necesare pentru realizarea activităţii informative/contrainformative. (2) Prestatorii de servicii poştale şi furnizorii de reţele şi/sau servicii de comunicaţii electronice, indiferent de tipul de proprietate sunt obligaţi: 1) să pună la dispoziție spaţii, echipamente şi condiţii tehnice necesare pentru înfăptuirea de către Serviciu a măsurilor contrainformative sau informative externe şi să prezinte, în acest scop, datele tehnice necesare; 4) să asigure accesul liber şi operativ al subdiviziunii specializate a Serviciului la toate interfeţele echipamentelor furnizorilor, la propriile reţele de comunicaţii electronice, să asigure condiţiile tehnice şi datele necesare pentru conectarea mijloacelor tehnice speciale predestinate înfăptuirii măsurilor contrainformative sau informative externe; 5) să asigure permanent şi continuu condiţiile tehnice necesare pentru conectarea şi funcţionarea mijloacelor tehnice speciale predestinate înfăptuirii măsurilor contrainformative sau informative externe în regim de timp real şi în volum deplin, în special în ceea ce priveşte: a) corespunderea specificaţiei echipamentului furnizorului cu formatul acceptat de mijloacele tehnice speciale;	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”. 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 şi că, la cererea persoanelor, Serviciul le compensează, în modul stabilit de legislaţia civilă, cheltuielile sau prejudiciile cauzate. 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”. La art. 7 alin. (2) pct. 1), după termenul “spaţii” 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 poştale şi furnizorii de reţele şi/sau servicii de comunicaţii electronice achită impozite şi taxe în bugetul de stat şi nu pot fi obligaţi să finanţeze suplimentar procurarea echipamentelor necesare pentru activitatea SIS.

b) disponibilitatea furnizorului de a conecta mijloacele tehnice speciale via conexiuni fixe sau prin comutator; 9) să asigure accesul continuu a Serviciului la bazele de date ale abonaţilor (ce vor conţine obligatoriu identificatorii tehnice şi datele de identitate ale abonaţilor, dacă acestea se cunosc), prin conectarea mijloacelor tehnice ale Serviciului la echipamentul furnizorilor de reţele şi/sau servicii de comunicaţii electronice, sau prin alte metode stabilite de comun acord, în scopul înfăptuirea măsurilor contrainformative în conformitate cu legea; 11) să-şi modernizeze şi/sau extindă reţelele de comunicaţii electronice şi infrastructura asociată astfel încât să nu afecteze continuitatea efectuării măsurilor contrainformative sau informative externe în reţelele de comunicaţii electronice. În cazul în care modernizarea şi/sau extinderea reţelei de comunicaţii electronice sau a infrastructurii asociate poate împiedica efectuarea măsurilor contrainformative sau informative externe, darea în exploatare a acestora va avea loc **concomitent cu instalarea, din contul furnizorului, a echipamentului suplimentar** necesar conectării mijloacelor tehnice speciale şi ajustării formatului pentru transmiterea informaţiilor cu formatul acceptat de mijloacele tehnice speciale.	La art. 7 alin. (2) pct. 4), sintagma „la toate interfeţele echipamentelor furnizorilor, la propriile reţele de comunicaţii electronice” ar trebui înlocuită cu sintagma „la toate interfețele propriilor reţele de comunicaţii electronice ale furnizorilor”. SIS nu ar trebui să aibă dreptul de a se conecta la echipamente ale furnizorilor care nu sunt parte a reţelor de comunicaţii electronice. La art. 7 alin. (2) pct. 5) lit. a), furnizorii ar trebui obligați să asigure corespunderea specificaţiei 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 şi poate întârzia punerea în funcţiune a acestuia. Orice soluții speciale solicitate de SIS trebuie să fie finanțate din contul bugetului de stat. La art. 7 alin. (2) pct. 9), obligația de a asigura accesul continuu a Serviciului la bazele de date ale abonaţilor, prin conectarea mijloacelor tehnice ale Serviciului la echipamentul furnizorilor de reţele şi/sau servicii de comunicaţii electronice, ar trebui exclusă, deoarece generează riscul accesului neautorizat şi divulgării neautorizate a informaţiilor privind posesorii numerelor de telefon sau numerele de telefon care aparţin anumitor persoane, inclusiv copierea neautorizată şi comercializarea bazelor de date ale abonaţilor. Mai mult ca atât, art. 12 din Legea nr. 420 prevede că informaţia privind identitatea abonaţilor se oferă în baza ordonanţei directorului sau directorului adjunct special împuternicit al SIS, iar informaţia privind posesorii numerelor de telefon sau numerele de telefon care aparţin anumitor persoane se oferă în baza mandatului judecătoresc.

	La art. 7 alin. (2) pct. 11), furnizorii trebuie să poată să-şi modernizeze şi/sau extindă reţelele de comunicaţii electronice şi infrastructura asociată fără nicio restricţie, fiind obligați doar să asigure interfeţele necesare pentru conectarea mijloacelor tehnice speciale şi corespunderea specificaţiei echipamentului furnizorului cu formatul standard pentru conectarea mijloacelor tehnice speciale (de exemplu, standardele ETSI). Furnizorii de reţele şi/sau servicii de comunicaţii electronice nu ar trebui obligaţi să amâne modernizarea şi/sau extinderea reţelelor de comunicaţii electronice (chiar dacă aceasta este o evoluţie standard al tehnologiei, cum ar fi implementarea tehnologiei 5G sau 6G) sau să procure echipamentele necesare pentru înfăptuirea de către Serviciu a măsurilor contrainformative sau informative externe. Furnizorii achită impozite şi taxe în bugetul de stat şi nu pot fi obligaţi să finanţeze suplimentar procurarea echipamentelor necesare pentru activitatea SIS.
Articolul 25. Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicaţii electronice ori a unui punct de acces la un sistem informatic cu sau fără aportul furnizorilor de servicii de comunicaţii electronice (1) Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicaţii electronice ori a unui punct de acces la un sistem informatic constă în stabilirea, cu sau fără aportul unui furnizor de servicii electronice, a identităţii abonatului, proprietarului sau utilizatorului unui sistem de comunicaţii electronice, unui mijloc de comunicaţii electronice ori a unui punct de acces la un sistem informatic, sau stabilirea dacă un anumit mijloc de comunicaţii 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	La art. 25 alin. (1), nu este clar ce se înţelege prin “sistem de comunicaţii electronice”, “mijloc de comunicaţii electronice” şi “punct de acces la un sistem informatic” (număr de telefon, adresă IP, dispozitiv mobil identificat prin cod IMEI). Pe de altă parte, prezentarea informaţiilor privind posesorii numerelor de telefon, posesorii IP adreselor statice şi dinamice sau a informaţiei ce identifică echipamentul de comunicaţii electronice (codurile IMEI) este expres prevăzută la art. 41. Această neclaritate face imposibilă determinarea modului corect de autorizare a prezentării anumitor informaţii de către furnizorii de comunicaţii

comunicaţii 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 tîrziu de 24 de ore din momentul primirii autorizației.	electronice. Or, conform art. 12, informaţiile prevăzute la art. 25 se oferă în baza ordonanţei directorului sau directorului adjunct special împuternicit al SIS, iar informaţiile prevăzute la art. 41 se oferă în baza mandatului judecătoresc. Prezenta normă ar trebui să se limiteze la identificarea titularilor numerelor de telefon sau adreselor IP statice, care sunt uşor accesibile şi nu cer o analiză a traficului. Adresa IP dinamică este alocată utilizatorului doar pe durata sesiunii de Internet. Astfel, adresele IP dinamice ajung sa fie utilizate de sute de mii de utilizatori. Posesorul unei adrese IP dinamice se determină numai în raport cu o comunicaţie (sesiune de Internet) specifică, a cărei dată şi oră se cunoaşte exact. Obţinând informaţia privind posesorul adresei IP dinamice, SIS obţine efectiv date privind sursa unei comunicaţii, care face obiectul art. 41 şi ar trebui să fie autorizată prin mandat judecătoresc. În mod similar, stabilirea mijloacelor de comunicaţii electronice (cod IMEI, adresă IP) prezente la un moment dat la o persoană se face numai în raport cu o comunicaţie specifică, a cărei dată şi oră se cunoaşte exact. Informaţia privind echipamentul utilizat pentru comunicaţie, de asemenea, face obiectul art. 41 şi ar trebui să fie autorizată prin mandat judecătoresc. La art. 25 alin. (3), stabilirea termenului maxim de 24 ore pentru prezentarea informaţiilor privind identitatea abonatului, proprietarului sau utilizatorului unui sistem de comunicaţii electronice ori a unui punct de acces la un sistem informatic ar

	obliga furnizorii să asigure prezența la serviciu a personalului responsabil pentru furnizarea unor asemenea informații în regim de 24/24 ore, 7/7 zile pe săptămână, inclusiv în zilele de sărbătoare. 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.
Articolul 38. Interceptarea comunicărilor cu sau fără înregistrarea acestora	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. 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.
Articolul 41. Colectarea informației de la furnizorii de servicii de comunicații electronice (1) Colectarea informației de la furnizorii de servicii de comunicații electronice constă în 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	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

comunicaţii electronice de către persoanele supuse măsurii contrainformative, precum şi obţinerea de la operatori a informaţiei disponibile, generate sau procesate în cadrul furnizării propriilor servicii de comunicaţii electronice, inclusiv de roaming, necesare pentru identificarea şi urmărirea sursei de comunicaţii electronice, identificarea destinaţiei, tipului, datei, orei şi duratei comunicaţiei electronice, identificarea echipamentului de comunicaţii electronice al utilizatorului sau al altui dispozitiv utilizat pentru comunicaţie, identificarea coordonatelor echipamentului terminal de comunicaţii mobile, şi în special despre: 1) posesorii numerelor de telefon (numele, prenumele, domiciliul); 2) numerele de telefon înregistrate pe numele unei persoane; 3) serviciile de comunicaţii electronice prestate utilizatorului; 4) sursa de comunicaţii electronice (datele de identificare tehnice; numele, prenumele şi domiciliul abonatului sau utilizatorului înregistrat); 5) destinaţia comunicaţiei electronice (datele de identificare tehnice al apelatului; datele de identificare tehnice ale punctului de acces redirecţionat, după caz; numele, prenumele şi domiciliul abonatului sau utilizatorului înregistrat); 6) tipul, data, ora şi durata comunicaţiei electronice, inclusiv ale tentativelor de apel eşuate. Prin tentativă de apel eşuată se înţelege comunicarea în care apelul a fost conectat cu succes, dar nu a fost răspuns sau a avut loc o intervenţie legată de gestionarea reţelei; 7) echipamentul de comunicaţii electronice al utilizatorului sau un alt dispozitiv utilizat pentru comunicaţie {codurile IMSI şi IMEI ale telefoanelor mobile ale apelantului şi apelatului; în cazul serviciilor preplătite anonime - data şi ora la care a	trebui exclus sau mutat la articolul ce reglementează interceptarea. Aşa cum am remarcat mai sus, art. 41 alin. (1) pct. 1), 7) şi 9) din prezentul articol sunt în contradicţie cu art. 25. Pentru a evita această contradicţie şi 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 şi stabilirea mijlocului de comunicaţii ar trebui să facă obiectul art. 41. La art. 41 alin. (1) pct. 4) și 5), este necesar de a defini clar ce se înţelege prin “date de identificare tehnice”. La art. 41 alin. (1) pct. 7), este necesar de a exclude referinţa 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 ţară, prefixul reţelei şi numărul de telefon mobil, identifică abonaţii. La art. 41 alin. (1) pct. 9), este necesar de a defini clar ce se înţelege prin “informaţia ce identifică echipamentul comunicaţional” al posesorilor IP adreselor statice şi dinamice. Adresa IP însăşi defineşte un echipament terminal. La art. 41 alin. (2), lit. b), care permite colectarea informaţiei de la furnizorii de servicii de comunicaţii electronice de sine stătător, cu utilizarea produselor de program sau mijloacelor tehnice speciale

fost iniţial activat serviciul şi denumirea locaţiei (Cell ID) din care a fost activat serviciul, precum şi orice date care pot servi pentru identificarea utilizatorului serviciului};	conectate la echipamentul furnizorilor, ar trebui exclusă.
8) locul echipamentului de comunicaţii mobile {denumirea locaţiei (Cell ID) de la începutul comunicaţiei; locaţia geografică a celulei prin referinţă la denumirea locaţiei, în perioada în care datele sunt reţinute};	În hotărârile sale pe dosarele Digital Rights Ireland şi Tele2 Sverige, 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.
9) posesorii IP adreselor statice şi dinamice (numele, prenumele, domiciliul, denumirea firmei, adresa juridică etc.), precum şi informaţia ce identifică echipamentul comunicaţional al acestora;	
registrele de evidenţă, generate sau procesate în procesul furnizării utilizatorilor a serviciilor de comunicaţii electronice, necesare pentru identificarea şi urmărirea sursei de comunicaţii electronice, precum şi alta date referitoare la traficul informaţional.	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:
(2) Colectarea informaţiei de la furnizorii de servicii de comunicaţii electronice se realizează:	• să fie clar și precis;
a) prin prezentarea nemijlocită către furnizorii de servicii de comunicaţii electronice a extrasului din mandatul judecătoresc, eliberat de către judecător concomitent cu mandatul judecătoresc, în care se va indica doar categoria de informaţii ce urmează a fi prezentată;	• 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;
b) prin intermediul subunităţii specializate a Serviciului, cu utilizarea produselor de program sau mijloacelor tehnice speciale conectate, în caz de necesitate, la echipamentul furnizorilor.	• să ofere garanții suficiente împotriva utilizării abuzive a datelor, inclusiv obligația de a păstra datele în UE și de a distruge ireversibil datele la sfârșitul perioadei de păstrare;
	• să permită accesul exclusiv în interesul combaterii criminalității grave;
	• să stabilească procedura de accesare a datelor reținute; și

	• să stabilească un sistem de revizuire independentă ex ante și ex post a cererilor de acces[1]. Acordarea posibilităţii ca SIS să acceseze de sine stătător la metadatele generează riscul accesului neautorizat şi divulgării neautorizate a informaţiilor protejate prin secretul corespondenţei. Faptul că art. 12 din Legea nr. 420 prevede că asemenea informaţii se oferă în baza mandatului judecătoresc nu împiedică SIS să acceseze asemenea date pe ascuns, fără mandat judecătoresc. 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,

[1] 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.

	investițiile suplimentare în creșterea capacității lor pentru a face față necesităților SIS ar trebui să fie eventual acoperite din contul bugetului public.
Articolul 44. Blocarea unui punct de acces conectat la un sistem informatic sau la reţele de comunicaţii electronice (1) Blocarea unui punct de acces conectat la un sistem informatic sau la reţele de comunicaţii electronice presupune deconectarea forţată de la un sistem informatic sau de la o reţea de comunicaţii electronice a unui mijloc de comunicaţii cu, sau fără, stabilirea interdicţiei de reconectare. (2) Blocarea unui punct de acces conectat la un sistem informatic sau la reţele de comunicaţii electronice se efectuează de către Serviciu cu utilizarea produselor de program, mijloacelor tehnice speciale sau de către furnizorii de servicii de comunicaţii electronice, la prezentarea extrasului din mandatul judecătoresc.	La art. 44, norma respectivă ar trebuie exclusă, deoarece este ineficientă. În primul rând, nu este clar ce se înţelege prin termenul "mijloc de comunicaţii". Dacă prin mijloc de comunicaţii se înţelege 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, investiţiile furnizorilor în crearea "listei negre" a dispozitivelor mobile ar fi irosite. Dacă prin mijloc de comunicaţii se înţelege un calculator, nu există posibilitatea de a bloca un calculator anume. Norma respectivă ar putea fi reformulată astfel ca să prevadă suspendarea contractului cu anumită persoană şi/sau pentru o anumită adresă, însă asemenea interdicţie nu ar împiedica persoana să acceseze serviciile prin intermediul cartelelor emise de operatori străini sau cartelelor anonime, sau prin intermediul reţelelor Wi-Fi publice, sau să utilizeze serviciile contractate de persoane terţe sau la adrese terţe.
Capitolul VI Controlul activității informative și contrainformative Articolul 57. Controlul parlamentar (1) Controlul parlamentar asupra activităţii	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 trebie să conțină informații destul de detaliate pentru a permite o apreciere obiectivă

	informative/contrainformative este exercitat de către Comisia securitate naţională, apărare şi ordine publică, prin intermediul Subcomisiei pentru exercitarea controlului parlamentar asupra activităţii Serviciului de Informaţii și Securitate al Republicii Moldova (în continuare – Subcomisia parlamentară).	asupra faptului dacă sunt comise abuzuri sau nu la acest subiect. 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. 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.
(2)	Directorul Serviciului prezintă anual, în şedinţă închisă, Subcomisiei parlamentare un raport general cu privire la activitatea informativă/contrainformativă, care va cuprinde, în mod obligatoriu, informaţii despre numărul total al măsurilor contrainformative efectuate, numărul măsurilor contrainformative, stabilite la art. 12 alin. (1), efectuate, pe fiecare măsură în parte.	
(3)	Subcomisia parlamentară poate solicita de la Preşedintele Judecătoriei Chișinău și Curții de Apel Chișinău informaţii privind numărul măsurilor contrainformative pentru care s-a eliberat mandat judecătoresc şi numărul celor refuzate de a fi autorizate.	
(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 şedinţei pot fi	

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