



## **Comisia securitate națională, apărare și ordine publică**

### **Raport asupra proiectului de lege privind activitatea contrainformativă și activitatea informativă externă (nr.422 din 17.11.2022), lectura II.**

În temeiul atribuțiilor funcționale stabilite de Regulamentul Parlamentului, Comisia securitate națională, apărare și ordine publică, a examinat în cadrul ședinței sale din data de 28 iunie a.c., amendamentele, propunerile și obiecțiile parvenite la proiectul de lege privind activitatea contrainformativă și activitatea informativă externă.

Decizia argumentată a Comisiei asupra acestora se conține în sinteza amendamentelor care împreună cu proiectul redactat sunt părți integrante la prezentul raport.

Astfel, ținem să menționăm că până la momentul actual în legislația națională nu a existat un act legislativ cadru și distinct care să reglementeze desfășurarea activităților contrainformative și informative externe care sunt realizate de către Serviciul de Informații și Securitate al Republicii Moldova, acestea fiind autorizate într-un mod parțial în cadrul unor procese conexe prevăzute de legislația în vigoare cu privire la activitatea specială de investigații.

Din considerentul sus-menționat, precum și în vederea asigurării unui proces legislativ cât mai transparent, a fost solicitată anticipat opinia experților Comisiei de la Veneția pe marginea prezentului proiect în pachet cu proiectul de lege nr.420 cu privire la Serviciul de Informații și Securitate al Republicii Moldova, adoptat de Parlamentul Republicii Moldova în lectură finală la data de 8 iunie anul curent. Raportul de expertiză al Comisiei de la Veneția, precum și avizele instituțiilor interesate, au fost plasate spre examinare și dezbateri publice pe site-ul oficial al Parlamentului.

În acest context, până la momentul actual, Comisia a organizat circa 20 de dezbateri publice, și ședințe al grupurilor de lucru interinstituționale, dedicate examinării amendamentelor, obiecțiilor și propunerilor ce se conțin în expertiza Comisiei de la Veneția, precum și în avizele instituțiilor interesate, la care au participat, fără restricții toți doritorii din partea societății civile, experților internaționali, mediului

de afaceri, justiției, organelor de drept, oficiului ombudsmanului, centrului național pentru protecția datelor cu caracter personal etc.,

În rezultatul procesului de consultări, Comisia consideră că redacția actuală a prezentului proiect de lege a fost substanțial îmbunătățită, și anume:

1. A fost revizuită conceptual lista măsurilor contrainformative care vor putea fi realizate de către SIS, aceasta fiind diminuată.

2. A fost revăzută procedura de autorizare a măsurilor contrainformative. Astfel, toate măsurile vor fi autorizate de către un judecător, cu excepția celor de identificare a abonatului sau utilizatorului unei rețele de comunicații electronice sau a unui serviciu al societății informaționale, care va putea fi autorizată de către directorul Serviciului.

3. Au fost mai clar delimitate activitățile SIS de prevenire al amenințărilor la adresa securității statului de cele de investigații penale. Astfel, s-a stabilit expres că rezultatele activității desfășurate cu mandat judecătoresc nu vor putea fi utilizate ca probă în cadrul unui dosar penal, iar dacă în contextul realizării activității contrainformative se va stabili că a fost săvârșită o infracțiune, SIS va sesiza Procuratura în vederea pornirii urmăririi penale. Investigarea acelei fapte penale se va realiza exclusiv prin mecanismele Codului de procedură penală și sub conducerea unui procuror.

4. A fost revăzut nivelul instanței de judecată care va autoriza măsurile în cauză. Astfel, s-a stabilit că mandatul judecătoresc va fi emis de către un judecător de la Curtea de Apel Chișinău, iar recursurile vor fi examinate de către un complet din trei judecători de la Curtea Supremă de Justiție.

5. A fost introdus un mecanism de control ex post. Astfel, după finalizarea realizării măsurilor contrainformative, procesul verbal în care s-au consemnat datele acelei măsuri, precum și toată informația obținută vor fi remise judecătorului care a autorizat măsura pentru verificarea legalității acțiunilor întreprinse și corespunderii mandatului emis. Dacă va constata că măsura este ilegală, judecătorul o va declara nulă și va sesiza Procuratura pentru investigarea iregularităților admise.

6. A fost introdus un mecanism mai riguros și mai eficient de control privitor la securizarea informațiilor. Astfel, s-a stabilit că suportul original pe care este înregistrată informația (audio/video) obținută în cadrul măsurii, după verificarea legalității de către judecător, va fi sigilată și păstrată separat de dosarul special. Prin urmare, în cazul unui

control se va putea asigura verificarea volumului inițial de informații culese, cu cele existente și prelucrate în dosarul special.

7. S-a fortificat esențial mecanismul de control parlamentar. Astfel, este prevăzut că Subcomisiei parlamentare de control asupra SIS i se va prezenta un raport cu privire la activitatea informativă/contrainformativă, care va cuprinde, în mod obligatoriu informații despre:

a) numărul total al măsurilor contrainformative dispuse, efectuate și respinse, pe fiecare măsură în parte;

b) numărul dosarelor speciale inițiate și clasate;

c) numărul persoanelor informate despre efectuarea în privința acestora a măsurilor contrainformative;

d) date privind eventuale încălcări la executarea prezentei Legi de către ofițerii de informații.

De asemenea, Subcomisia dată va putea înainta întrebări privind activitatea desfășurată, recomandări Serviciului de Informații și Securitate, va putea solicita inițierea unei anchete parlamentare sau sesiza Procurorul General. De asemenea, aceasta va publica pe pagina web a Parlamentului rezultatele controlului activității informative/contrainformative, în măsura în care să nu dezvăluie informații atribuite la secretul de stat.

8. A fost revăzut mecanismul de realizare a măsurilor contrainformative în rețelele de comunicații electronice. Astfel, textul legii a fost ajustat conform propunerilor și de comun acord cu furnizorii de comunicații electronice, excluzând posibilitatea culegerii informații într-un volum ce depășește mandatul eliberat.

9. Au fost introduse garanții privind realizarea măsurilor contrainformative contra avocaților și jurnaliștilor. Astfel, în demersul înaintat pentru autorizarea măsurii se va menționa expres dacă persoana vizată are statut de avocat sau jurnalist, astfel judecătorul va cunoaște că măsura este îndreptată în privința acestora.

De asemenea, s-a instituit interdicția autorizării măsurilor cu privire la raporturile legale de asistență juridică dintre avocat și clientul său și în privința jurnaliștilor, în scopul stabilirii surselor de informații ale acestora. În cazul în care astfel de informații vor fi culese accidental, acestea nu pot fi utilizate și se distrug cu autorizarea judecătorului.

10. A fost implementat un mecanism suplimentar privind protecția și gestionarea datelor cu caracter personal. În acest sens, prelucrarea și controlul asupra prelucrării datelor cu caracter personal în cadrul activității informative/ contrainformative se va efectua în condițiile legislației privind protecția datelor cu caracter personal, ținând cont de particularitățile prevăzute de prezenta Lege. Totodată, excepțiile ce vizează prelucrarea datelor cu caracter personal de către serviciul de inteligență, menționate în Directivele UE sau Protocolul de amendare a Convenției nr. 108 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, din 26.06.2020, urmează a fi implementate în legislația specială din domeniul respectiv.

În rezultatul dezbaterilor, cu votul majorității membrilor săi, Comisia se pronunță pentru adoptarea proiectului de lege în cauză de către plenul Parlamentului, în lectura a doua.

**Lilian CARP**  
**Președintele Comisiei**



*Ex: Vitalie Lungu*  
*consultant principal*  
*022 820 519*

## **L E G E**

### **privind activitatea contrainformativă și activitatea informativă externă**

---

Parlamentul adoptă prezenta lege organică

#### **Capitolul I DISPOZIȚII GENERALE**

##### **Articolul 1. Noțiuni, scop și domeniu de reglementare**

(1) Prezenta lege stabilește cadrul normativ al activității contrainformative și activității informative externe (în continuare – *activitate informativă/contrainformativă*), realizate de către Serviciul de Informații și Securitate al Republicii Moldova (în continuare – *Serviciu*) sau, după caz, de Ministerul Apărării, modalitatea și condițiile dispunerii și realizării măsurilor contrainformative și măsurilor informative externe, precum și ale efectuării controlului asupra legalității acestora, garanțiile minime de protecție a persoanelor supuse măsurilor contrainformative.

(2) Activitatea contrainformativă constă din ansamblul măsurilor, acțiunilor, operațiunilor și procedurilor desfășurate de către Serviciu în scopul identificării, prevenirii și contracarării vulnerabilităților, factorilor de risc și amenințărilor, conform competenței stabilite în Legea nr. 136/2023 privind Serviciul de Informații și Securitate al Republicii Moldova.

(3) Activitatea informativă externă constă din ansamblul măsurilor, acțiunilor și operațiunilor desfășurate în scopul planificării, culegerii, verificării, evaluării, prelucrării analitice, stocării, păstrării și valorificării datelor și informațiilor despre posibilitățile reale sau potențiale, despre acțiunile, planurile sau intențiile statelor ori ale organizațiilor străine, ale unor entități anticonstituționale sau ale unor persoane, care constituie sau ar putea constitui factori de risc sau amenințări la adresa securității Republicii Moldova, precum și în scopul obținerii informațiilor relevante pentru asigurarea securității naționale sau

pentru crearea condițiilor favorabile asigurării și promovării intereselor strategice și realizării cu succes a politicii de securitate ale Republicii Moldova.

(4) Desfășurarea activității informative/contrainformative în alte scopuri decât cele indicate în prezenta lege nu se admite.

## **Articolul 2.** Principiile desfășurării activității informative/contrainformative

Activitatea informativă/contrainformativă se desfășoară conform următoarelor principii:

- a) legalitate;
- b) egalitatea tuturor în fața legii;
- c) respectarea drepturilor și libertăților fundamentale și reglementarea exclusiv prin lege a restrângerii exercițiului acestora;
- d) neutralitate politică și imparțialitate;
- e) îmbinarea metodelor și mijloacelor de activitate publică și secretă;
- f) oportunitate;
- g) proporționalitate;
- h) caracterul activ al măsurilor realizate;
- i) confidențialitate;
- j) eficiență și eficacitate.

## **Articolul 3.** Subiecții care desfășoară activitate informativă/contrainformativă

(1) Activitatea informativă/contrainformativă este desfășurată de către Serviciu prin intermediul ofițerilor de informații și securitate (în continuare – *ofițeri de informații*) din cadrul subunităților specializate ale acestuia.

(2) Activitatea informativă externă în domeniul militar este desfășurată de către Ministerul Apărării prin intermediul militarilor prin contract din cadrul organelor și structurilor specializate ale acestuia.

(3) Alte entități sau persoane decât cele prevăzute de prezentul articol nu sunt în drept să desfășoare activitate informativă/contrainformativă.

## **Articolul 4.** Drepturile, împuternicirile și obligațiile subiecților care desfășoară activitate informativă/contrainformativă

(1) În cadrul desfășurării activității informative/contrainformative, Serviciul și ofițerii de informații dispun de drepturile, împuternicirile și au obligațiile stabilite în Legea nr. 136/2023 privind Serviciul de Informații și Securitate al

Republicii Moldova și în Legea nr. 170/2007 privind statutul ofițerului de informații și securitate.

(2) În cadrul desfășurării activității informative externe în domeniul militar, Ministerul Apărării și militarilor prin contract dispun de drepturile, împuternicirile și au obligațiile stabilite în Legea nr. 162/2005 privind statutul militarului și în alte acte normative în domeniul apărării.

#### **Articolul 5. Utilizarea mijloacelor tehnice la desfășurarea activității informative/contrainformative**

În procesul desfășurării activității informative/contrainformative este permisă utilizarea sistemelor informaționale, a mijloacelor tehnice speciale destinate pentru obținerea ascunsă a informației, a aparatelor de înregistrare video/audio și a altor mijloace tehnice.

#### **Articolul 6. Dosarul special**

(1) În scopul acumulării și sistematizării informațiilor, al verificării și evaluării rezultatelor activității informative/contrainformative, precum și al adoptării în baza acestora a deciziilor corespunzătoare, sunt deschise dosare speciale la care se anexează toate informațiile și materialele colectate. Deschiderea dosarului special este supusă înregistrării obligatorii.

(2) Dosarul special este deschis:

a) în baza raportului ofițerului de informații din cadrul subunității specializate, aprobat de către directorul Serviciului sau directorul adjunct împuternicit în acest sens;

b) în baza raportului militarului prin contract din cadrul organelor și structurilor specializate ale Ministerului Apărării, aprobat de către conducătorul organului sau structurii respective.

Dosarul special se consideră deschis din data înregistrării acestuia.

(3) Măsurile contrainformative și măsurile informative externe nu pot fi desfășurate în afara unui dosar special.

(4) Fiecare dosar special prevede un mecanism de evidență a persoanelor care au luat cunoștință de informațiile și materialele dosarului, care să includă cel puțin:

a) numele, prenumele și funcția persoanei respective;

b) data și ora începerii studierii informațiilor și materialelor dosarului și data și ora finalizării acesteia;

- c) menționați vizând accesul la dosarul special integral, la anumite documente, sau compartimente ale acestuia;
- d) semnătura persoanei respective.

(5) Serviciul și Ministerul Apărării asigură măsurile necesare pentru a proteja informațiile și materialele păstrate în dosarele speciale împotriva dezvăluirii, modificării sau distrugerii neautorizate.

#### **Articolul 7. Gestionarea dosarului special clasat**

(1) După clasare, dosarul special se păstrează în depozitul special al Serviciului sau, după caz, cel al Ministerului Apărării. Termenul de păstrare al dosarului special clasat este echivalent termenului de secretizare.

(2) După expirarea termenului de păstrare al dosarului special clasat se decide asupra prelungirii termenului de secretizare, conform Legii nr. 245/2008 cu privire la secretul de stat, sau asupra distrugerii acestuia, iar dacă informațiile și materialele dosarului au valoare istorică sau științifică, acestea se desecretizează și se transmit spre păstrare în Arhiva Națională a Republicii Moldova.

#### **Articolul 8. Reglementarea departamentală a activității informative/contrainformative**

Organizarea, metodele desfășurării măsurilor contrainformative și celor informative externe; procedurile interne de autorizare, regulile de întocmire a proceselor-verbale cu privire la gestionarea, păstrarea și distrugerea informațiilor și materialelor obținute, măsurile de asigurare a integrității și confidențialității acestora și a activităților informative/contrainformative; regulile de desfășurare a operațiunilor sub acoperire și cu privire la conducerea și gestionarea activității realizate sub acoperire; modul de înregistrare a dosarelor speciale, categoria acestora, deschiderea, gestionarea, clasarea, termenele de păstrare și procedura de distrugere a acestora; utilizarea resurselor financiare alocate pentru realizarea măsurilor contrainformative și celor informative externe; modalitatea de conlucrare cu persoanele care colaborează confidențial cu Serviciul sau, după caz, cu Ministerul Apărării, inclusiv modul de documentare a informațiilor prezentate de către aceștia, categoriile acestor persoane; organizarea, personalul și resursele, sursele, planurile, procedura, tactica, metodele și mijloacele desfășurării activității informative/contrainformative, precum și valorificarea rezultatelor acesteia constituie informații atribuite la secretul de stat și sunt reglementate prin actele interne ale Serviciului sau, după caz, ale Ministerului Apărării.

## **Capitolul II MĂSURILE CONTRAINFORMATIVE**

### **Secțiunea 1 Autorizarea măsurilor contrainformative**

#### **Articolul 9. Măsurile contrainformative**

(1) În cadrul desfășurării activității contrainformative pot fi realizate următoarele măsuri contrainformative:

1) cu autorizarea directorului Serviciului sau a directorului adjunct împuternicit – identificarea abonatului sau a utilizatorului unei rețele de comunicații electronice ori a unui serviciu al societății informaționale;

2) cu mandat judecătoresc:

a) cercetarea domiciliului și/sau, după caz, instalarea în acesta a aparatelor care asigură supravegherea video/audio, fotografierea sau constatarea unor circumstanțe de fapt;

b) supravegherea domiciliului prin utilizarea mijloacelor tehnice;

c) interceptarea comunicărilor;

d) obținerea accesului la informația care se află sau se procesează într-un sistem informatic, pe dispozitive sau echipamente de comunicații și/sau monitorizarea acesteia;

e) colectarea informației de la furnizorii de servicii de comunicații electronice;

f) reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimiterilor poștale;

g) înregistrarea video/audio a conținutului comunicărilor;

h) blocarea accesului la rețelele de comunicații electronice pentru un sistem informatic, un dispozitiv sau un echipament ori pentru o societate informațională, blocarea unor servicii de comunicații electronice;

i) ridicarea operativă;

j) obținerea accesului la informația financiară sau monitorizarea tranzacțiilor financiare;

k) urmărirea vizuală și/sau documentarea cu ajutorul metodelor și mijloacelor tehnice, precum și localizarea ori urmărirea prin sistemul de poziționare globală sau prin alte mijloace tehnice.

(2) Lista măsurilor indicate la alin. (1) este exhaustivă și poate fi modificată sau completată doar prin lege.

#### **Articolul 10. Temeiurile desfășurării măsurilor contrainformative**

Drept temeieri pentru desfășurarea măsurilor contrainformative pot servi:

1) informațiile privind:

a) pericolele indicate la art. 4 alin. (2) din Legea securității statului nr. 618/1995 și faptele indicate la art. 3 pct. 2) lit. b) și c) din Legea nr. 136/2023 privind Serviciul de Informații și Securitate al Republicii Moldova;

b) circumstanțele care pun în pericol securitatea investigatorului sub acoperire, a ofițerului de informații, a persoanelor care colaborează confidențial cu Serviciul sau a membrilor familiilor lor;

2) interpelările organizațiilor internaționale sau ale autorităților altor state, în conformitate cu tratatele internaționale la care Republica Moldova este parte sau în baza acordurilor de colaborare între Serviciu și autoritățile de profil din alte state;

3) necesitatea de a obține informații în interesul asigurării securității Republicii Moldova, al menținerii și dezvoltării potențialului ei tehnico-științific, economic sau de apărare, al creării condițiilor pentru promovarea politicii externe și interne;

4) asigurarea protecției secretului de stat;

5) colectarea informațiilor necesare cu privire la persoanele supuse verificării pentru:

a) acordarea accesului la informații ce constituie secret de stat;

b) admiterea la muncă la obiectivele infrastructurii critice;

c) stabilirea sau întreținerea relațiilor de colaborare cu acestea la organizarea și desfășurarea măsurilor contrainformative și/sau informative externe;

6) verificarea candidaților sau titularilor funcțiilor publice;

7) asigurarea securității interne;

8) colectarea informațiilor necesare cu privire la persoanele care colaborează confidențial cu Serviciul, precum și cu privire la persoanele supuse verificării pentru admiterea acestora la organizarea și desfășurarea unor măsuri contrainformative și/sau informative externe ori pentru acordarea accesului la informațiile și materialele acumulate pe parcursul realizării acestor măsuri.

#### **Articolul 11. Procedura autorizării măsurilor contrainformative de către directorul Serviciului sau directorul adjunct împuternicit**

(1) Realizarea măsurii contrainformative prevăzute la art. 9 alin. (1) pct. 1) se autorizează, prin ordonanță, de către directorul Serviciului sau directorul adjunct împuternicit în acest sens, în baza demersului conducătorului subunității care desfășoară activitatea contrainformativă în cadrul unui dosar special deschis și înregistrat.

(2) Demersul indicat la alin. (1) cuprinde: circumstanțele de fapt care servesc drept temei pentru realizarea măsurii contrainformative; argumentarea necesității măsurii respective; numărul dosarului special în cadrul căruia urmează a fi realizată măsura contrainformativă.

(3) Pentru emiterea ordonanței indicate la alin. (1), directorul Serviciului sau directorul adjunct împuternicit, pe lângă temeinicia demersului, examinează suplimentar dacă:

- a) măsura solicitată urmărește un scop legitim;
- b) măsura este proporțională cu restrângerea exercițiului drepturilor sau libertăților persoanei, garantate de lege, și cu necesitatea realizării acesteia.

(4) Ordonanța directorului Serviciului sau a directorului adjunct împuternicit cuprinde:

- a) data emiterii;
- b) numărul dosarului special în cadrul căruia este autorizată măsura contrainformativă;
- c) măsura contrainformativă autorizată.

(5) Directorul Serviciului, directorul adjunct împuternicit refuză autorizarea măsurii contrainformative dacă constată că demersul prezentat este neîntemeiat, nu urmărește un scop legitim sau măsura solicitată este disproporțională în raport cu restrângerea exercițiului drepturilor sau libertăților persoanei.

#### **Articolul 12. Procedura autorizării măsurilor contrainformative prin emiterea mandatului judecătoresc**

(1) În sensul prezentei legi, mandatul judecătoresc reprezintă autorizarea de a realiza, în cadrul unui dosar special deschis și înregistrat, măsurile contrainformative prevăzute la art. 9 alin. (1) pct. 2).

(2) Mandatul judecătoresc este emis, în baza demersului în formă scrisă al directorului Serviciului sau al directorului adjunct împuternicit, de către un judecător din cadrul Curții de Apel Chișinău desemnat în acest sens.

(3) Demersul pentru emiterea mandatului judecătoresc conține următoarele informații:

- a) numele, prenumele și funcția persoanei care solicită emiterea mandatului judecătoresc;
- b) datele de identitate ale persoanei supuse măsurii contrainformative, dacă acestea sunt cunoscute;
- c) deținerea statutului de avocat sau de jurnalist de către persoana supusă măsurii contrainformative și circumstanțele de fapt care exclud incidența interdicției stabilite la alin. (6);
- d) măsura contrainformativă pentru care se solicită autorizarea;
- e) circumstanțele de fapt care servesc drept temei pentru realizarea măsurii contrainformative și, după caz, consecințele posibile ale acesteia;
- f) argumentarea proporționalității măsurii contrainformative, pentru care se

solicită autorizarea, cu restrângerea exercițiului drepturilor sau libertăților persoanei;

g) în cazul solicitării prelungirii termenului de realizare a măsurii contrainformative, temeiurile și motivele care justifică prelungirea;

h) rezultatele care se preconizează a fi obținute în urma realizării măsurii contrainformative;

i) termenul de realizare a măsurii respective;

j) locul desfășurării măsurii contrainformative;

k) alte informații care au importanță pentru justificarea măsurii contrainformative și care ar susține legalitatea și temeinicia autorizării acesteia.

(4) Examinarea demersului pentru emiterea mandatului judecătoresc are loc în decurs de 24 de ore. La solicitarea judecătorului, la examinarea demersului participă și ofițerul de informații, care dă explicațiile de rigoare. Pe parcursul examinării demersului, judecătorului, la solicitarea acestuia sau din inițiativa Serviciului, i se prezintă informațiile și materialele care justifică necesitatea realizării măsurii respective, fără a dezvălui datele de identificare ale persoanelor care colaborează confidențial cu Serviciul.

(5) Pentru emiterea mandatului judecătoresc, judecătorul verifică suplimentar dacă:

a) măsura solicitată urmărește un scop legitim;

b) este imposibilă realizarea scopului prevăzut de prezenta lege pe altă cale;

c) măsura solicitată este proporțională cu restrângerea exercițiului drepturilor și libertăților fundamentale.

(6) Este interzisă autorizarea realizării măsurilor contrainformative:

a) în privința raporturilor legale de asistență juridică dintre avocat și clientul său;

b) în privința jurnaliștilor, cu scopul stabilirii surselor de informații ale acestora.

(7) Informațiile care cad sub incidența alin. (6) și care au fost colectate accidental nu pot fi folosite de către Serviciu și se distrug, cu autorizarea judecătorului.

(8) După verificarea legalității și a temeiniciei demersului indicat la alin. (2), judecătorul, prin încheiere, autorizează realizarea măsurii contrainformative sau respinge demersul. În temeiul încheierii privind autorizarea, judecătorul emite un mandat judecătoresc care este obligatoriu pentru executare.

(9) Mandatul judecătoresc se transmite nu mai târziu de 24 de ore de la depunerea demersului pentru emiterea acestuia. Încheierea motivată este redactată și emisă în cel mult 48 de ore.

(10) Încheierea indicată la alin. (8) conține următoarele informații: data și locul întocmirii încheierii; numele și prenumele judecătorului; numele, prenumele și funcția persoanei care solicită emiterea mandatului judecătoresc; organul care va realiza măsurile contrainformative; datele de identitate ale persoanei supuse măsurilor contrainformative, dacă acestea sunt cunoscute; temeiurile și motivele care justifică necesitatea realizării și, respectiv, autorizării măsurilor contrainformative; măsurile contrainformative autorizate; termenul de realizare a măsurilor contrainformative; locul desfășurării măsurilor contrainformative; alte informații care au importanță pentru justificarea autorizării măsurilor contrainformative.

(11) Măsurile contrainformative care pot fi realizate doar cu mandat judecătoresc pot fi desfășurate, ca excepție, fără mandat judecătoresc, în baza ordonanței motivate a directorului Serviciului sau a directorului adjunct împuternicit, în cazul în care există circumstanțe excepționale care nu permit amânarea acesteia, iar mandatul judecătoresc nu poate fi obținut fără expunerea la un risc esențial de întârziere care să poată duce la pierderea informațiilor relevante sau să pună într-un pericol iminent securitatea statului sau a persoanelor. În acest caz, judecătorul este informat în termen de 24 de ore de la dispunerea măsurii contrainformative despre desfășurarea acesteia, prezentându-i-se toate informațiile și materialele în care este argumentată necesitatea realizării măsurii respective și circumstanțele excepționale care nu au permis amânarea acesteia. Dacă există temeiuri și motive suficiente, judecătorul confirmă, prin încheiere motivată, legalitatea realizării măsurii contrainformative. În caz contrar, judecătorul declară ilegalitatea desfășurării măsurii respective.

(12) Măsurile contrainformative inițiate în temeiul alin. (11) se desfășoară până la emiterea încheierii motivate a judecătorului, ulterior procedându-se conform încheierii respective.

(13) Concomitent cu confirmarea legalității realizării măsurilor contrainformative, judecătorul, la solicitarea directorului Serviciului sau a directorului adjunct împuternicit, emite mandat judecătoresc privind autorizarea continuării desfășurării acestora.

(14) La declararea ilegalității desfășurării măsurii contrainformative, realizarea măsurii respective se sistează.

(15) Încheierea motivată a judecătorului privind respingerea demersului pentru emiterea mandatului judecătoresc, precum și încheierea motivată privind declararea ilegalității desfășurării măsurii contrainformative pot fi contestate de către Serviciu cu recurs la Curtea Supremă de Justiție.

(16) Recursul indicat la alin. (15) se examinează de un complet de 3 judecători, în condițiile alin. (4).

(17) Recursul indicat la alin. (15) se depune în termen de 3 zile lucrătoare de la data emiterii încheierii motivate și conține temeiurile de fapt și de drept privind netemeinicia și/sau ilegalitatea încheierii contestate.

(18) După examinarea recursului indicat la alin. (15), completul Curții Supreme de Justiție, prin decizie:

- a) admite recursul, casează încheierea și, după caz, emite mandat judecătoresc sau confirmă legalitatea realizării măsurilor contrainformative;
- b) respinge recursul și menține încheierea.

(19) Redactarea și emiterea deciziei indicate la alin. (18) se efectuează în conformitate cu prevederile alin. (9).

### **Articolul 13. Condițiile speciale de realizare a măsurilor contrainformative autorizate prin mandat judecătoresc**

(1) Realizarea măsurilor contrainformative se autorizează în temeiurile prevăzute la art. 10.

(2) În temeiurile indicate la art. 10 pct. 4)–6) poate fi autorizată realizarea doar a măsurilor contrainformative prevăzute la art. 9 alin. (1) pct. 1) și pct. 2) lit. e) și j).

(3) Cu acordul expres sau la cererea prealabilă, în formă scrisă, a persoanelor care contribuie la desfășurarea activității informative/contrainformative, pot fi realizate măsurile contrainformative prevăzute de prezenta lege, atât în privința acestora, cât și a rudelor și a membrilor familiilor lor, dacă există un pericol iminent la adresa vieții, sănătății sau a altor drepturi fundamentale ale acestora ori dacă realizarea măsurilor respective este necesară pentru prevenirea unei infracțiuni sau a unor consecințe nefavorabile care vizează persoanele menționate.

**Articolul 14.** Termenul pentru care se autorizează realizarea măsurilor contrainformative

(1) Măsurile contrainformative prevăzute la art. 9 alin. (1) pct. 2) care nu reprezintă măsuri de realizare unică, cu excepția celor prevăzute la art. 9 alin. (1) pct. 2) lit. a), se autorizează pentru un termen de până la 90 de zile, cu posibilitatea prelungirii acestuia cu perioade succesive, precum și cu perioade care nu se succed, de până la 90 de zile.

(2) Măsura contrainformativă prevăzută la art. 9 alin (1) pct. 2) lit. a) se autorizează pentru un termen de până la 30 de zile, cu posibilitatea prelungirii acestuia cu perioade succesive, precum și cu perioade care nu se succed, de până la 30 de zile.

(3) Durata totală a desfășurării unei măsuri contrainformative în privința unei persoane, dispusă cu privire la o faptă concretă, nu poate depăși, cumulativ, 24 de luni, iar finalizarea acesteia nu poate avea loc peste mai mult de 4 ani de la inițierea măsurii. La fiecare solicitare privind prelungirea termenului de realizare a măsurii contrainformative, judecătorul are obligația de a examina temeiurile și motivele care justifică prelungirea acestuia, iar în cazul în care consideră că solicitarea respectivă nu este motivată, respinge prelungirea termenului.

(4) Desfășurarea măsurilor contrainformative trebuie să înceapă la data indicată în actul prin care s-a dispus realizarea acesteia sau, cel târziu, la data expirării termenului pentru care măsura respectivă a fost autorizată.

**Articolul 15.** Încetarea desfășurării măsurii contrainformative înainte de termen

Directorul Serviciului sau directorul adjunct împuternicit dispune, prin ordonanță, încetarea măsurii contrainformative înainte de expirarea termenului pentru care a fost emis mandat judecătoresc imediat ce au dispărut temeiurile și motivele care au justificat autorizarea măsurii. Despre încetarea înainte de termen a măsurii contrainformative și temeiurile încetării este informat judecătorul care a eliberat mandatul judecătoresc.

**Articolul 16.** Consemnarea măsurilor contrainformative

(1) După finalizarea desfășurării măsurii contrainformative și constatarea lipsei necesității continuării acesteia sau după încetarea acesteia înainte de termen, ofițerul de informații care a realizat măsura respectivă întocmește câte un proces-verbal pentru fiecare măsură contrainformativă autorizată, în care consemnează:

a) denumirea măsurii contrainformative realizate, locul și data desfășurării acesteia, după caz, ora începerii și finalizării acesteia, date cu privire la autorizarea măsurii sau cu privire la mandatul judecătoresc;

b) funcția, numele și prenumele ofițerului de informații care întocmește procesul-verbal. Dacă măsura contrainformativă a fost realizată nemijlocit de către ofițerii de informații din cadrul subunităților de asigurare a activității informative/contrainformative care fac parte din personalul criptic al Serviciului, în procesul-verbal se indică funcția, numele și prenumele conducătorului subunității respective, care verifică corectitudinea informațiilor indicate în procesul-verbal și îl semnează. În cadrul subunităților menționate se ține evidența strictă a ofițerilor de informații care au realizat măsuri contrainformative și au întocmit procese-verbale;

c) numele, prenumele și statutul persoanelor care au participat la realizarea măsurii. Datele respective nu se consemnează în procesul-verbal în cazul ofițerilor de informații din cadrul subunităților de asigurare a activității informative/contrainformative care fac parte din personalul criptic al Serviciului, precum și nici în cazul persoanelor care colaborează confidențial cu Serviciul;

d) faptele constatate, precum și acțiunile întreprinse în cadrul realizării măsurii contrainformative;

e) informațiile privind utilizarea mijloacelor tehnice, condițiile și modalitățile de aplicare a acestora, obiectele față de care au fost aplicate mijloacele respective, rezultatele obținute; mențiunea privind înregistrarea informațiilor acumulate.

(2) În cazul înregistrării rezultatelor măsurii contrainformative, la procesul-verbal se anexează suportul material al informațiilor.

(3) Procesul-verbal și suportul material al informațiilor se anexează la dosarul special.

#### **Articolul 17. Verificarea legalității realizării măsurilor contrainformative de către judecător**

(1) După finalizarea desfășurării măsurii contrainformative și constatarea lipsei necesității continuării acesteia sau după încetarea acesteia înainte de termen, pentru verificarea respectării legalității măsurii, ofițerul de informații transmite, în termen de 10 zile lucrătoare, judecătorului care a autorizat măsura respectivă procesul-verbal privind măsura contrainformativă, la care anexează toate informațiile și materialele acumulate ca urmare a realizării acesteia.

(2) În procesul de verificare a respectării legalității, judecătorul stabilește dacă măsura contrainformativă a fost realizată: în privința persoanelor și pentru investigarea faptelor, indicate în demersul pentru emiterea mandatului

judecătoresc; conform mandatului judecătoresc emis; cu respectarea termenelor de realizare.

(3) Dacă măsura a fost realizată în conformitate cu legislația, judecătorul, prin încheiere, confirmă legalitatea realizării măsurii contrainformative.

(4) În cazul în care judecătorul constată că măsura contrainformativă s-a desfășurat cu încălcarea vădită a drepturilor și libertăților persoanei ori au fost depășite prevederile mandatului judecătoresc, acesta, prin încheiere, declară drept nule rezultatele măsurii contrainformative și informează Procuratura Generală pentru investigarea încălcărilor admise.

(5) Încheierea privind declararea drept nule a rezultatelor măsurii contrainformative poate fi contestată cu recurs conform prevederilor art. 12.

(6) Originalul suportului material al informațiilor care conține înregistrările datelor obținute, după verificarea legalității conform prezentului articol, este sigilat de către judecător și se păstrează în cadrul Serviciului într-un mod care să asigure nonrepudierea informației și să excludă accesul ofițerului de informații care a desfășurat cercetarea cazului. La dosarul special se anexează o copie a suportului respectiv. Originalul suportului material se prezintă în cadrul controlului sau poate fi utilizat în alte scopuri, cu autorizarea judecătorului, la solicitarea motivată a directorului Serviciului sau directorului adjunct împuternicit.

#### **Articolul 18. Utilizarea rezultatelor măsurilor contrainformative**

(1) Rezultatele realizării măsurilor contrainformative sunt utilizate:

- a) la realizarea atribuțiilor Serviciului;
- b) la desfășurarea altor măsuri contrainformative.

(2) În cazul în care în urma desfășurării măsurilor contrainformative se constată că există bănuieli rezonabile cu privire la săvârșirea unei infracțiuni sau pregătirea săvârșirii acesteia, printr-un raport este informat neîntârziat procurorul desemnat în acest sens din cadrul Procuraturii Generale.

(3) Rezultatele măsurilor contrainformative din cadrul unui dosar special pot fi utilizate în cadrul altui dosar special doar cu autorizarea judecătorului care a emis mandatul judecătoresc.

(4) Rezultatele realizării măsurilor contrainformative nu sunt admise ca probe în procesul penal.

**Articolul 19.** Confidențialitatea informației cu privire la măsurile contrainformative și cele informative externe

(1) Informația cu privire la desfășurarea măsurilor contrainformative și celor informative externe, cu privire la personalul, resursele, sursele, mijloacele, metodele, planurile și rezultatele activității informative/contrainformative, precum și cu privire la organizarea, procedurile și tactica desfășurării măsurilor contrainformative și celor informative externe constituie secret de stat și poate fi desecretizată numai în conformitate cu legislația.

(2) Persoanele care au luat cunoștință, în virtutea funcției, statutului, circumstanțelor sau întâmplător, de desfășurarea măsurilor contrainformative sau celor informative externe ori de rezultatele acestora sunt obligate să păstreze confidențialitatea informațiilor respective.

(3) Orice divulgare neautorizată a informațiilor indicate la alin. (1) atrage răspunderea prevăzută de legislație.

**Articolul 20.** Informarea persoanei despre măsurile contrainformative realizate în privința sa

(1) După finalizarea cercetării cauzei și clasării dosarului special, dacă în cadrul acestuia au fost realizate măsurile contrainformative prevăzute la art. 9 alin. (1) pct. 2), Serviciul, în termen de 5 zile lucrătoare de la data clasării dosarului respectiv, informează persoanele în privința cărora au fost realizate măsurile respective. Materialele ce atestă informarea persoanelor se anexează la dosarul special.

(2) În fiecare caz în care este informată o persoană conform alin. (1), Serviciul notifică despre aceasta judecătorul care a emis mandatul judecătoresc.

(3) Informarea persoanei nu are loc dacă există motive întemeiate de a considera că aceasta ar putea expune unui risc esențial viața sau sănătatea persoanelor, ar periclita altă investigație în desfășurare, ar dăuna securității statului sau ar aduce prejudicii scopului pentru care au fost realizate măsurile contrainformative.

(4) Cu privire la existența motivelor menționate la alin. (3) ofițerul de informații care a efectuat cercetarea cauzei întocmește un raport în formă scrisă, în care specifică detaliat motivele respective și îl prezintă spre aprobare directorului Serviciului. Dacă raportul este aprobat, directorul Serviciului solicită judecătorului care a emis mandatul judecătoresc autorizarea neinformării persoanei.

(5) În urma examinării demersului directorului Serviciului indicat la alin. (4), judecătorul constată existența sau lipsa temeiurilor pentru neinformarea persoanei, stabilește dacă temeiurile respective au caracter permanent sau provizoriu și, după caz, autorizează neinformarea persoanei sau respinge demersul. În funcție de caracterul permanent sau provizoriu al temeiurilor constatate, judecătorul poate autoriza neinformarea permanentă sau neinformarea pentru o perioadă determinată, dar nu mai mare de 1 an. La expirarea perioadei respective, Serviciul este obligat să reevalueze temeiurile care au stat la baza neinformării persoanei și să întreprindă acțiunile necesare, în conformitate cu prevederile prezentului articol, inclusiv, după caz, să solicite autorizarea neinformării persoanei pentru o nouă perioadă. Respingerea demersului pentru autorizarea neinformării persoanei poate fi contestată de către Serviciu cu recurs, aplicându-se, corespunzător, prevederile art. 12.

(6) În cazul în care temeiurile care au stat la baza neinformării persoanei supuse măsurii contrainformative au dispărut înainte de expirarea perioadei stabilite, ofițerul de informații întocmește un raport în acest sens și îl prezintă spre aprobare directorului Serviciului, prin care solicită informarea neîntârziată a persoanei în privința căreia a fost realizată măsura respectivă. În cazul aprobării raportului, persoana este informată în condițiile alin. (1).

(7) Încheierea judecătorului privind autorizarea neinformării persoanei, precum și rapoartele aprobate de către directorul Serviciului se anexează la dosarul special.

## **Secțiunea a 2-a** **Măsurile contrainformative**

### **Articolul 21. Identificarea abonatului sau utilizatorului unei rețele de comunicații electronice ori al unui serviciu al societății informaționale**

(1) Identificarea abonatului sau utilizatorului unei rețele de comunicații electronice ori al unui serviciu al societății informaționale constă în stabilirea datelor de identificare ale abonatului sau ale utilizatorului unei rețele de comunicații electronice (identificatorul internațional al abonatului mobil (IMSI), numărul de telefon, numărul de serie al modulului de identificare a abonatului (al cartelei SIM), adresa de internet protocol (IP), adresele fizice de prestare a serviciului fix) ori al unui serviciu al societății informaționale, precum și a datelor de identificare ale abonaților (numele, prenumele, IDNP, adresa), ori în stabilirea faptului dacă un serviciu de comunicații electronice este activ sau a fost activ la o anumită dată, ori în stabilirea, fără suportul furnizorului de servicii electronice, prezenței mijloacelor de comunicații electronice într-un moment dat la o persoană.

(2) În cazul în care măsura contrainformativă se realizează cu suportul unui furnizor de servicii electronice, acestuia i se prezintă extrasul din ordonanța corespunzătoare a directorului Serviciului sau a directorului adjunct împuternicit privind autorizarea măsurii, în care este indicat doar tipul informației care urmează a fi prezentată. După recepționarea extrasului din ordonanță, furnizorul de servicii electronice prezintă informațiile solicitate în cel mai restrâns termen, fără păstrarea copiei (inclusiv în format electronic) a răspunsului și datelor remise.

**Articolul 22.** Cercetarea domiciliului și/sau, după caz, instalarea în acesta a aparatelor care asigură supravegherea video/audio, fotografierea sau constatarea unor circumstanțe de fapt

(1) Cercetarea domiciliului și/sau, după caz, instalarea în acesta a aparatelor ce asigură supravegherea video/audio, fotografierea sau constatarea unor circumstanțe de fapt presupune accesul secret sau legendat în interiorul domiciliului, fără înștiințarea proprietarului, a posesorului sau a persoanei care locuiește sau se află în domiciliul respectiv, în scopul instalării aparatelor care să asigure supravegherea, precum și al studierii acestuia pentru descoperirea urmelor activității, persoanelor care prezintă interes, pentru obținerea altor informații necesare constatării circumstanțelor de fapt, observării și înregistrării evenimentelor care se desfășoară în domiciliu. Aparatele care asigură supravegherea efectuează interceptarea și înregistrarea de la distanță a informației sau înregistrarea informației nemijlocit în domiciliu, cu ridicarea ulterioară a acestora.

(2) În cadrul cercetării domiciliului este permisă prelevarea mostrelor pentru cercetarea comparativă, dacă aceasta nu va duce la deconspirarea măsurii contrainformative realizate.

(3) După expirarea termenului de realizare a măsurii sau în cazul încetării măsurii înainte de termen, este permis accesul secret sau legendat în domiciliu, cu autorizarea prealabilă a directorului Serviciului sau directorului adjunct împuternicit, pentru demontarea aparatelor respective. În acest caz, domiciliul nu se cercetează și nu se întreprind alte acțiuni decât cele de demontare a aparatelor. Cu privire la pătrunderea în domiciliu și demontarea aparatelor se întocmește un proces-verbal, în care se indică data și persoanele care au pătruns în domiciliu. Procesul-verbal se remite pentru informare judecătorului care a autorizat măsura respectivă.

(4) Demontarea aparatelor are loc într-un termen cât mai restrâns, după expirarea termenului de realizare a măsurii sau după încetarea măsurii. Se interzice utilizarea în orice mod a informației înregistrate după expirarea termenului de

realizare a măsurii sau după încetarea măsurii, inclusiv vizualizarea sau audierea acesteia, informația respectivă fiind distrusă neîntârziat.

### **Articolul 23. Supravegherea domiciliului prin utilizarea mijloacelor tehnice**

Supravegherea domiciliului prin utilizarea mijloacelor tehnice presupune supravegherea domiciliului din exterior, fără acordul proprietarului, al posesorului sau al persoanei care locuiește sau se află în domiciliul respectiv, prin utilizarea mijloacelor tehnice, în scopul stabilirii evenimentelor ce se desfășoară în interiorul domiciliului, a convorbirilor, a altor sunete sau circumstanțe de fapt, cu înregistrarea celor stabilite.

### **Articolul 24. Interceptarea comunicărilor**

(1) Interceptarea comunicărilor reprezintă accesul și monitorizarea în regim de timp real a conținutului comunicărilor efectuate prin intermediul rețelelor de comunicații electronice sau al altor mijloace tehnice de comunicare, cu înregistrarea comunicărilor respective, precum și colectarea, înregistrarea în regim de timp real a tipului comunicării, a datelor de trafic (transfer) și a datelor de localizare asociate comunicărilor respective.

(2) Mandatul judecătoresc pentru autorizarea efectuării interceptării comunicărilor trebuie să conțină, suplimentar, identificatorii tehnici sau datele de identificare ale abonatului sau ale echipamentului prin intermediul căruia se realizează comunicările care urmează a fi interceptate.

### **Articolul 25. Efectuarea și certificarea interceptării comunicărilor**

(1) Asigurarea tehnică a interceptării comunicărilor se realizează de către subunitatea specializată a Serviciului, cu utilizarea produselor de program sau a mijloacelor tehnice speciale conectate, în caz de necesitate, la echipamentul furnizorilor de rețele/de servicii de comunicații electronice și/sau la dispozitivele persoanei interceptate. Ofițerii de informații ai subunității care asigură tehnic interceptarea comunicărilor, angajații care efectuează nemijlocit ascultarea înregistrărilor, vizualizarea informațiilor comunicate, traducerea acestora, întocmirea stenogramei sunt obligați să păstreze secretul informațiilor obținute și poartă răspundere pentru încălcarea acestei obligații.

(2) Informația obținută în procesul interceptării comunicărilor poate fi ascultată și vizualizată de către ofițerul de informații în regim de timp real.

(3) Stenograma constituie reproducerea în formă scrisă a comunicărilor interceptate care au importanță pentru dosarul special. În stenograma comunicărilor se indică data, ora și durata comunicării, numele persoanelor ale căror comunicări sunt stenografiate, dacă sunt cunoscute, precum și alte date relevante. Stenograma se întocmește de către angajații subunității care asigură activitatea informativă/contrainformativă, iar în caz de necesitate sau la solicitarea ofițerului de informații care realizează măsura contrainformativă – personal de către acesta.

(4) Comunicările interceptate se stenografiază, de regulă, în limba în care a avut loc comunicarea. În cazul în care comunicarea a avut loc în altă limbă decât limba română, comunicarea se traduce în limba română de către un traducător.

(5) În cadrul subunității de asigurare a activității informative/contrainformative se ține evidența strictă a ofițerilor de informații care au avut acces la comunicarea interceptată, a angajaților care au întocmit stenograma sau au tradus comunicarea.

(6) Comunicările interceptate se păstrează integral pe suportul material oferit de către subunitatea specializată ofițerului de informații. Acest suport se păstrează în dosarul special. Accesul la suportul respectiv este supus evidenței, fiind înregistrate:

- a) numele, prenumele și funcția persoanei care a avut acces;
- b) data și ora inițierii accesului și data și ora finalizării accesului;
- c) mențiuni despre faptul dacă s-a ascultat/vizualizat informația înregistrată pe suportul material;
- d) temeiul/motivul ascultării/vizualizării informației;
- e) semnătura persoanei care a avut acces.

**Articolul 26.** Accesul la informația care se află sau se procesează într-un sistem informatic, pe dispozitive sau echipamente de comunicații și/sau monitorizarea acesteia

(1) Accesul la informația care se află într-un sistem informatic, pe dispozitive sau echipamente de comunicații presupune întreprinderea unor acțiuni care să permită obținerea informației care se află într-un sistem informatic, pe dispozitive sau echipamente de comunicații ori este stocată pe un alt suport tehnic, cu înregistrarea informației necesare pe un suport material.

(2) Monitorizarea informației care se află sau se procesează într-un sistem informatic, pe dispozitive sau echipamente de comunicații presupune întreprinderea unor măsuri care să permită monitoringul, în regim de timp real, al acțiunilor care se întreprind într-un sistem informatic, în dispozitiv sau echipament,

să permită obținerea informației care se prelucrează, precum și a datelor informatice asociate acțiunilor respective.

(3) Accesul la informația care se află sau se procesează într-un sistem informatic, pe dispozitive sau echipamente de comunicații și/sau monitorizarea acesteia poate fi efectuată:

a) prin stabilirea unui canal permanent sau temporar de conexiune fizică dintre subunitatea specializată a Serviciului și echipamentul persoanei fizice/juridice care deține sistemul informatic, dispozitivele sau echipamentele de comunicații ori suportul tehnic respectiv;

b) prin intermediul unor produse de program;

c) prin prezentarea nemijlocită către deținătorul sistemului informatic, al dispozitivelor sau echipamentelor de comunicații ori al suportului tehnic a extrasului din mandatul judecătoresc corespunzător, eliberat de către judecător concomitent cu mandatul judecătoresc, în care este indicată tipul de informații care urmează a fi prezentate.

(4) Accesul la informația care se află sau se procesează într-un sistem informatic sau monitorizarea acesteia nu poate fi realizat conform prevederilor prezentului articol dacă prezenta lege prevede o altă modalitate de obținere a informației respective.

#### **Articolul 27. 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 suportul furnizorilor de servicii de comunicații electronice, 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, pentru identificarea destinației, tipului, datei, orei și duratei comunicației electronice, pentru identificarea echipamentului de comunicații electronice al utilizatorului sau a altui dispozitiv utilizat pentru comunicație, pentru identificarea coordonatelor echipamentului terminal de comunicații mobile, informație, în special, despre:

a) numerele de telefon înregistrate pe numele unei persoane;

b) serviciile de comunicații electronice prestate utilizatorului;

c) sursa de comunicații electronice (numărul de telefon sau adresa de internet protocol (IP) ale apelantului);

d) destinația comunicației electronice (numărul de telefon sau adresa de internet protocol (IP) ale apelatului; numărul de telefon spre care este redirecționat apelul);

e) 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 avut loc un răspuns sau a avut loc o intervenție legată de gestionarea rețelei;

f) echipamentul de comunicații electronice al utilizatorului sau un alt dispozitiv utilizat pentru comunicație (identificatorul internațional al echipamentului mobil (IMEI) al apelantului și cel al apelatului; adresa media acces control (adresa MAC) a echipamentului de acces la serviciile fixe amplasat în locația clientului (CPE); în cazul serviciilor preplătite anonime – data și ora la care a fost inițial activat serviciul și denumirea locației (Cell ID) din care a fost activat serviciul);

g) locația 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).

(2) Colectarea informației de la furnizorii de servicii de comunicații electronice se realizează prin prezentarea nemijlocită către furnizorii de servicii de comunicații electronice a extrasului din mandatul judecătoresc corespunzător, eliberat de către judecător concomitent cu mandatul judecătoresc, în care se indică doar tipul de informații care urmează a fi prezentate.

#### **Articolul 28. Reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimiterilor poștale**

(1) Reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimiterilor poștale constă în următoarele acțiuni, întreprinse fără înștiințarea expeditorului și destinatarului trimiterilor poștale:

a) oprirea livrării trimiterii poștale pentru o perioadă strict determinată sau relativ determinată ori livrarea trimiterii poștale la o anumită dată sau într-un anumit interval de timp;

b) accesarea și verificarea trimiterii poștale, vizualizarea și înregistrarea informației existente, identificarea obiectelor sau substanțelor ce se află în trimiterea poștală.

(2) În cadrul realizării măsurilor prevăzute de prezentul articol este permisă:

a) efectuarea constatărilor tehnico-științifice care să permită identificarea obiectelor sau a substanțelor din trimiterea poștală ori a altor circumstanțe de fapt;

b) copierea, înregistrarea pe suport material, cu ajutorul mijloacelor tehnice, a informațiilor care se conțin în trimiterea poștală;

c) prelevarea mostrelor.

(3) Mandatul judecătoresc pentru reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimiterilor poștale trebuie să conțină denumirea instituției poștale asupra căreia se pune obligația de a reține trimiterele poștale, numele și prenumele persoanei sau persoanelor ale căror trimiteri poștale trebuie să

fie reținute, adresele exacte ale persoanelor respective, dacă sunt cunoscute, sau alte elemente caracteristice, în baza cărora se vor putea identifica trimiterile poștale, genul de trimiteri poștale față de care este orientată măsura contrainformativă.

(4) Concomitent cu mandatul judecătoresc, judecătorul eliberează și un extras din acesta care se transmite conducătorului instituției poștale sau furnizorului de trimiteri poștale, pentru care executarea măsurii indicate în extrasul respectiv este obligatorie.

(5) Conducătorul instituției poștale sau furnizorul de trimiteri poștale informează neîntârziat ofițerul de informații despre reținerea trimiterilor poștale indicate în extrasul din mandatul judecătoresc, fiind obligat să asigure și să păstreze confidențialitatea măsurii contrainformative realizate.

#### **Articolul 29. Înregistrarea video/audio a conținutului comunicărilor**

Înregistrarea video/audio a conținutului comunicărilor presupune înregistrarea secretă video/audio a comunicărilor transmise de persoane în spații deschise, în locuri publice sau în încăperi care nu constituie domiciliu, precum și a comunicărilor transmise către sau în prezența unui ofițer de informații sau a unei persoane care colaborează confidențial cu Serviciul, fără a cunoaște statutul acestora.

#### **Articolul 30. Blocarea accesului la rețelele de comunicații electronice pentru un sistem informatic, un dispozitiv sau un echipament ori pentru o societate informațională, blocarea unor servicii de comunicații electronice**

(1) Blocarea accesului la rețelele de comunicații electronice pentru un sistem informatic, un dispozitiv sau un echipament ori pentru o societate informațională, blocarea unor servicii de comunicații electronice presupun:

a) blocarea posibilității accesării unor rețele de comunicații electronice de un sistem informatic, un dispozitiv sau un echipament ori de o societate informațională;

b) suspendarea unui serviciu de comunicații electronice sau a unui serviciu al societății informaționale pentru un număr de telefon, pentru o adresă statică de internet protocol (IP), pentru o persoană sau o adresă fizică.

(2) Acțiunile prevăzute la alin. (1) lit. a) se efectuează de către Serviciu cu utilizarea produselor de program sau a mijloacelor tehnice speciale, iar cele

prevăzute la alin. (1) lit. b) – de către furnizorii de servicii de comunicații electronice, la prezentarea extrasului din mandatul judecătoresc corespunzător.

### **Articolul 31. Ridicarea operativă**

Ridicarea operativă reprezintă ridicarea secretă, cu ulterioara returnare secretă, a bunurilor, documentelor, suporturilor materiale de informații cu scopul examinării și analizării acestora, al efectuării constatării tehnico-științifice, al colectării informațiilor necesare, precum și pentru prelevarea și examinarea mostrelor.

### **Articolul 32. Accesul la informația financiară sau monitorizarea tranzacțiilor financiare**

(1) Accesul la informația financiară reprezintă obținerea de la bănci, de la alte persoane/organizații care intermediază tranzacțiile financiare sau de la alte instituții competente a înscrisurilor sau informațiilor, aflate în posesia acestora, referitoare la depuneri, la conturi sau la tranzacțiile unei persoane ori la circulația unor anumite mijloace bănești.

(2) Monitorizarea tranzacțiilor financiare reprezintă operațiunile prin care se asigură cunoașterea, inclusiv în regim de timp real, a conținutului tranzacțiilor financiare efectuate prin intermediul băncilor, al altor persoane/organizații care intermediază tranzacțiile financiare sau al altor instituții competente, referitoare la depuneri, la conturi sau la tranzacțiile unei persoane ori la circulația unor anumite mijloace bănești.

(3) Băncilor, altor persoane/organizații care intermediază tranzacțiile financiare și altor instituții competente li se prezintă extrasul din mandatul judecătoresc corespunzător, în care se indică doar tipul de informații care urmează a fi prezentate și, după caz, termenul de efectuare a monitorizării.

### **Articolul 33. Urmărirea vizuală și/sau documentarea cu ajutorul metodelor și mijloacelor tehnice, precum și localizarea sau urmărirea prin sistemul de poziționare globală ori prin alte mijloace tehnice**

(1) Urmărirea vizuală și/sau documentarea cu ajutorul metodelor și mijloacelor tehnice reprezintă observarea, cu fixarea observațiilor, a unor imobile, spații, mijloace de transport, bunuri, a acțiunilor/inacțiunilor persoanei, a altor circumstanțe de fapt care se desfășoară, cu sau fără utilizarea mijloacelor tehnice de înregistrare.

(2) Localizarea sau urmărirea prin sistemul de poziționare globală sau prin alte mijloace tehnice constă în folosirea mijloacelor tehnice pentru determinarea locului unde se află sau s-a aflat persoana sau obiectul, precum și în monitorizarea deplasării sau aflării acestora, cu înregistrarea informației obținute.

### **Capitolul III** **ACTIVITATEA INFORMATIVĂ EXTERNĂ**

#### **Articolul 34. Sarcinile activității informative externe**

Activitatea informativă externă are sarcina de identificare, prevenire și contracarare a factorilor de risc și a amenințărilor externe sau de proveniență externă la adresa securității naționale, a consecințelor în cazul materializării acestora, precum și de protecție și promovare a intereselor strategice ale Republicii Moldova și ale partenerilor săi.

#### **Articolul 35. Măsurile informative externe**

Serviciul și Ministerul Apărării sunt în drept să creeze, să achiziționeze, să dețină și să utilizeze tactici, metode, mijloace și surse specifice pentru planificarea, culegerea, verificarea, evaluarea, prelucrarea analitică, stocarea, păstrarea și valorificarea informațiilor necesare realizării activității informative externe.

#### **Articolul 36. Condițiile și modul de desfășurare a activității informative externe**

(1) Desfășurarea măsurilor informative externe se admite doar în scopul realizării sarcinilor prevăzute de prezenta lege.

(2) Realizarea măsurilor informative externe și aplicarea tacticilor, metodelor și mijloacelor specifice de desfășurare a activității informative externe se efectuează în conformitate cu actele interne ale Serviciului sau, după caz, ale Ministerului Apărării.

### **Capitolul IV** **ASIGURAREA FINANCIARĂ, TEHNICO-MATERIALĂ** **ȘI ȘTIINȚIFICĂ A ACTIVITĂȚII** **INFORMATIVE/CONTRAINFORMATIVE**

#### **Articolul 37. Asigurarea financiară și tehnico-materială a activității informative/contrainformative**

(1) Asigurarea financiară și tehnico-materială a activității informative/contrainformative se efectuează din contul mijloacelor financiare alocate Serviciului sau, după caz, Ministerului Apărării din bugetul de stat, conform legislației.

(2) Proiectele de acte cu privire la asigurarea financiară și tehnico-materială a activității informative/contrainformative se examinează și se aprobă de către autoritățile competente în ședințe închise, constituie secret de stat și nu pot fi făcute publice.

### **Articolul 38. Asigurarea științifică a activității informative/contrainformative**

(1) În cadrul desfășurării activității informative/contrainformative pot fi efectuate constatări tehnico-științifice sau expertize extrajudiciare.

(2) Constatarea tehnico-științifică efectuată în cadrul activității informative/contrainformative reprezintă activitatea desfășurată de un specialist în scopul explicării unor fapte sau circumstanțe, al constatării unor situații, care necesită deținerea unor competențe și cunoștințe speciale.

(3) În cadrul efectuării constatării tehnico-științifice, specialistul nu soluționează chestiuni cu caracter juridic.

(4) Constatările tehnico-științifice se dispun și se efectuează în conformitate cu prevederile prezentei legi.

(5) Expertizele extrajudiciare se dispun și se efectuează în conformitate cu legislația în vigoare.

### **Articolul 39. Temeiurile pentru dispunerea și efectuarea constatării tehnico-științifice**

(1) Constatarea tehnico-științifică se efectuează în temeiul dispoziției scrise a ofițerului de informații sau, după caz, a militarului prin contract, care desfășoară activitate informativă/contrainformativă, aprobată de către conducătorul subunității specializate.

(2) În dispoziția cu privire la efectuarea constatării tehnico-științifice se menționează, în mod obligatoriu, circumstanțele de fapt și chestiunile la care urmează să dea răspuns specialistul și se anexează materialele care urmează a fi cercetate.

**Articolul 40.** Subiecții abilitați cu dreptul de efectuare a constatărilor tehnico-științifice

(1) Constatarea tehnico-științifică este efectuată de către specialiștii din cadrul Serviciului sau, după caz, al Ministerului Apărării.

(2) În cazul în care în cadrul Serviciului sau al Ministerului Apărării nu activează specialiști care să dețină competențe și cunoștințe speciale într-un anumit domeniu de activitate sau dacă complexitatea cauzei impune, efectuarea constatării tehnico-științifice poate fi solicitată specialiștilor din afara Serviciului sau Ministerului Apărării.

(3) Constatarea tehnico-științifică poate fi solicitată specialiștilor din afara Serviciului sau Ministerului Apărării doar cu consimțământul acestora, în baza unui acord sau contract.

**Articolul 41.** Organizarea și efectuarea constatării tehnico-științifice

(1) La recepționarea dispoziției cu privire la efectuarea constatării tehnico-științifice, conducătorul subunității de constatare tehnico-științifică desemnează un specialist care deține competențele și cunoștințele necesare pentru efectuarea acesteia.

(2) Specialistul desemnat conform alin. (1) înregistrează dispoziția respectivă și, în termen de 3 zile, își expune opinia dacă deține competențele și cunoștințele necesare pentru a efectua constatarea.

(3) În caz de necesitate, specialistul poate solicita informații și materiale suplimentare de la ofițerul de informații sau militarul prin contract care a dispus efectuarea constatării.

(4) După examinarea materialelor și întreprinderea acțiunilor care se impun, specialistul întocmește un raport de constatare tehnico-științifică în care își expune opinia asupra chestiunilor prezentate spre examinare, explică faptele, circumstanțele neclare, constată situațiile de fapt.

(5) Raportul de constatare tehnico-științifică conține următoarele informații:

- a) datele de identificare ale specialistului;
- b) datele cu privire la studiile sau calificările deținute de specialist pentru efectuarea cercetărilor, precum și la experiența în domeniu;
- c) datele cu privire la ofițerul de informații sau militarul prin contract care a dispus efectuarea constatării;
- d) chestiunile prezentate spre examinare;

- e) circumstanțele de fapt;
- f) cercetările efectuate, cu descrierea metodelor de cercetare aplicate;
- g) concluziile.

## **Capitolul V**

### **CONTROLUL ACTIVITĂȚII INFORMATIVE/CONTRAINFORMATIVE**

#### **Articolul 42. Controlul parlamentar**

(1) Controlul parlamentar asupra activității informative/contrainformative este efectuat de către subcomisia parlamentară pentru exercitarea controlului parlamentar asupra activității Serviciului (în continuare – *subcomisie parlamentară*), în conformitate cu prevederile Regulamentului Parlamentului, adoptat prin Legea nr. 797/1996, și ale regulamentului de activitate al subcomisiei respective, aprobat prin hotărârea Parlamentului.

(2) Subcomisia parlamentară informează sistematic despre activitatea sa comisia parlamentară pentru securitatea națională, apărare și ordinea publică.

(3) Până la prezentarea în ședința în plen a Parlamentului a raportului anual privind activitatea Serviciului, directorul Serviciului prezintă subcomisiei parlamentare, în ședință închisă, un raport cu privire la activitatea informativă/contrainformativă, care să cuprindă, în mod obligatoriu, informații despre:

- a) numărul total al măsurilor contrainformative dispuse, realizate și respinse, pe fiecare măsură în parte;
- b) numărul dosarelor speciale deschise și al celor clasate;
- c) numărul persoanelor informate despre realizarea în privința acestora a măsurilor contrainformative;
- d) date privind eventualele încălcări admise de ofițerii de informații în executarea prevederilor prezentei legi.

(4) În cadrul ședinței indicate la alin. (3) pot fi prezentate informații despre operațiunile finalizate realizate de către Serviciu dacă dezvăluirea acestora nu va dăuna securității statului. Informații despre operațiunile în derulare nu se prezintă.

(5) După prezentarea informației conform alin. (3), membrii subcomisiei parlamentare pot adresa întrebări cu privire la activitatea informativă/contrainformativă desfășurată de către Serviciu în anul precedent. În baza informației prezentate, subcomisia parlamentară poate formula recomandări privind activitatea informativă/contrainformativă a Serviciului.

(6) După examinarea informației privind activitatea informativă/contrainformativă a Serviciului conform prevederilor prezentului articol, subcomisia parlamentară ia act de informația prezentată și publică pe pagina web oficială a Parlamentului rezultatele controlului activității informative/contrainformative, în care, în mod obligatoriu, sunt specificate numărul măsurilor contrainformative realizate de către Serviciu, pe fiecare măsură în parte, și numărul încheierilor privind respingerea demersului pentru emiterea mandatului judecătoresc, pe fiecare măsură în parte, într-un mod în care să nu fie dezvăluite informațiile atribuite la secret de stat.

(7) În cazul în care subcomisia parlamentară constată că există bănuieli rezonabile privind admiterea încălcărilor grave în activitatea informativă/contrainformativă a Serviciului, aceasta poate solicita efectuarea unei anchete parlamentare sau poate sesiza Procurorul General.

(8) Raportul anual privind activitatea Serviciului conține, în mod obligatoriu, un compartiment cu privire la activitatea informativă/contrainformativă desfășurată de către Serviciu și la măsurile întreprinse de către acesta în urma recomandărilor subcomisiei parlamentare.

#### **Articolul 43. Controlul exercitat de către procuror**

(1) Controlul exercitat de către procuror asupra activității contrainformative se efectuează de către procurorii din cadrul Procuraturii Generale, abilitați în acest sens de către Procurorul General.

(2) Controlul se efectuează fie în baza petițiilor depuse de către persoanele ale căror drepturi și interese legitime se presupune că au fost încălcate, fie, din oficiu, în cazul în care procurorului i-au devenit cunoscute informații despre încălcarea legislației în legătură cu desfășurarea măsurilor contrainformative, dacă faptele respective pot constitui infracțiuni.

(3) În cadrul controlului exercitat de către procuror, informația privind persoanele care au colaborat sau colaborează confidențial cu Serviciul poate fi prezentată doar procurorului din categoria celor menționați la alin. (1), abilitat în acest sens prin ordinul Procurorului General. Informația respectivă se prezintă doar dacă aceasta este în legătură directă cu obiectul controlului efectuat și doar dacă este absolut necesară realizării controlului respectiv.

(4) Înainte de a fi abilitați să exercite controlul asupra activității contrainformative, procurorilor li se perfectează dreptul de acces la secretul de stat, dacă nu dispun de dreptul respectiv.

**Articolul 44. Controlul intern**

(1) Controlul intern asupra activității informative/contrainformative se realizează de către directorul Serviciului, directorul adjunct împuternicit în acest sens și, după caz, de ministrul apărării, inclusiv prin intermediul subunităților interne de control și al conducătorilor subunităților specializate.

(2) Persoanele care nu sunt implicate nemijlocit în lucrul cu persoanele care colaborează confidențial cu Serviciul sau cu Ministerul Apărării, inclusiv directorul și directorii adjuncți ai Serviciului, ministrul apărării, nu sunt în drept să solicite informații despre identitatea reală a persoanelor care colaborează confidențial cu Serviciul sau cu Ministerul Apărării dacă aceasta nu este dictată de o necesitate stringentă de serviciu.

**Articolul 45. Controlul judecătoresc**

Controlul judecătoresc se efectuează prin verificarea temeiniciei realizării măsurilor contrainformative la emiterea mandatului judecătoresc sau în cazul în care se evaluează legalitatea acțiunilor efectuate.

**Articolul 46. Controlul extern asupra cheltuirii mijloacelor financiare**

Controlul extern asupra cheltuirii mijloacelor financiare alocate pentru asigurarea realizării activității informative/contrainformative se efectuează de către Curtea de Conturi, în ședință închisă, în condițiile Legii nr. 245/2008 cu privire la secretul de stat. Controlul respectiv se efectuează în limite care să nu permită dezvăluirea conținutului, formelor, tacticii, metodelor și mijloacelor activității informative/contrainformative, a datelor de identificare ale persoanelor care colaborează confidențial cu Serviciul sau cu Ministerul Apărării, a operațiunilor în derulare și a operațiunilor care au fost finalizate, dar a căror dezvăluire ar putea dăuna securității statului.

**Articolul 47. Controlul asupra prelucrării datelor cu caracter personal în cadrul activității informative/contrainformative**

Prelucrarea și controlul asupra prelucrării datelor cu caracter personal în cadrul activității informative/contrainformative se efectuează în condițiile legislației privind protecția datelor cu caracter personal, ținând cont de particularitățile prevăzute de prezenta lege.

## **Capitolul VI DISPOZIȚII FINALE ȘI TRANZITORII**

### **Articolul 48**

(1) Prezenta lege intră în vigoare după 90 de zile de la data publicării acesteia în Monitorul Oficial al Republicii Moldova, cu excepția prezentului articol care intră în vigoare la data publicării.

(2) În termen de 60 de zile de la data publicării prezentei legi:

a) președintele Curții de Apel Chișinău și cel al Curții Supreme de Justiție vor stabili numărul de judecători care vor fi abilitați cu competența de a emite mandate judecătorești și de a examina recursuri, în sensul prezentei legi, vor desemna judecătorii respectivi și vor organiza procesul de repartizare aleatorie a demersurilor/recursurilor Serviciului;

b) judecătorii desemnați conform prevederilor lit. a) vor iniția procesul de perfectare a dreptului de acces la secretul de stat, dacă nu dispun de acesta;

c) Procurorul General va desemna procurorii abilitați cu dreptul de control asupra activității contrainformative.

(3) Guvernul, în termen de 6 luni de la data publicării prezentei legi, va prezenta Parlamentului propuneri privind aducerea legislației în vigoare în concordanță cu aceasta.

**PREȘEDINTELE PARLAMENTULUI**

**SINTEZA**  
**amendamentelor, obiecțiilor și propunerilor**  
**la proiectul de Lege privind activitatea contrainformativă și activitatea informativă externă**  
**(nr. 422 din 17.11.2022) lectura II.**

Autorul amendamentelor obiecțiilor și propunerilor	Conținutul amendamentelor obiecțiilor și propunerilor	Decizia Comisiei
<p><b>A.O.</b>  <b>„Amnesty International Moldova”</b>                      Nr. 05/23 din                      09.03.2023</p>	<p><b>1. Art. 7 alin. (1)</b> este o duplicare a prevederii din Proiectul de lege cu privire la Serviciul de Informații și Securitate, care conferă Serviciului dreptul de a primi asistență de la persoane juridice. După cum s-a menționat anterior, o astfel de asistență ar trebui acordată Serviciului doar în baza unui mandat judecătoresc.</p> <p>Atunci când analizăm acest articol, este important să ne amintim Principiile Internaționale de Necesitate și Proportionalitate (privind aplicarea drepturilor omului la supravegherea comunicațiilor). Conform principiilor în cauză, „Statele nu ar trebui să oblige furnizorii de servicii sau furnizorii de hardware sau software să construiască în sistemele lor capacități de supraveghere sau monitorizare sau să colecteze sau să rețină anumite informații exclusiv în scopuri de supraveghere de stat. Reținerea sau colectarea <i>a priori</i> a datelor nu ar trebui să fie niciodată solicitată furnizorilor de servicii.” Prin urmare, este important ca prevederile articolului 7 să fie aplicate în contextul anumitor cazuri concrete și să nu fie interpretate într-un mod care să oblige furnizorii să își adapteze tehnologia pentru a oferi Serviciului acces direct și <i>a priori</i> la informațiile utilizatorilor. În același timp, deși furnizorii ar putea fi obligați să păstreze confidențialitatea conținutului măsurilor contrainformative, „Statele nu ar trebui să interfereze cu furnizorii de servicii în eforturile lor de a publica procedurile pe care le aplică atunci când evaluează și se conformează cererilor statului de supraveghere a comunicațiilor, când aderă la astfel de proceduri și publică înregistrările cu privire la cererile de supraveghere a comunicațiilor din partea statului.” În plus, prevederile articolului 7 nu ar trebui interpretate într-un mod care să împiedice furnizorii să informeze utilizatorii despre măsurile contrainformative la care sunt supuși. În caz contrar, această obligație ar fi în contradicție cu Principiul 8 privind Informarea Utilizatorilor, care prevede după cum urmează: „Obligația de a notifica revine statului, dar furnizorii de servicii de comunicații ar trebui să fie liberi să notifice persoanele cu privire la Supravegherea comunicațiilor, din oficiu sau la cerere.” În plus, prevederea de la art. 7 alin. (9) este ambiguă deoarece permite</p>	<p><b>Se acceptă.</b>                      Articolul a fost exclus.</p>

	<p>Serviciului să acceseze bazele de date ale abonaților „prin alte metode stabilite de comun acord” cu furnizorul de rețea, fără a defini care pot fi acele metode. O astfel de prevedere nu este suficient de clară așa cum cere jurisprudența CtEDO,5 poate duce la abuzuri și poate încălca drepturile persoanelor.</p> <p><b>2. Articolul 9 alin. (3)</b> nu oferă suficiente garanții împotriva abuzurilor deoarece această dispoziție dă dreptul Serviciului de a decide subiectiv asupra distrugerii materialelor din dosarele speciale fără autorizarea prealabilă a unui judecător. Dacă materialele din dosarele speciale sunt distruse și persoana împotriva căreia Serviciul a întreprins măsuri nu a știut despre acestea, există riscul ca încălcări ale drepturilor omului să nu fie niciodată descoperite. În același timp, nu este suficient de clar care ar fi „oricare alt temei legal” care ar permite distrugerea sau păstrarea informațiilor, ce ar influența luarea unei decizii în defavoarea alteia (de păstrare în loc de distrugere, sau invers), și cine vor fi acele persoane care vor avea acces la informație dacă aceasta este păstrată.</p>	<p><b>Se acceptă parțial.</b> Norma a fost revizuită, excluzând posibilitatea distrugerii materialelor.</p>
<p><b>3. Articolul 12 alin. (1) lit. a)</b> stabilește că SIS poate avea acces la informația financiară sau monitorizarea tranzacțiilor financiare doar cu autorizarea Directorului SIS/ directorului adjunct. Dreptul directorului Serviciului/ al directorilor adjuncți de a autoriza măsuri contrainformative trebuie exclus, iar măsurile trebuie autorizate prin mandat judecătoresc. Acest argument este justificat de ingerința pe care măsurile contrainformative o au asupra drepturilor persoanelor, indiferent de nivelul pretins de intruziune pe care le-ar avea. Mai mult, alin. (1) lit. a) din prezentul articol care prevede că Serviciul „poate avea acces la informații financiare sau monitoriza tranzacțiile financiare” doar cu autorizarea directorului/directorului adjunct al Serviciului trezește îngrijorări. Anterior, în acest sens, Comisia de la Veneția și-a exprimat îngrijorarea cu privire la un proiect de lege precedent „care permitea Serviciului accesul la toate tranzacțiile financiare și informațiile financiare, în afara unei urmăriri penale, fără un mandat judecătoresc și, prin urmare, în absența oricărui control extern.”6 Comisia de la Veneția a menționat, de asemenea, că astfel de măsuri ar putea crea un potențial de supraveghere în masă. Această prevedere trebuie revizuită ținând</p>	<p><b>Se acceptă.</b> Norma a fost revizuită conceptual, măsura dată va fi autorizată de judecător.</p>	

4. **Articolul 5** alin. (5), întrucât include „întreprinderile, instituțiile și organizațiile, indiferent de tipul lor de proprietate” în calitate de subiecți ai căror sisteme informaționale pot fi accesate de către Serviciu, și în vederea securizării drepturilor lor la viață privată în conformitate cu prevederile art. 8 CEDO, art. 5 alin. (4) trebuie să fie completat prin introducerea necesității ca acest acces să fie în mod obligatoriu autorizat de către judecător.

**5. Articolul 15:**

*Art. 15 alin. (6)* conferă Serviciului dreptul de a decide dacă prezintă sau nu materiale judecătorului în procesul de solicitare a unei autorizații. În consecință, judecătorul eliberează o autorizație exclusiv pe baza argumentelor prezentate de ofițer, fără nici o documentație care să dovedească necesitatea autorizării unei măsuri. Mai mult de atât, acest alineat nu obligă Serviciul să atașeze acele materiale la demers, chiar dacă acestea sunt prezentate. În astfel de cazuri există o mare posibilitate de abuzuri. De exemplu, CtEDO a susținut în jurisprudența sa că „având în vedere riscul ca un sistem de supraveghere secretă pentru protecția securității naționale să submineze sau chiar să distrugă democrația sub învelișul apărării acesteia, Curtea trebuie să fie convinsă că există garanții eficiente împotriva abuzului.” Prin urmare, prezentul alineat ar trebui modificat pentru a obliga Serviciul să furnizeze materiale în timpul solicitării unui mandat judecătoresc și să atașeze respectivele documente la demersul prezentat judecătorului.

Datorită formulării sale ambigue, nu este clar din prevederea *alin. (11)* care sunt „*excepțiile*” care ar permite Serviciului să întreprindă măsuri contrainformative fără mandat judecătoresc. Comisia de la Veneția a recomandat autorităților moldovenești „să precizeze circumstanțele pentru autorizarea de urgență”<sup>8</sup> atunci când ar putea fi dispuse măsuri speciale de investigație fără un mandat de securitate. Prin urmare, legiuitorul ar trebui să definească suficient de clar situațiile excepționale.

*Art. 15 alin. (12)* poate fi interpretat într-un mod în care Serviciului i se permite să efectueze măsuri chiar înainte ca judecătorul să emită decizia de autorizare care conține toate cerințele ce trebuie respectate de către Serviciu (motivele care au stat la baza autorizării măsurii, tipul măsurii, termenul și locul efectuării acesteia etc.). În schimb, Serviciul ar trebui să înceapă să pună în aplicare măsura numai după ce judecătorul a emis o autorizație corespunzătoare cu cerințe și limitări clare care trebuie respectate.

**Se acceptă parțial.**  
Norma a fost exclusă.

**Se acceptă.**

Norma a fost modificată.

A se vedea textul „*Pe parcursul examinării demersului, judecătorului, la solicitarea acestuia sau din inițiativa Serviciului, se prezintă materialele ce confirmă necesitatea efectuării acestor măsuri*”

**Nu se acceptă.** Norma prevede textul „*existența unui risc esențial de întârziere care poate duce la pierderea informațiilor relevante sau pune în pericol imediat securitatea statului sau a persoanelor*”.

**Nu se acceptă.** Propunerea reiese dintr-o interpretare eronată a normei în cauză. Norma se referă strict la cazurile de efectuare a măsurilor contrainformative în condiții speciale, ca excepție fără mandat judecătoresc, dar cu autorizarea ulterioară obligatorie.

În conformitate cu *art. 15 alin. (13)* judecătorul nu este obligat să elibereze un mandat judecătoresc după declararea măsurii ca fiind legală, acesta fiind solicitat în mod subiectiv de către Serviciu. Acest alineat trebuie modificat pentru a exclude interpretările prin care Serviciului i se permite să continue măsurile pe baza faptului că judecătorul a declarat măsura efectuată în acele circumstanțe excepționale ca fiind legală. Dacă Serviciul dorește să continue măsura după expirarea acestor 24 de ore și după ce judecătorul a declarat măsurile ca fiind legale, Serviciul ar trebui să fie obligat să solicite o autorizație suplimentară. În absența unei autorizații, Serviciul nu va fi constrâns să respecte cerințele incluse într-o autorizație, cum ar fi termenul de realizare a măsurii.

*Art. 15 alin. (14)* trebuie modificat astfel încât să includă obligația Serviciului de a informa persoana fizică sau juridică în privința măsurii căreia a fost supusă și ulterior declarată ilegală de către judecător. Totodată, înainte ca materialul adunat în timpul măsurii contrainformative să fie distrus, acesta ar trebui prezentat persoanelor, astfel încât acestea să aibă o înțelegere clară despre informațiilor colectate de către Serviciu. Această modificare este necesară și pentru a permite persoanei să conteste acțiunile Serviciului în fața autorităților competente.

6. Prevederea de la **art. 16 alin. (3)** este discriminatorie deoarece spre deosebire de orice altă persoană care poate fi supusă măsurilor contrainformative în cazul în care faptele lor constituie infracțiune și/sau reprezintă o amenințare la adresa securității naționale, persoanele care contribuie la activitatea contrainformativă precum și rudele lor pot fi supuse unor măsuri contrainformative numai cu acordul lor scris. Prin urmare, există riscul ca aceste persoane să nu fie împiedicate să acționeze în detrimentul securității naționale și să nu fie trase la răspundere pentru acțiunile lor, deoarece este puțin probabil ca acestea să își dea acordul de a fi supuse măsurilor contrainformative.

**Se acceptă.** Alineatul (12) și (13) au fost modificate în scopul excluderii unei interpretări abuzive.

**Nu se acceptă.** Reglementările privind informarea persoanei se regăsesc la art. 23. Totodată, au fost excluse prevederile ce stabilesc posibilitatea distrugerii materialelor culese.

**Nu se acceptă.** În cazul dat este o situație specială în care pot fi efectuate măsurile contrainformative și anume pentru a proteja persoanele care contribuie la desfășurarea activității informative/contrainformative și numai dacă există pericol iminent pentru viața, sănătatea sau alte drepturi fundamentale ale acestora, ori dacă este necesară pentru prevenirea infracțiunii sau a unor consecințe nefavorabile ce vizează persoanele menționate. Norma respectivă nu instituie imunitate de investigație.

Sunt măsuri contrainformative efectuate în scop de protecție și nu de colectare a informațiilor. Reglementări similare sunt și în activitatea specială de investigații. În cazul în care aceste categorii de persoane vor săvârși fapte ce prezintă pericol

<p>păentru securitate statului, ele vor fi investigate în condiții generale.</p> <p><b>Se acceptă.</b></p> <p><b>Nu se acceptă.</b> Interpretarea semantică a textului nu generează neclaritățile invocate în obiecție.</p>	<p>7. <b>Articolul 17 alin. (5)</b> prevede durata totală a "măsurilor speciale de investigație", în timp ce acest proiect de lege reglementează activitatea contrainformativă și informativă externă. Astfel, există riscul ca în lipsa unei prevederi clare privind durata măsurilor contrainformative, acestea să fie conduse în mod abuziv, pe o perioadă nedeterminată, și să încalce drepturile persoanelor. Formularea „măsuri speciale de investigație” trebuie înlocuită cu „măsuri contrainformative”.</p> <p>Dispoziția de la alin. (6) poate conduce la interpretări subiective și abuzive, prin care măsurile contrainformative vor fi începute la data expirării termenului pentru care măsura a fost autorizată și vor fi continuate după expirarea mandatului. În această privință, este necesar să reiterăm cauza Iordachi și alții c. Moldova, în care CtEDO a criticat autoritățile naționale pentru faptul că legislația națională „nu prevede o limitare clară în timp a unei măsuri de autorizare a interceptării comunicațiilor telefonice”.</p> <p><b>8. Articolul 23:</b> Alin. (1) al prezentului articol stabilește că Serviciul are obligația de a informa persoanele despre măsurile contrainformative care au fost întreprinse în privința lor, dar numai despre cele care au fost autorizate prin mandat judecătoresc. Prin urmare, persoana nu poate cunoaște despre măsurile care au fost efectuate cu autorizarea directorului/directorului adjunct al Serviciului. Reiterând comentariile referitoare la art. 12, în lipsa unui control extern și în lipsa unei informări a persoanelor, există riscul nedescoperirii încălcării drepturilor persoanelor vizate. Acest risc a fost confirmat și de Comisia de la Veneția, care a stabilit că retragerea dreptului de a fi informat despre astfel de măsuri contribuie la faptul că „o eventuală încălcare a drepturilor persoanei în cauză nu va fi niciodată descoperită”.<sup>10</sup> De asemenea, CtEDO a considerat o astfel de abordare ca fiind inacceptabilă și care încalcă articolul 8 din CEDO.<sup>11</sup> Astfel, reinvocăm necesitatea autorizării prin mandat judecătoresc a tuturor măsurilor contrainformative și, efectiv, obligația Serviciului de a informa persoanele despre efectuarea tuturor măsurilor cărora au fost supuse.</p> <p>Având în vedere alin. (5) al prezentului articol, se impune reiterarea cerințelor Comisiei de la Veneția privind necesitatea controlului periodic asupra condițiilor de neinformare a persoanelor cu privire la măsurile înfăptuite. Comisia a menționat că „Jurisprudența CtEDO permite amânarea informării”,<sup>12</sup> în timp ce prevederile acestui articol includ posibilitatea</p>
<p><b>Se acceptă parțial.</b> A fost revăzut substanțial mecanismul de autorizare a măsurilor contrainformative (inclusiv rolul directorului/adjunct al SIS în autorizare). Totodată, proiectul a fost completat cu norme suplimentare ce țin de controlul legalității măsurilor după finalizarea acestora. Considerăm că nu există temeiuri pentru a admite riscul abuzurilor factorilor de decizie sau a subiecților de aplicare a legii.</p> <p><b>Se acceptă parțial.</b> În dependență de caracterul permanent sau provizoriu al temeiurilor de neinformare, judecătorul, poate autoriza neinformarea permanentă sau neinformarea pentru o anumită</p>	<p><b>Se acceptă parțial.</b> A fost revăzut substanțial mecanismul de autorizare a măsurilor contrainformative (inclusiv rolul directorului/adjunct al SIS în autorizare). Totodată, proiectul a fost completat cu norme suplimentare ce țin de controlul legalității măsurilor după finalizarea acestora. Considerăm că nu există temeiuri pentru a admite riscul abuzurilor factorilor de decizie sau a subiecților de aplicare a legii.</p> <p><b>Se acceptă parțial.</b> În dependență de caracterul permanent sau provizoriu al temeiurilor de neinformare, judecătorul, poate autoriza neinformarea permanentă sau neinformarea pentru o anumită</p>

<p>neinformării permanente.</p> <p>Sintagma „ofiter de investigații” de la alin. (6) contravine prevederilor art. 4 din același proiect de lege care stabilește că singura autoritate care are dreptul de a desfășura activitate contrainformativă sau informativă externă este Serviciul prin „ofiterii de informații și securitate”, iar alte persoane decât aceștia nu au dreptul să desfășoare o astfel de activitate. Ca urmare, alin. (6) anulează obligația Serviciului de a informa persoanele cu privire la măsurile la care au fost supuse în cazul în care au dispărut condițiile de neinformativitate. Prin acest abuz, oamenii riscă să nu afle despre încălcările drepturilor lor și să nu poată contesta acțiunile Serviciului. Astfel, sintagma ”ofiter de investigații” trebuie înlocuită cu sintagma ”ofiter de informații și securitate/ ofiter de informații.”</p>	<p>perioadă de timp determinată, dar nu mai mare de 1 an, Serviciul fiind obligat la expirarea perioadei respective să reevalueze temeiurile de neinformativitate și să întreprindă acțiunile necesare, în conformitate cu prevederile prezentului articol, inclusiv, după caz, să solicite neinformativitate pentru o nouă perioadă de timp.</p> <p><b>Se acceptă.</b></p>
<p><b>9. Art. 36 alin. (4)</b> conferă Serviciului dreptul extensiv de a pătrunde în locuința unei persoane. Sau, altfel spus, instalarea echipamentului de supraveghere este o măsură intruzivă în viața privată a persoanei, efectuată numai după ce un judecător o autorizează. Atunci nu este clar de ce pentru demontarea unui astfel de echipament, care la fel presupune pătrunderea în domiciliul persoanei și intruziune în viața sa privată, nu judecătorul autorizează această măsură, ci Directorul/directorul adjunct al Serviciului. Pentru a exclude abuzurile și pentru a proteja dreptul la viața privată al persoanelor, o astfel de acțiune ar trebui efectuată pe baza unui mandat judecătoresc. Prin urmare, propunem ca măsura de demontare a echipamentului de supraveghere să fie inclusă în mandatul judecătoresc care autorizează instalarea acestuia, totodată în acest mandat fiind indicat și un termen limită pentru demontarea echipamentului de supraveghere.</p>	<p><b>Se acceptă parțial.</b></p> <p>În cazul dat nu este vorba de o imixtiune în viața privată, în care s-ar acumula informații despre persoană și fapte. Este o măsură strict tehnică.</p> <p>Atragem atenția asupra textului „În cazul dat domiciliul nu se cercetează și nu se întreprind alte acțiuni, decât cele de demontare a aparatului. Despre faptul pătrunderii în domiciliu și demontării aparatului se întocmește un proces-verbal, în care se indică data și persoanele care au pătruns în domiciliu. Totodată, norma a fost completată în final cu textul:</p> <p><i>Procesul verbal se remite pentru informare judecătorului care a autorizat măsura.</i></p>

<p>Demontarea aparatajului are loc în termeni restrânși reieșind din circumstanțele de fapt și specificul misiunii de instalare/demontare a tehnicii special. Fixarea unui termen fix (1 zi-2 zile) este irațional și imposibil deseori de realizat.</p>	<p><b>Se acceptă parțial.</b>  Articolul a fost completat cu prevederi suplimentare ce vizează procedura de control. De asemenea, în proiect a fost introdus un nou articol privind controlul legalității efectuării măsurilor contrainformative de către judecător, <i>post factum</i>.  Totodată, în cadrul grupului de lucru de pe lângă Comisia parlamentară securitate națională, apărare și ordin publică s-a revăzut proiectul prin prisma eficacității mecanismelor de control și supraveghere a activității contrainformative.</p>	<p>Formulara „cât mai scurt timp” de la art. 36 alin. (5) este foarte ambiguă. În schimb, Serviciul ar trebui să aibă un interval de timp clar în care echipamentele utilizate pentru supraveghere să fie demontate, după cum a fost sugerat supra, care să fie indicat în mandatul judecătoresc de autorizare a măsurii de instalare a echipamentelor de supraveghere.</p>	<p><b>10. Articolul 57. Controlul parlamentar</b>  Controlul parlamentar reprezintă un mecanism ineficient de control al activității Serviciului. Acesta se efectuează o dată în an de către Comisia Securitate Națională, prin intermediul Subcomisiei pentru exercitarea controlului parlamentar, în baza raportului Directorului SIS, doar pe cauzele care au fost soluționate. Informații despre operațiunile în derulare nu se prezintă. În baza raportului, Subcomisia poate înainta recomandări. Totodată, Comisia de la Veneția a specificat că în cazul în care politicienii nu au legitimitate în fața societății, atunci acest mecanism poate fi insuficient pentru a da garanțiile necesare societății.<sup>13</sup> Totodată, efectiv, orice organism parlamentar cu funcție de supraveghere nu va exercita o ”supraveghere independentă” ci mai degrabă un control asupra Serviciului. O alternativă constă în crearea unui organ de experți pe securitate independenti, posibil cu reprezentare politică, și/ sau membri ai societății civile. Însă, chiar și în cazul creării unui astfel de mecanism, este puțin probabil să poată compensa pericolele cauzate drepturilor omului dacă pragul condițiilor necesare pentru autorizare a măsurilor este foarte scăzut.</p>
			<p><b>11. Articolul 58. Controlul exercitat de către procuror</b>  Se efectuează în baza plângerilor depuse de către persoane ale căror drepturi și interese legitime se presupune că au fost încălcate sau din oficiu, în cazul în care procurorul i-au devenit cunoscute informații despre încălcarea legislației la efectuarea măsurilor contrainformative, dacă aceste fapte pot constitui infracțiuni (alin. 2). Ținând cont de faptul că persoanele sunt notificate despre măsurile contrainformative întreprinse doar după clasarea dosarului sau pot să nu fie notificate în general, atunci există riscul ca violarea drepturilor persoanelor să nu fie depistată. Prin urmare, reiterăm necesitatea revizuirii condițiilor de informare a persoanelor cu privire la măsurile contrainformative cărora au fost supuse.</p>
			<p><b>12. Articolul 60. Controlul exercitat de către magistrați</b>  Se realizează prin verificarea temeiniciei înfăptuirii măsurilor contrainformative la eliberarea mandatului judecătoresc sau atunci când se apreciază legalitatea acțiunilor efectuate în absența mandatului judecătoresc.</p>

<p>Prin urmare, acest tip de control se realizează doar o singură dată. Ar fi benefic ca să se realizeze un control periodic dacă măsura contrainformativă este adecvată sau nu și legalitatea acesteia, în dependență de evoluția circumstanțelor. În această privință, Comisia de la Veneția a menționat că în cazul în care autorizarea măsurilor se efectuează fără careva cerințe stricte, atunci controlul ulterior trebuie să fie unul riguros.</p>	<p>judecător, <i>post factum</i>. Totodată, în cadrul grupului de lucru de pe lângă Comisia parlamentară securitate națională, apărare și ordin public s-a revăzut proiectul prin prisma eficacității mecanismelor de control și supraveghere a activității contrainformative.</p>
<p>1. Articolul 6 prevede, că persoanele care colaborează confidențial cu Serviciul (în continuare SIS) sânt persoane fizice care, printr-un acord scris sau verbal, și-au dat consimțământul să ofere confidențial informații Serviciului, să participe confidențial la pregătirea și efectuarea activității informative/contrainformative, fapt ce contravine articolului 4, care prevede că, alte autorități sau persoane decât cele prevăzute în prezentul articol nu au dreptul să efectueze activitatea informativă/contra-informativă.</p> <p>2. La articolul 10 și 11, nu sunt prevăzute clauze privind controlul legalității măsurilor întreprinse, înainte de nimicire materialelor, precum și informarea persoanelor a căror drepturi au fost lezate, fiind supuse măsurilor de informative/contra-informative.</p>	<p><b>Se acceptă parțial.</b> Articolul 6 a fost exclus.</p>
<p><b>Uniunea Avocaților din Republica Moldova (nr. UA/45/2023 din 17.01.2023)</b></p>	<p><b>Nu se acceptă.</b> Controlul legalității și informarea persoanelor se realizează înainte de procedura de de nimicire a materialelor sau clasare a dosarului special. A se vedea articolul ce ține de controlul legalității efectuării măsurilor contrainformative de către judecător și articolul privind informarea persoanei despre măsurile contrainformative înlăptuite în privința sa.</p>

3. La articolul 12 alineatul (1) se propune abuziv sub paravanul unei intenții nobile și re-denumirea activității din activitatea specială de investigații în - activitate informativă/contra-informativă, de a acorda Directorului SIS drepturi de autorizare a măsurilor speciale de investigații-informative/contrainformative, care conform Codului de Procedură Penală și Legii nr. 59/2012 privind activitatea specială de investigații sunt autorizate de către instanța de judecată sau Procuror.

Astfel, articolul 12 alineatul 1) litera a) accesul la informația financiară sau monitorizarea tranzacțiilor financiare, este identic prevederilor Legii nr. 59/2012 privind activitatea specială de investigații, al cărei subiect este și SIS (art.18 alin. 1 litera f) - monitorizarea sau controlul tranzacțiilor financiare și accesul la informația financiară;), doar că, în Legea nr. 59 privind activitatea specială de investigații, aceste măsuri se efectuează cu autorizarea instanței de judecată.

Articolul 12 alineatul 1) litera b) - *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*; este identic prevederilor Legii nr. 59/2012 privind activitatea specială de investigații, al cărei subiect este și SIS (art. 18 alineatul 2 litera a) - identificarea abonatului, proprietarului sau a utilizatorului unui sistem de comunicații electronice ori al unui punct de acces la un sistem informatic;), doar că în Legea nr. 59 privind activitatea specială de investigații, aceste măsuri se efectuează cu autorizarea procurorului.

Articolul 12 alineatul 1) litera c) - *urmărirea vizuală și/sau documentarea sau ajutorul metodelor și mijloacelor tehnice, precum și localizarea sau urmărirea prin sistemul de poziționare globală ori prin alte mijloace tehnice*, este identic prevederilor Legii nr. 59/2012 privind activitatea specială de investigații, al cărei subiect este și SIS (art.18 alineatul 2 litera b) - urmărirea vizuală), doar că în Legea nr. 59 aceste măsuri se efectuează cu autorizarea procurorului.

Concomitent, art. 12 alin. (1) p. 1) lit. c) din proiectul Legii privind activitatea contrainformativă și activitatea informativă externă, permite urmărirea vizuală și/sau documentarea cu ajutorul metodelor și mijloacelor tehnice, precum și localizarea sau urmărirea prin sistemul de poziționare globală ori prin alte mijloace tehnice, doar cu autorizarea directorului Serviciului sau directorului adjunct special împuternicit.

Totodată, norma juridică dată prezintă inadvertențe, în condițiile în care potrivit art. 12 alin. (1) p. 2) lit. g) din aceeași lege, este stabilit că urmărirea vizuală cu înregistrarea audio a conținutului comunicărilor transmise de către

**Se acceptă.**  
Articolul 12 a fost revizuit substanțial.

	<p>persoane în spații deschise, locuri publice sau încăperi ce nu constituie domiciliu, se efectuează cu mandat judecătoresc.</p> <p>În acest sens, nu este clar care este diferența dintre aceste activități, or, altfel, potrivit art. 12 alin. (1) p. 1) lit. c) din Legea privind activitatea contrainformativă și activitatea informativă externă, este permisă orice urmărirea vizuală și/sau documentarea cu ajutorul metodelor și mijloacelor tehnice, a oricărei persoane, fără mandat judecătoresc.</p> <p>Articolul 12 aliniatul 1) litera d) - <i>controlul transmiterii banilor sau altor valori materiale, precum și prestării serviciilor</i>, este identic prevederilor Legii nr. 59/2012 privind activitatea specială de investigații, al cărei subiect este și SIS (art. 18 alin. (2) lit. c) controlul transmiterii banilor sau a altor valori materiale extorcate), doar că în Legea nr. 59 privind activitatea specială de investigații, aceste măsuri se efectuează cu autorizarea procurorului.</p> <p>Astfel, remarcăm că, articolul 12 aliniatul (1) subalin. 1) și 2) sunt identice prevederilor Legii nr. 59/2012 privind activitatea specială de investigații, al cărei subiect este și SIS, conform art. 18. Scopurile ambelor legi sunt similare, doar că Legea nr. 59 privind activitatea specială de investigații, prevede un sistem de control și garanții împotriva abuzurilor mai eficient, comparativ cu proiectul dat.</p> <p>În același timp, art. 12 alin. (1) subalin. 2), care prevede efectuarea măsurilor contrainformative cu mandat judecătoresc, impune modificarea Codului de procedură penală prin reglementarea competențelor corespunzătoare ale judecătorilor sau altor autorități în vederea eliberării mandatului judecătoresc prevăzut prin acest proiect.</p>	<p><b>Nu se acceptă.</b></p> <p>Activitatea informativă externă și activitatea contrainformativă reprezintă un mecanism distinct de activitatea specială de investigații și nu se încadrează în reglementările Codului de Procedură Penală și Legii 59/2012 privind activitatea specială de investigație.</p>
<p>4. La articolul 17 termenii stabiliți de efectuare a măsurilor informative/contrainformative contravin termenilor stabiliți de prevederile Codului de Procedură Penală și Legii 59/2012 privind activitatea specială de investigație.</p>		

<p><b>Nu se acceptă.</b> A se vedea art. 11. <b>„...modul de înregistrare a dosarelor speciale, categoria acestora, pornirea, gestionarea, încetarea, termenele de păstrare și procedura de nimicire a acestora, precum și utilizarea resurselor financiare alocate pentru efectuarea măsurilor contrainformative sau informative externe, modalitatea de conlucrare cu persoanele care colaborează confidențial cu Serviciul, inclusiv modul de documentare a informațiilor prezentate de către aceștia, categoriile acestor persoane, organizarea, forțele, mijloacele, sursele, metodele, planurile, procedura și tactica efectuării activității informative/contrainformative, precum și valorificarea rezultatelor acestora constituie informații atribuite la secretul de stat și sînt reglementate prin acte normative departamentale ale Serviciului”.</b></p> <p>Totodată, activitatea informativă externă și activitatea contrainformativă reprezintă un mecanism distinct de activitatea specială de investigații și nu se încadrează în reglementările Codului de Procedură Penală și Legii 59/2012 privind activitatea specială de investigație.</p> <p><b>Se acceptă.</b> Art. 28 a fost exclus din redacția proiectului.</p>	<p>5. La articolul 23 se prevede că, după finalizarea cercetării cauzei și clasării dosarului special, dacă în cadrul acestuia au fost înfăptuite măsuri contrainformative prevăzute la art. 12 alin. (1) pct. 2) (<i>doar măsurile autorizate de instanța de judecată</i>) Serviciul, în termen de 5 zile lucrătoare de la data clasării, va informa persoanele în privința cărora aceste măsuri au fost înfăptuite. Atragem atenția că în proiectul de lege nu se prevede temeiul de clasare și termenul în care urmează a fi clasat dosarul special, fapt ce demonstrează că SIS nu a luat în calcul să informeze persoanele supuse măsurilor informative/contra-informative autorizate de Directorul SIS, ceea ce contravine prevederilor imperative ale Codului de Procedură Penală și Legii nr. 59/2012 privind activitatea specială de investigație.</p>
<p>6. La rândul său, art. 28 din proiect, stabilește procedura investigației sub acoperire, care poate fi dispusă cu autorizarea directorului Serviciului sau directorului adjunct special imputernicit, însă nu prevede interdicția investigatorului sub acoperire să provoace comiterea de infracțiuni.</p>	<p>6. La rândul său, art. 28 din proiect, stabilește procedura investigației sub acoperire, care poate fi dispusă cu autorizarea directorului Serviciului sau directorului adjunct special imputernicit, însă nu prevede interdicția investigatorului sub acoperire să provoace comiterea de infracțiuni.</p>

	<p>7. În același timp, proiectul de Lege privind activitatea contrainformativă și activitatea informativă externă, nu prevede exceptarea de la efectuarea măsurilor contrainformative <i>împotriva avocaților în exercitarea profesiei și implicit, nu stabilește interdicția de a efectua măsuri contrainformative cu privire la raporturile legale de asistență juridică dintre avocat și clientul său.</i> La fel, proiectul nu prevede interdicția de a cerceta biroul sau domiciliul avocatului în exercitarea profesiei și/sau, după caz, instalarea în ele a aparatelor ce asigură supravegherea audio, video, de fotografiat, de constatare a unor stări de fapt, cu sau fără efectuarea înregistrărilor, precum și interdicția de a stenografa comunicările dintre avocat și persoana pe care o apără.</p> <p>Acest fapt pune în pericol grav garantarea independenței exercitării profesiei de avocat, consfințită la art. 52 și 53 din Legea nr. 1260/2002 cu privire la avocatură și la art. 26 alin. (4) din Constituția Republicii Moldova.</p>	<p><b>Se acceptă.</b></p> <p>Proiectul a fost completat cu prevederi ce interzic realizarea oricărei măsuri contrainformative cu privire la raporturile legale de asistență juridică dintre avocat și clientul său.</p>
<p><b>Asociația Bussinesului European (EBA)</b> (nr. 01/23-EC din 25 ianuarie 2023)</p>	<p>1. Art. 1, va fi dispersat și completat în 3 articole, cu renumerotarea succesivă a normelor din proiect, după cum urmează:</p> <p><b>„Articolul 1. Scopul și obiectul de reglementare</b>(1) Prezenta lege are scopul de a stabili cadrul juridic al Serviciului de Informații și Securitate al Republicii Moldova (în continuare – Serviciul), necesară în vederea asigurării securității Republicii Moldova.</p> <p>(2) Prezenta lege reglementează măsurile contrainformative și măsurile informative externe, modalitatea și condițiile de dispunere și efectuare a acestora, limitările admise pentru drepturile și libertățile persoanelor dar și modalitatea de repunere în drepturile restrânse, precum și măsurile de efectuare a controlului asupra legalității acestora.</p> <p><b>Articolul 2. Domeniul de aplicare</b></p> <p>(1) Prezenta lege se aplică:</p> <ol style="list-style-type: none"> <li>1) Serviciului de informații și securitate;</li> <li>2) Ministerelor și altor autorități administrative centrale;</li> <li>3) Instituțiilor publice;</li> <li>4) Autoritățile administrative autonome;</li> <li>5) Întreprinderilor de stat;</li> <li>6) Autoritățile administrației publice locale;</li> <li>7) Organizațiilor necomerciale;</li> <li>8) Altor instituții și organizații de drept privat, în raport cu care sunt opozabile prevederile legii.</li> </ol> <p>(2) Prezenta lege nu se aplică:</p> <ol style="list-style-type: none"> <li>1) Relațiilor dintre avocat și client în cadrul unei acțiuni concrete;</li> <li>2) Relațiilor dintre medic și pacient privind intervențiile medicale;</li> </ol>	<p><b>Nu se acceptă.</b></p> <p>Redacția finală a articolului 1 a fost abordată și definitivată în cadrul grupului de lucru de pe lângă Comisia parlamentară securitate națională, apărare și ordine publică.</p>

3) Adoptator și copil adoptabil în cadrul acțiunii de adopție;

4) La înfăptuirea justiției;

5) Altor situații prevăzute de lege.

### **Articolul 3. Noțiuni utilizate**

*Activitatea contrainformativă* - ansamblul măsurilor, acțiunilor, operațiunilor și procedeele relevante și proporționale desfășurate de către Serviciu în scopul protejării procesului de decizie politico-statal, protejării instituțiilor statului și a societății față de riscurile și amenințările la adresa securității Republicii Moldova, identificării intențiilor, planurilor și obiectivelor activității subversive, spionajului sau a crimei organizate ce periclitează securitatea statului, prevenirea, contracararea sau neutralizarea materializării acestora, studierea organizării, metodelor, capacităților și caracteristicilor părții adverse, urmate de acțiuni de depistare, prevenire și contracarare.

*Activitatea informativă externă* - ansamblul măsurilor, acțiunilor și operațiunilor relevante și proporționale desfășurate de către Serviciu, pentru planificarea, culegerea, verificarea, prelucrarea analitică și valorificarea datelor și informațiilor despre posibilitățile reale sau potențiale, acțiunile, planurile sau intențiile statelor sau organizațiilor străine, ale unor entități neconstituționale sau ale unor persoane, care constituie riscuri sau amenințări la adresa securității Republicii Moldova”.

Expunerea în redacția propusă a celor 3 articole a urmărit executarea în tocmai a imperativului statuat la art. 45 alin. (1) lit. a) din Legea nr. 100/2017 cu privire la actele normative, care stabilește expres că în dispozițiile generale urmează a fi stabilit distinct: obiectul, scopul și domeniul de aplicare a legii și explică termenii și noțiunile. A se menționa că redacția inițială a proiectului nu conținea: scopul, domeniul de aplicare dar și nu delimita conform normelor tehnicii legislative noțiunile definite.

Mai mult, proiectul nu cuprindea expres subiecții la care se aplică/referă această lege dar și subiecții la care nu se referă, fapt indicat la art. 3 din proiect.

Totodată mijloacele și procedeele listate la noțiunile de activitate informativă și contrainformativă, au fost completat și condiționate cu cuvântul „relevante și proporționale” pentru a exclude înțelesul greșit că aceste măsuri pot fi realizate în lipsă de necesitate, relevanță sau disproporționat.

A se menționa că din definiția activitatea informativă externă necesită a fi exclus textul:

- „ sau ar putea constitui” – sintagma dată generează situații iluzorii care ar putea fi determinate doar de o presupunere fără circumstanțe obiective sau probe/material probatoriu sau substrat factologic demonstrat de a crede că o

<p>anumită persoană ar putea genera riscuri reale. Aceste prevederi creează spațiu nelimitat de abuz în privința persoanelor în raport cu care ar putea să se creadă asupra potențialelor riscuri care pot fi aduse securității Republicii Moldova, însă în raport cu care să nu existe nici un fel de dovezi rezonabile.</p> <p>- „ precum și pentru obținerea informațiilor relevante pentru asigurarea securității de stat sau pentru crearea condițiilor favorabile asigurării și promovării intereselor strategice și realizării cu succes a politicii de securitate națională a Republicii Moldova.” – a fost exclus din noțiunea activitatea informativă externă deoarece prevederile în cauză sunt nedeterminate, imprecise și neclare, cea ce în sensul art. 54 alin. (1) lit. a), b), f), h), i) din Legea nr. 100/2017 cu privire la actele normative, determină fie excluderea acestor norme fie definirea clară a acestora. În același context a se menționa că textul reclamat creează denaturat concluzia că activitatea informativă în prima parte de definiție include orice acțiuni chiar dacă ele nu sunt relevante, iar în a doua parte, presupune administrarea informațiilor relevante însă pentru anumite circumstanțe nedeterminate însă care ar fi favorabile promovării intereselor strategice. Așadar, norma vizată conține un amalgam de verbe și adjective care generează un înțeles confuz.</p> <p>În aceeași ordine de idei, în scopul respectării regulilor tehnicii de tehnică legislativă prevăzute la art. 54 alin. (1) din Legea nr. 100/2017 cu privire la actele normative, se necesită a fi definite următoarele noțiuni a cărui înțeles este neclar:</p> <p>a) <i>Activitate subversivă;</i>  b) <i>Spionaj;</i>  c) <i>Valorificarea datelor;</i>  d) <i>Prelucrarea analitică;</i></p>	<p><b>Nu se acceptă.</b></p> <p>Este inoportună definirea expresă a principiilor general cunoscute.</p> <p>Totodată redacția finala a art. 2 a fost abordată și definitivă în cadrul grupului de lucru de pe lângă Comisia parlamentară de securitate națională, apărare și ordine publică.</p>
<p>2. Art. 2 va avea următorul cuprins:</p> <p>„Activitatea informativă/contrainformativă este realizată în corespundere cu următoarele principii:</p> <p>a) Legalității – orice măsură dispusă, inclusiv colectarea și prelucrarea informațiilor, secretizarea și nimitirea va fi realizată în strictă conformitate cu cerințele stabilite de prezenta lege și de alte acte normative în corespundere cu dreptul internațional;</p> <p>b) Egalității tuturor în fața legii – activitatea informativă/contrainformativă va fi realizată în privința oricărei persoane incidente legii, indiferent de statut, poziție socială, funcție exercitată sau oricare alt calificativ;</p> <p>c) Respectării drepturilor și libertăților omului și reglementarea exclusiv prin lege</p>	<p>2. Art. 2 va avea următorul cuprins:</p> <p>„Activitatea informativă/contrainformativă este realizată în corespundere cu următoarele principii:</p> <p>a) Legalității – orice măsură dispusă, inclusiv colectarea și prelucrarea informațiilor, secretizarea și nimitirea va fi realizată în strictă conformitate cu cerințele stabilite de prezenta lege și de alte acte normative în corespundere cu dreptul internațional;</p> <p>b) Egalității tuturor în fața legii – activitatea informativă/contrainformativă va fi realizată în privința oricărei persoane incidente legii, indiferent de statut, poziție socială, funcție exercitată sau oricare alt calificativ;</p> <p>c) Respectării drepturilor și libertăților omului și reglementarea exclusiv prin lege</p>

a restrângerii exercițiului acestora – la orice etapă de dispunere și efectuare a activității informative/contrainformative, inclusiv în cazul stocării, prelucrării informațiilor prin aceste activități, vor exista remedii proporționale și legitime, de restrângere și repunerea persoanelor vizate în drepturile vizate, cu asigurarea unui control independent și imparțial cu privire la respectarea acestor garanții;

d) Oportunității – puterea discreționară a Serviciului sau a organelor cu drept de dispunere a măsurilor informative/contrainformative, va fi realizată prin optarea celei mai potrivite și proporționale soluții, pentru atingerea scopului stabilit, în conformitate cu legea;

e) prin optarea între mai multe soluții posibile corespunzător scopului;

f) Proporționalității – activitatea informativă/contrainformativă va fi dispusă și realizată doar atunci când alte mijloace mai puțin intruzive pentru persoanele vizate nu există sau implică resurse și mijloace disproportionale, cu asigurarea criteriilor de ingerință justificată: doar dacă este prevăzută de lege; urmărește un scop legitim; este necesară într-o societate democratică; este determinată perioada de timp; există remediu pentru repunerea în drepturile restrânse;

g) caracterului activ al măsurilor realizate activitatea informativă/contrainformativă este realizată prompt și doar atunci când există premise certe pentru a fi prevenite sau înlăturate circumstanțele care atentează la securitatea Republicii Moldova;

h) Confidențialității, îmbinării metodelor și mijloacelor de activitate publică și secretă – asigurarea confidențialității și securității metodelor și mijloacelor, este realizată prin măsuri organizatorice și tehnice adecvate și proporționale obiectivelor urmărite;

i) *Neutralității politice și imparțialității* – puterea discreționară și modul de dispunere și efectuare a măsurilor informative/contrainformative, sunt realizate independent și în strictă conformitate cu legea, fără a aduce atingere activităților legitime de: concepere, exprimare și realizare a voinței politice, inclusiv formării opiniei publice sau a libertății de exprimare.”

Completarea prevederilor în cauză este imperioasă în condițiile respectării cerințelor prevăzute la art. 54 alin. (1) lit. i) din Legea nr. 100/2017 cu privire la actele normative. A se menționa că prevederile în cauză instituie principiul care reprezintă norme materiale care se aplică în pe tot textul legii inclusiv în cazul procedurilor de dispunere și efectuare, astfel definirea acestor principii care în versiunea inițială sunt redactate sub forma unor termeni, este absolut necesară. De menționat că proiectul de lege instituie niște împuterniciri

	<p>deosebit de largi Serviciului, iar criteriile de eligibilitate, proporționale sau cerințe prin care se va asigura ingerința în viața privată a persoanelor fizice inclusiv ingerința în activitatea persoanelor juridice, nu sunt stabilite. Anume din acest motiv este foarte important ca aceste principii să aibă rolul de criterii care vor fi puse în aplicare atât de către Serviciu dar și autoritățile abilitate cu dreptul de control și dispunere a acestor activități informative/contrainformative.</p>
<p><b>Se acceptă parțial.</b>          Articolul 3 a fost exclus.</p>	<p>3. La art. 3 alin. (1) și alin. (3), cuvintele „prezentei legi” se substituie cu cuvintele „actelor normative”. Propunerea în cauză este relevantă în contextul cerințelor tehnicii legislative prevăzute la art. 3 alin. (1) lit. c) din Legea nr. 100/2017 cu privire la actele normative, conform căroră, la elaborarea actului normativ trebuie să respecte cerința de legalitate și echilibru între reglementările concurente dar și cerința de predictibilitate a normelor juridice, pentru a nu admite discordanță cu regimul juridic ale altor acte normative care reglementează spre exemplu: domeniul protecției datelor cu caracter personal, libertatea de exprimare etc. A se menționa că păstrarea normelor vizate în versiunea inițială, exclude nejustificat și îngreunează aplicabilitatea altor prevederi legale. Ar rezulta că infracțiunile și faptele contravenționale prevăzute de Codul penal și Codul contravențional, în contextul activității informative/contrainformative (unor activități extrem de largi în care s-ar putea de încadrat orice nu ar face Serviciu), sunt condiționate la prevederile prezentei legi – aspect inadmisibil, care încalcă cras siguranța raporturilor juridice.</p>
<p><b>Se acceptă parțial.</b>          Articolul 3 a fost exclus.</p>	<p>4. La art. 3 se completează cu 2 alineate noi:          - „(4) Termenul de prescripție de atragere la răspundere disciplinară, civilă, contravențională sau penală începe a curge din momentul în care s-a făcut cunoscut faptul încălcării”          - (5) Orice informație, orice probă care au fost acumulate cu încălcarea prevederilor prezentei legi, ale actor acte normative sau a drepturilor și libertăților omului sînt nule și se consideră inexistente.”          Propunerile este justificată prin faptul că activitatea informativă/contrainformativă prin definiție reprezintă o activitate confidențială care se atribuie la secret de stat. Așadar, reieșind din faptul că conform Legii nr. 245/2008 termenul de secretizare pentru activitatea informativă/contrainformativă este NELIMITAT, este necesar de echilibrat aceste norme legale, care sunt imprescriptibile în raport cu drepturile și libertățile persoanelor, în mod corespunzător fiind necesar de stabilit și răspunderea pentru astfel de fapte, pentru că la moment, configurația legală oferă loc de abuz și evitare în totalitate a răspunderii, prin secretizarea pe o</p>

<p>perioadă nelimitată a oricăror informații chiar dacă acestea pot constitui contravenție sau infracțiune. În același context, a se menționa că alin. (5) propus spre completare conține referințe similare celor regăsite la art. 4 alin. (5) din Legea nr. 59/2012 privind activitatea specială de investigații.</p>	<p><b>Nu se acceptă.</b>          Articolul 4 alin. (1) stabilește <i>Activitatea informativă/contrainformativă este efectuată de către Serviciu, prin intermediul ofițerilor de informații și securitate (în continuare - ofițeri de informații) din cadrul subunităților specializate ale acestuia.</i></p>
<p>5. La art. 5 alin. (1), se completează cu cuvintele: „ale căror sarcini și atribuțiile prevăzute de contract sau fișa de post implică expres astfel de activități”. Propunerea vine să detalieze că activitatea informativă/contrainformativă este permisă a fi realizată nu de către orice ofițer de informații și securitate, însă doar celor care fișa de post sau contractul prevede expres astfel de activități, inclusiv completările în cauză au sarcina de a exclude eventualele abuzuri care pot fi admise.</p>	<p><b>Se acceptă.</b></p>
<p>6. La articolul 5 în titlul și la alin. (1), după cuvântul „Drepturile” se completează cu cuvintele „și obligațiile”. Propunerea este înaintată în corespundere cu rigorilor statuate la art. 46 alin. (2) lit. b) din Legea nr. 100/2017 cu privire la actele normative, care stabilește expres că actul normativ trebuie să prevadă nu doar drepturile persoanelor reglementate (în cazul dat Serviciu și ofițerii de informații și securitate) dar și obligațiile acestora.</p> <p>7. La art. 5 alin. (2) lit. a), c) și d) și e) se exclud. Normele vizate în sine presupun o activitate informativă/contrainformativă care necesită a fi autorizată în mod corespunzător, motiv pentru care prevederile în cauză și necesită a fi încadrate în Capitolul II sau III care reglementează activitatea de dispunere și efectuare a activității informative/contrainformative.</p> <p>Așadar, dacă se dorește efectuarea înregistrărilor video/audio atunci aceste activități necesită a fi stabilite expres în cadrul măsurilor informative/contrainformative, similar cum este stabilit spre exemplu la art. 12 alin. (1) pct. 1) lit. c), pct. 2) lit. a) etc. din proiectul de lege, în care se specifică expres utilizarea unor astfel de mijloace, raționamente opozabile și pentru celelalte situații. A se menționa că în corespundere cu raționamentele CtEDO, simplul fapt al colectării datelor cu caracter personal de către o autoritate publică, în sensul art. 8 din CEDO, acest fapt reprezintă o ingerință în viața privată. În acest context, nu este posibilă prin definiție înregistrarea video/audio de către o autoritate publică a datelor cu caracter personal fără a admite o ingerință în viața privată, iar pentru ca această ingerință să fie justificată așa cum stabilește CtEDO, aceasta trebuie să fie dispusă și realizată în ordinea procedurii și garanțiilor stabilite pentru activitatea informativă/contrainformativă cu autorizarea persoanelor responsabile.</p>	<p><b>Se acceptă.</b></p>

<p><b>8.</b> La art. 5 se completează cu un alineat nou:  „(21) În cadrul efectuării activității informative/contrainformative ofiterii de informații sunt obligați:</p> <p>a) să respecte drepturile și interesele legitime ale persoanei;</p> <p>b) să înțeprindă, în limitele competenței, toate măsurile în vederea apărării drepturilor și libertăților omului, protecției tuturor formelor de proprietate ocrotite de lege pentru asigurarea securității statului și a ordinii publice să asigure protecția vieții private în legătură cu prelucrarea datelor cu caracter personal, să asigure inviolabilitatea domiciliului, corespondenței și a regimului juridic al informațiilor cu accesibilitate limitată;</p> <p>c) să execute indicațiilor superiorilor sau a procurorului doar dacă sunt legitime;</p> <p>d) să informeze Procuratura, Instanța de judecată, Centrul Național pentru Protecția Datelor cu Caracter Personal cu privire la informațiile și faptele care sunt realizate cu încălcarea prezentei. legi sau ale altor acte normative, corespunzător domeniul de competență;</p> <p>e) să respecte proporționalitatea dintre scopul urmărit și legătura de cauzalitate cu activitatea informativă/contrainformativă, mijloacele puse în aplicare și drepturile restrânse ale persoanelor vizate.”</p> <p>Normele de referință necesită a fi introduse în proiectul de lege având în vedere rigorile prevăzute de tehnica legislativă pentru proiecte de lege, în special care rezultă din prevederile art. 46 alin. (2) lit. b) din Legea nr. 100/2017 cu privire la actele normative, care stabilesc expres dispozițiile de conținut trebuie să conțină nu doar drepturile subiecților reglementați dar și obligațiile acestora.</p>	<p><b>Nu se acceptă.</b>  Statutul juridic al ofiterului de informații de securitate este reglementat doar în Legea nr.170/2007 privind statutul ofiterului de informații și securitate.</p>
<p><b>9.</b> La art. 5 alin. (3) și alin. (4) se exclud. A se menționa că prevederile în cauză reprezintă o tautologie juridică pe motiv că norme similare, cu o reglementare mai detaliată și mai extinsă se regăsește la art. 8 alin. (1) pct. 7) și pct. 9), pct. 11), pct. 20) din proiectul de lege nr. 420 cu privire la Serviciul de Informații și Securitate al Republicii Moldova, fapt care contravine art. 54 alin. (1) lit. g) din Legea nr. 100/2017 cu privire la actele normative.</p> <p><b>10.</b> La art. 6 alin. (1) cuvintele „sau verbal” se exclude. Norma vizată creează premise pentru abuzuri sau evitarea responsabilității din partea ofiterilor de informații și securitate în vederea declarării fictive cu privire la încheierea unor astfel de acorduri confidențiale cu persoane. Este arhicunoscut faptul în cercurile Serviciului, asupra numeroaselor cazuri de declarare fictivă privitor la încheierea acordurilor de colaborare confidențială, care legitimează practic orice bârfă sau aluzie cu privire al fapte și evenimente care de regulă sunt prescrise tot de către ofiterul de informații și securitate rău intenționat, dar și</p>	<p><b>Se acceptă.</b></p> <p><b>Se acceptă parțial.</b>  Articolul 6 a fost exclus.</p>

<p>permite obținerea unor surse necuvenite de remunerare în numele persoane declarate fictiv ca fiind colaborator. Așadar, prin includerea posibilității încheierii verbale a acestor acorduri, circumstanțele descrise mai devreme devin a fi și mai accesibile.</p>	<p>11. La art. 6 alin. (1) cuvintele „precum și să contribuie într-un alt mod, neinterzis de lege, la activitatea informativă/contrainformativă” se exclud. Prevederile în cauză distorsionează obiectul de reglementare a prezentei legi, care are obiectiv de a institui limitativ, specific și proporțional cu drepturile restrânse a unor activități și măsuri JUSTIFICATE care sunt în măsură să contribuie la contracararea faptelor care atentează la securitatea Statutului, pe când normele de referință oferă posibilitatea acestor persoane care vor colabora cu Serviciu (după cum a fost menționat și mai sus, ar putea „colabora” fictiv) de a contribui într-un mod neinterzis de lege. A se menționa că sfera de reglementare a prezentului proiect este sfera dreptului public unde este aplicabilă regula „ceea ce nu este permis este interzis” și nu a dreptului privat unde se stabilește viceversa „ceea ce nu este interzis este permis”.</p>	<p><b>Se acceptă parțial.</b> Articolul 6 a fost exclus.</p>
<p>12. La art. 6 alin. (9) cuvintele „ceea ce o lipsește de posibilitatea de a colabora în continuare” se exclud. Condiționalitatea de a nu mai putea colabora mai departe nu poate constitui pretext pentru a nu obține indemnizația dată, pe motiv că aceasta se acordă pentru prejudiciile și suferințele survenite în legătură cu colaborarea anterioară și nu cea care ar urma să aibă loc. Mai mult, art. 6 ar fi oportun de a fi excluse din acest proiect de lege și încadrat la art. 25 din proiectul de lege nr. 420 cu privire la Serviciul de Informații și Securitate al Republicii Moldova, pe motiv că norma de referință conține reglementări similare.</p>	<p>13. La art. 6 alin. (3) va avea următorul cuprins: „Activitățile indicate la alin. (1) se acordă Serviciului gratuit sau remunerat din bugetul de stat”. A se menționa că proiectul de lege la art.6 alin. (1) stabilește expres activitățile în care poate fi implicată persoana care va colabora, iar cuvântul „sprijin” este unul nedeterminat și gerează înțeles extins și injust, contrar prevederilor art. 54 alin. (1) lit. a) din Legea nr. 100/2017 cu privire la actele normative.</p>	<p><b>Se acceptă parțial.</b> Articolul 6 a fost exclus.</p>
<p>14. La art. 6 alin. (5) norma necesită a fi concretizată, în special de inclus cazurile în care pot fi dispuse măsurile informative/contrainformative dar și necesitatea existenței acordului persoanei vizate și a membrilor de familie, având în vedere că orice activități de protecție în privința unei persoane pot avea loc cu condiția că aceasta le consimte. Aceste detalieri sunt necesare pentru a exclude eventualele cazuri de abuz prin care măsurile extrem de intruzive ce se referă la activitatea informativă/contrainformativă să poată fi aplicate nestingherit și tendențios.</p>	<p><b>Se acceptă parțial.</b> Articolul 6 a fost exclus.</p>	

<p><b>Se acceptă parțial.</b> Articolul 7 a fost exclus.</p>	<p>15. La art. 7 alin. (1) după cuvintele „prezentei legi” se completează cu cuvintele „sau ale altor acte normative, în limita autorizației emise”, cuvintele „imediat, gratis” se substituie cu cuvântul „gratuit”. A se menționa că acest proiect de lege nu poate limita sau exclude caracterul regulatoriu ale altor legi care stabilește cerințe față de modul de prelucrare a datelor și asigurarea măsurilor de protecție, din care motiv, pentru asigurarea securității raporturilor juridice, prevederile în cauză au fost racordate prin extinderea și la alte acte normative. Mai mult, reieșind din faptul că activitatea informativă/contrainformativă reprezintă o activitate autorizată, pentru a exclude posibilitatea utilizării abuzive și necontrolate a acestor prevederi în raport cu orice persoană fizică sau juridică, obligația de a prezenta informația se va limita la obiectul dispus de autorizație. În același context, reieșind din faptul că cuvintele „imediat și gratis” sunt contradictorii și pot genera situații de risc pentru mediul de afaceri de la care se va solicita prezentarea informațiilor, prevederile în cauză au fost modificate pentru a fi previzibile.</p>
<p><b>Se acceptă parțial.</b> Articolul 7 a fost exclus.</p>	<p>16. La art. 7 alin. (2) pct. 1), după cuvintele „comunicații electronice” se completează cu cuvintele „în limita autorizației”. A se menționa că activitatea informativă/ contrainformativă nu presupune o activitate permanentă/sistematică/nedeterminată, care constituie o activitate specifică determinată de condițiile și termenele stabilite în autorizație. Așadar, în formula expusă, ar rezulta că Serviciul ar putea cere filtrarea traficului de date sau a corespondenței în regim permanent/nelimitat. Astfel, pentru a exclude eventualele interpretări, dar și pentru a îmbunătăți precizia normei, s-a propus includerea condiționalității că aceste măsuri să derive în limita interioară a autorizației specifice pentru fiecare caz în parte.</p>
<p><b>Se acceptă parțial.</b> Articolul 7 a fost exclus.</p>	<p>17. La art. 7 alin. (2) pct. 3 după cuvintele „Tehnologia Informației” se completează cu cuvintele „și Centrul Național pentru Protecția Datelor cu Caracter Personal”. Propunerea rezultă din competențele funcționale atribuite Centrului Național pentru Protecția Datelor cu Caracter Personal prin Legea nr. 133/2011 privind protecția datelor cu caracter personal și art. 71 alin. (3) din Legea nr. 241/2007 privind comunicațiile electronice. A se menționa că unul dintre obiectivele de bază prevăzute de proiectul de lege, este de a asigura proporționalitatea restrângerilor drepturilor fundamentale, în special dreptul la viața privată, dar și asigurării unor mecanisme corespunzătoare de confidențialitate și securitate în cazul realizării activității informative/contrainformative, opozabile speței fiind art. 4 și art. 29 și 30 din Legea nr.133/2011 privind protecția datelor cu caracter personal.</p>
<p><b>Se acceptă parțial.</b> Articolul 7 a fost exclus.</p>	<p>18. La art. 7 alin. (2) pct. 4) cuvântul „toate” se exclude, după cuvintele „,comunicații electronice” se completează cu cuvântul „necesare”. Redacția</p>

<p>proiectului generează riscul de a solicita în exces la infrastructura software/hardware și administrativă, inclusiv atunci când nu este necesar sau este excesivă. Normele de referință au scopul de a echilibra prevederile în cauză.</p>	<p>19. La art. 9 alin. (1) se completează la final cu cuvintele: „ și care va conține cel puțin: data inițierii, ofițerii de informație și securitate desemnați; persoanele fizice și juridice vizate de activitatea informativă/contrainformativă; autorizațiile măsurilor informative/contrainformative; informațiile și documentele colectate în cadrul dosarului și temeiul legal; perioada de stocare, secretizare și repunerii în drepturile restrânse ale persoanelor vizate; resursele informaționale și registrele accesate cu includerea tipului operațiunilor realizate: vizualizare, extragere; oricare alte date relevante. Dosarul special se consideră a fi inițiat din momentul efectuării măsurilor informative/contrainformative sau a oricăror activități în legătură cu acestea în privința unei persoane concrete.” Completarea în cauză este necesară pentru a determina clar momentul pornirii/inițierii dosarului special și începerea a curgerii termenelor dar și respectării cerințelor prevăzute de prezenta lege.</p>	<p><b>Se acceptă.</b>  Articolul 9 a fost completat cu 2 alineate noi.  <i>Dosarul special se inițiază în baza raportului ofițerului de informații din cadrul subunității specializate, aprobat de către directorul Serviciului sau directorul adjunct special împuternicit. Dosarul special se consideră inițiat din data înregistrării acestuia.</i>  <i>Măsurile contrainformative și măsurile informative externe nu pot fi realizate în afara unui dosar special.</i></p>	<p>Totodată, alin. (2) din redacția actuală prevede reglementări relevante celor propuse:  (2) <i>Fiecare dosar special va include un mecanism de evidență a persoanelor care au făcut cunoștință cu materialele dosarului, care va include:</i>  a) <i>numele, prenumele și funcția persoanei;</i>  b) <i>data, anul și ora inițierii luării de cunoștință cu materialele dosarului și data, anul și ora finalizării acesteia;</i>  c) <i>mențiuni vizând accesul la dosarul special integral, anumite documente sau compartimente ale acestuia,</i>  d) <i>semnătura persoanei.</i></p>	<p><b>Se acceptă parțial.</b>  Art. 10 a fost reformulat conceptual. Totodată, proiectul prevede deja un articol privind <i>Informarea persoanei despre</i></p>
	<p>20. La art. 10 după cuvintele „clasarea dosarului special,” se completează cu cuvintele „persoanele vizate se informează cu privire la prelucrarea acestor date după care”. Redacția proiectului nu asigură un echilibru asupra drepturilor restrânse în legătură cu activitatea informativă/contrainformativă.</p>			

<p>A se menționa că în cazul în care evităm informarea persoanei cu privire la faptul prelucrării informațiilor care s-au adeverit a fi irelevante, cu distrugerea acestora, în acest fel facem ca persoana să nu mai poată fi repusă în drepturile restrânse, și face imposibilă revendicarea încălcării dreptului la viața privată în legătură cu această prelucrare a datelor. Conchidem că versiunea proiectului generează un remediu perfect pentru ștergerea tuturor probelor și urmelor în ceea ce privește eventualele colectări excesive și ilegale de date și oferă posibilitatea Serviciului de a evita orice răspundere, or, norma vizată nu prevede care sunt criteriile după care informația va fi determinată ca fiind irelevantă și cine va decide în cazul dat. Mai mult, prevederile în cauză sunt periculoase deoarece nu face distincția dintre cazurile de colectare excesivă și ilegală și cazurile când informația s-a dovedit a fi irelevantă. În același context, este evitat orice mecanism de control și de verificare cu privire la faptul dacă datele sunt irelevante sau nu.</p>	<p><b>Nu se acceptă.</b>  Articolul 11 este indispensabil întrucât oferă soluții pentru întreg spectrul de probleme care necesită o reglementare detaliată la nivel departamental (datorită specificului activității contrainformative și activității informative externe, inclusiv datorită clasificării informațiilor detaliate privind tactica și metodică AIC).</p> <p>Totodată, drepturile și garanțiile persoanelor fizice sunt asigurate plenar prin reglementările existente în proiectul legii. Activitatea contrainformativă și informativă externă va avea filtre de supraveghere și control atât la nivel intern cât și extern.  Concomitent actele normative departamentale nu pot excede prevederile legii.</p> <p><b>Se acceptă.</b>  Articolul a fost revizuit conceptual.</p>
<p>21. Art. 11 care conține un volum exorbitant de atribuții atribuite Serviciului urmează a fi exclus pe motiv că contravine art. 3 alin. (1) lit. c) și f) din Legea nr. 100/2017 cu privire la actele normative. De menționat că este inacceptabil și contrar regulilor tehnicii legislative ca efectul regulator al actului legislativ superior să fie detașat și echivalat cu puterea actelor normative departamentale ale Serviciului, care vor fi emise unilateral, fără consultare publică, fără a se publica în Monitorul Oficial și fără a putea face cunoștință cu conținutul acestora. Prevederile acestui articol urmează a fi excluse pentru că sunt abuzive și creează riscul de reglementare exagerată și necontrolată, ceea ce reprezintă un pericol iminent pentru mediul de afaceri, mediul asociativ dar și la general.</p>	<p>22. La art. 12 alin. (1) pct. 1), cu excepția prevederilor de la lit. d), h), i), se exclud.  Din start urmează a fi menționat că așa cum raționalizează CEDO, măsurile care limitează drepturile persoanelor trebuie să fie proporționale și adecvate gravității faptelor și valorilor sociale protejate de lege. Anume din acest</p>

considerent, măsurile intruzive realizate de către organele statului și care limitează esențial drepturile fundamentale ale persoanei, NU pot fi realizate în orice situație sau procedură precum: procedură administrativă, civilă, contravențională, disciplinară etc. – doarece valorile sociale protejate în aceste cazuri NU sunt în măsură să justifice ingerințele admise în viața privată a persoanelor.

De menționat că procedura de dispunere și efectuare a măsurilor repetă obiectul de

reglementare a Legii nr. 59/2012 privind activitatea specială de investigație dar și scopul legii penale prevăzut la art. 2 alin. (1) din Codul penal, care stabilește expres că **Legea penală apără, împotriva infracțiunilor, persoana, drepturile și libertățile acesteia, proprietatea, mediul înconjurător, orînduirea constituțională, suveranitatea, independența și integritatea teritorială a Republicii Moldova**, pacea și securitatea omenirii, precum și întreaga ordine de drept, aspecte reflectate expres în mai multe prevederi ale Codului:

- Art. 338 Spionajul;
- Art. 339 Uzurparea puterii de stat;
- Art. 340 Rebeliunea armată;
- Art. 342 Atentarea la viața Președintelui Republicii Moldova, a Președintelui Parlamentului sau a Prim-ministrului;
- Art. 343 Diversiunea;
- Art. 344 Divulgarea secretului de stat;
- Art. 347 Profanarea simbolurilor de stat;
- Art. 351 Uzurparea de calități oficiale;
- Etc.

În cele din urmă, prevederile proiectului determină o procedură paralelă de procesul penal, care presupune eschivarea de la principalele garanții ale procesului penal, precum: prezumția de nevinovăție, dreptul la apărare, dreptul la justiție etc. prin dispunerea și realizarea măsurilor deosebit de intruzive de către aceeași autoritate publică, care ar putea să acopere propriile nereușite sau abuzuri prin dispunerea și efectuarea măsurilor contrainformative în exces cu scopul de a șantaja sau denigra anumite persoane.

În cele din urmă, la general considerăm inoportună, nenecesară și abuzivă intenția de a trece setul de măsuri caracteristice procesului penal în afara acestui, care va încălca cras drepturile și libertățile persoanei, motiv pentru care considerăm necesar păstrarea acestor activități în interiorul procesului penal.

<p>A se atenționa că unele și aceleași fapte fac obiectul de reglementare a 2 legi: proiectul privind activitatea informativă/contrainformativă și Codul de procedură penală – ceea ce va duce la încălcarea principiului că nimeni nu poate fi tras la răspundere pentru una și aceeași faptă de mai multe ori, inclusiv, va genera dualitatea de norme aplicabile ceea ce va sfida cerințele unui proces echitabil, în toate cazurile, orice neclarități vor fi interpretate în favoarea persoanelor vizate și în final la condamnarea Republicii Moldova la CEDO.</p>	<p><b>23.</b> La art. 12 dorim să menționăm că nu cunoaștem aplicarea în practică internațională a unei așa măsuri ca "blocarea unui punct de acces conectat la un sistem informatic sau la rețelele de comunicații". Totodată, considerăm că modul în care a fost detaliată această măsură în art. 44 al Proiectului, lasă de dorit, fiindcă nu este clar: în ce circumstanțe poate fi dispusă măsura, pentru ce infracțiuni, pentru ce perioadă și care sunt condițiile în baza cărora se decide deconectarea definitivă sau este permisă reconectarea punctului de acces și notificarea persoanei supuse acestei măsuri cu privire la aplicarea măsurii și drepturile acesteia.</p>	<p><b>24.</b> Totodată, dorim să menționăm că măsura cu privire la interceptarea comunicărilor conține în sine înregistrarea comunicărilor voce, text și transfer de date/internet, pe când la momentul actual acestea au reglementări distincte 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><b>25.</b> La art. 15 alin. (14) după cuvintele „judecătorul dispune” se completează cu cuvintele cu informarea în prealabil a persoanelor vizate de măsurile ilegale cu punerea la dispoziție a unei copii a informațiilor”. Completările în cauză sunt necesare pentru restabilirea drepturilor restrânse ale persoanelor vizate și după caz realizarea acțiunii în regres prin obținerea despăgubirilor în cazul activităților ilegale. A se menționa că la momentul norma este abuzivă deoarece nu prevede mecanismul de informare a persoanei și generează premise de evitare a răspunderii de către Serviciu în cazul acțiunilor ilegale constatate de către instanță.</p>	<p><b>26.</b> La art. 17 alin. (1) și (2) cifrele „90” se vor substitui cu cifrele „30”. Termenul de 90 de zile este excesiv și depășește limitele admise spre exemplu de procesul penal care la fel este stabilit la 30 de zile.</p>
	<p><b>Se acceptă parțial.</b> Textul a fost revizuit conceptual conform deciziei grupului de lucru de pe lângă Comisia parlamentară securitate națională, apărare și ordine publică.</p>	<p><b>Se acceptă parțial.</b> Articolul 12 a fost revizuit și articolul 38 (Interceptarea comunicărilor cu înregistrarea acestora) a fost modificat la fel.</p>	<p><b>Se acceptă parțial.</b> Norma a fost revizuită, fiind exclusă posibilitatea distrugerii materialelor. Totodată, ca măsură de garanție împotriva abuzului au fost introdus articolul ce vizează <i>Controlul legalității efectuării măsurilor contrainformative de către judecător.</i> Totodată, atragem atenția asupra articolului 23 <i>Informarea persoanei despre măsurile contrainformative înfăptuite în privința sa.</i></p>	<p><b>Nu se acceptă.</b> Activitatea contrainformativă este distinctă de activitatea specială de investigații</p>

<p>realizată în cadrul procesului penal. Acesta și este scopul existenței unei legi speciale separate.</p>	<p><b>Se acceptă parțial.</b> Art. 17 alin. (3) a fost exclus.</p>	
<p><b>Nu se acceptă.</b> Activitatea contrainformativă este distinctă de activitatea specială de investigații realizată în cadrul procesului penal. Acesta și este scopul existenței unei legi speciale separate.</p>	<p>27. La art. 17 alin. (3) cuvintele „, , cu posibilitatea de prelungire pe perioade succesive precum și pe perioade care nu se succed, de până la 6 luni” se exclud. Aceste prevederi sunt abuzive și generează posibilitatea nejustificată de a aplica repetitiv prelungirea unui termen care este finit/exhaustiv, or, includerea unor mecanisme repetitive de prelungire a termenului la înfinit sunt abuzive și încalcă grav dreptul la viața privată – circumstanțe opozabile și pentru alin. (4) din același articol.</p>	<p><b>Nu se acceptă.</b> Activitatea contrainformativă este distinctă de activitatea specială de investigații realizată în cadrul procesului penal. Acesta și este scopul existenței unei legi speciale separate.</p>
<p><b>Nu se acceptă.</b> <i>Confidențialitatea datelor cu privire la măsurile contrainformative</i> reprezintă o condiție indispensabilă pentru a nu prejudicia activitatea contrainformativă. Din acest considerent, conform deciziei grupului de lucru de pe lângă Comisia parlamentară securitate națională, apărare și ordine publică, articolul urmează a fi păstrat.</p>	<p>28. La art. 17 alin. (5) textul „2 ani” se substituie cu cuvintele „ 6 luni”. Termenul de 2 ani este excesiv și limitează nejustificat pe o perioadă extrem de mare drepturile și libertățile fundamentale. A se menționa că termenul stabilit în cadrul activităților contrainformative/informative nu poate depăși termenul stabilit în cadrul procesului penal de Legea nr. 59/2012 privind activitatea specială de investigație care la fel stabilește termenul maxim de 6 luni.</p> <p>29. La art. 22 alin. (2) și (3) se exclud. Prevederile în cauză reprezintă tautologie juridică și generează o supraplementare, pe motiv că odată ce informațiile sunt atribuite la secret de stat, modul de acces, stocare și prelucrare a datelor este prevăzut de Legea 245/2008 cu privire al secretul de stat. A se menționa că asigurarea secretului de stat și asigurarea confidențialității datelor sunt aspecte diferite, iar în contextul normelor de reglementare, se formalizează colizia dintre prevederile proiectului și legea organică indicată.</p>	<p><b>Nu se acceptă.</b> A se vedea art. 12 alin. (1) pct. 1) care a fost revizuit substanțial. Astfel, măsurile care reprezintă o ingerință serioasă în viața privată a persoanei se autorizează conform art. 12 alin. (1) pct. 2)</p>
<p><b>Nu se acceptă.</b> A fost introdus un nou articol privind controlul legalității efectuării măsurilor contrainformative de către judecător. Totodată, în cadrul grupului de lucru de pe lângă Comisia parlamentară securitate națională, apărare și ordine publică s-a</p>	<p>30. La art. 23 alin. (1) după textul: alin. (1) se completează cu textul: „pct. 1) și”. De menționat că proiectul tendențios indică obligația de informare a persoanei doar în cazurile autorizate de instanță însă nu și cazurile în care măsurile sunt autorizate de Serviciu.</p> <p>31. La art. 23 alin. (3) se exclude. Norma dată este abuzivă și creează premise Serviciului de a nu informa niciodată în cazurile în care va considera necesar sau în cazurile spre exemplu de abuz sau încălcare pentru a putea evita răspunderea pentru ilegalitățile admise. Orice ne-informare reprezintă restrângerea dreptului care trebuie să aibă început și sfârșit, orice creare de mecanisme care extind excesiv acest termen se consideră o încălcare nejustificată a drepturilor fundamentale ale persoanei – circumstanțe care se</p>	<p><b>Nu se acceptă.</b> A fost introdus un nou articol privind controlul legalității efectuării măsurilor contrainformative de către judecător. Totodată, în cadrul grupului de lucru de pe lângă Comisia parlamentară securitate națională, apărare și ordine publică s-a</p>

<p>aplică în mod corespunzător alin. (4) - (7).</p>	<p>revăzut proiectul prin prisma eficacității mecanismelor de control și supraveghere a activității contrainformative.</p> <p><b>Se acceptă.</b></p>
<p>32. La art. 24 alin. (3) cuvintele: „directorului Serviciului sau directorului adjunct special împuternicit, în care se va indica doar categoria de informații ce urmează a fi prezentată și, după caz, termenul de efectuare a monitorizării” se exclud. Accesul la tranzacțiile financiare se realizează doar în baza autorizației emise de instanța de judecată, motiv pentru care normele de referință urmează a fi excluse pe motiv că creează pericol pentru siguranța secretului bancar și a cerințelor de păstrare a confidențialității clienților.</p>	<p><b>Se acceptă.</b>          Articolul 12 a fost revizuit substanțial (<i>Procedura de autorizare a măsurilor contrainformative</i>), corespunzător au fost modificate și articolele menționate.</p>
<p>33. Art. 26-45 urmează a fi modificat corespunzător modului de autorizare propus, care să fie efectuat de către instanța de judecată.</p>	<p><b>Se acceptă parțial.</b>          A fost introdus un articol nou ce vizează controlul asupra prelucrării datelor cu caracter personal în cadrul activității informative/contrainformative.</p>
<p>34. La Capitolul VI se va completa cu un articol nou: „Articolul 601 Controlul respectării dreptului la viața privată sau a altor drepturi fundamentale în cazul efectuării măsurilor informative/contrainformative se realizează de Centrul Național pentru Protecția Datelor cu Caracter Personal, Avocatul Poporului sau alte autorități publice investite cu astfel de prerogative”. Modificarea este argumentată prin faptul că nu poate fi exclus Serviciul de sub controlul acest 2 instituții are au mandat clar în ceea ce privește domeniile de activitate care vizează în mod inerent activitatea Serviciului.</p>	<p><b>Se acceptă parțial.</b>          Articolele 38-39 au fost reformulate. Totodată, urmează a fi accentuat faptul că activitatea informativă externă și activitatea contrainformativă reprezintă un mecanism distinct de activitatea specială de investigații și nu se încadrează în reglementările Codului de Procedură Penală și Legii 59/2012 privind activitatea specială de investigație.</p>
<p>35. Referitor la interceptarea comunicărilor, art. 38-39 din Proiect, dorim să menționăm că, CEDO s-a expus la condițiile de efectuare a acestei măsuri și a emis un șir de recomandări, care sunt necesare a fi reflectate în proiect, în special (vezi Ghidul CEDO privind art. 8 din Convenție – Dreptul la respectarea vieții private și de familie, redacția 31.12.2018): ”Punctul 511. O lege privind măsuri de supraveghere secretă trebuie să ofere următoarele garanții minime de protecție împotriva abuzurilor de putere: să definească natura infracțiunilor susceptibile să genereze emiteră unui mandat de interceptare și categoriile de persoane susceptibile să facă obiectul unei măsuri de interceptare; să stabilească un termen limită pentru durata executării măsurii în cauză; să prevadă procedura care trebuie urmată pentru examinarea, utilizarea și păstrarea datelor obținute, măsurile de precauție care trebuie luate pentru comunicarea datelor către alte părți și circumstanțele în care este posibilă sau necesară ștergerea ori distrugerea”</p> <p>”Punctul 515. Sfera de aplicare a măsurilor de supraveghere secretă:</p>	<p><b>Se acceptă parțial.</b>          Articolele 38-39 au fost reformulate. Totodată, urmează a fi accentuat faptul că activitatea informativă externă și activitatea contrainformativă reprezintă un mecanism distinct de activitatea specială de investigații și nu se încadrează în reglementările Codului de Procedură Penală și Legii 59/2012 privind activitatea specială de investigație.</p>

cetățenilor trebuie să li se ofere indicii adecvate privind circumstanțele în care autoritățile publice sunt abilitate să recurgă la astfel de măsuri. În special, este important să se stabilească în mod clar natura infracțiunilor susceptibile să genereze emiterea unui mandat de interceptare și să fie definite categoriile de persoane susceptibile să facă obiectul unei interceptări a convorbirilor telefonice”. La moment, Codul de Procedură Penală prevede lista infracțiunilor pentru care poate fi aplicată această măsură și considerăm că Proiectul de asemenea ar trebui să prevadă această listă.

Totodată, Ghidul menționează că ”Măsurile de interceptare ce vizează o persoană care nu este bănuită de o infracțiune, dar care ar putea deține informații cu privire la o astfel de infracțiune, pot fi justificate în temeiul art. 8 din Convenție [Greuter împotriva Țărilor de Jos (dec.), privind o măsură de interceptare a convorbirilor telefonice dispusă și supravegheată de către un judecător, despre care reclamantul a fost informat]. Cu toate acestea, categoriile de persoane care pot face obiectul unei măsuri de interceptare a convorbirilor telefonice nu sunt definite suficient de clar în cazul în care acestea includ nu numai suspecți sau acuzați, ci și „orice altă persoană implicată în săvârșirea unei infracțiuni”, fără să ofere nicio explicație cu privire la modul în care trebuie interpretată această sintagmă [Lordachi și alții împotriva Republicii Moldova, pct. 44, în care reclamantul au susținut că erau expuși unui risc serios de a face obiectul unei măsuri de interceptare a convorbirilor telefonice, din cauza faptului că erau membri ai unei organizații guvernamentale, specializată în reprezentarea reclamanților în fața Curții; a se vedea și Roman Zakharov împotriva Rusiei (MC), pct. 245; Szabó și Vissy împotriva Ungariei, pct. 67 și 73]. În cauza Amann împotriva Elveției (MC), privind un dosar deschis și păstrat de către autorități în urma interceptării unei convorbiri telefonice, Curtea a constatat o încălcare, întrucât, printre altele, legislația relevantă nu reglementa în detaliu situația persoanelor care erau monitorizate „întâmplător”.

36. Referitor la art. 41 din Proiect, colectarea informației de la furnizorii de servicii de comunicații electronice, considerăm că redacția actuală necesită a fi revizuită, fiindcă dublează parțial reglementările cu privire la identificarea abonatului/utilizatorului unui sistem de comunicații sau interceptare, ceea ce contravine tehnicii legislative, iar scopul acestei măsuri este obținerea informației cu privire la comunicări, adică lista apelurilor. De altfel în legislația românească această măsură are denumirea de ”obținerea listei convorbirilor telefonice (art. 153 CPP al României). Respectiv, propunem următoarea redacție:

**Articolul 41.** Obținerea informației cu privire la comunicările telefonice

**Se acceptă parțial.**

Articolul 41 a fost reformulat, conform deciziei grupului de lucru instituit pe lângă Comisia parlamentară securitate națională, apărare și ordine publică.

<p><b>Asociația Națională a Companiilor din Domeniul TIC (ATIC)</b> Nr.12 din 15 februarie 2023</p>	<p>(1) Obținerea informației cu privire la comunicările telefonice a persoanelor supuse măsurii contrainformative, inclusiv de roaming, precum: tipul, data, orei și durata comunicației electronice, identificarea echipamentului de comunicații electronice al utilizatorului sau al altui dispozitiv utilizat pentru comunicație, identificarea coordonatelor echipamentului care a deservit terminalul de comunicații mobile, și în special despre:</p> <ol style="list-style-type: none"> <li>1) serviciile de comunicații electronice prestate utilizatorului;</li> <li>2) destinația comunicației electronice (datele de identificare tehnice al apelatului; datele de identificare tehnice ale punctului de acces redirectionat);</li> <li>3) 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>4) echipamentul de comunicații electronice al utilizatorului sau un alt dispozitiv utilizat pentru comunicație {codurile IMSI și IMEI ale telefoanelor mobile ale apelantului și apelatului; };</li> <li>5) identificarea coordonatelor echipamentului care a deservit terminalul de comunicații mobile {denumirea locației (Cell ID) de la începutul comunicației; locația geografică a celei prin referință la denumirea locației, în perioada în care datele sunt reținute};</li> </ol> <p>(2) Colectarea informației de la furnizorii de servicii de comunicații electronice se realizează: prin prezentarea nemijlocită către furnizorii de servicii de comunicații electronice a extrasului din mandatul judecătoresc/închirerea judecătorului în care se va indica doar categoria de informații ce urmează a fi prezentată;</p>
<p><b>Se acceptă.</b> Articolul 7 a fost exclus.</p>	<p><b>1. La articolul 7.</b> <b>La art. 7 alin. (1),</b> 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 și că, la cererea persoanelor, Serviciul le compensează, în modul stabilit de legislația 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”.</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.

**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.

**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.

**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.

**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 înfăptuirea de către Serviciu a măsurilor contrainformative sau informativă externe. Furnizorii achită impozite și taxe în bugetul de stat și nu pot fi obligați să finanțeze suplimentar procurarea echipamentelor necesare pentru activitatea SIS.

## 2. La articolul 25.

**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).

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.

Această neclaritate face imposibilă determinarea modului corect de autorizare a prezentării anumitor informații de către furnizorii de comunicații 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 adreselor 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.

## Se acceptă.

Norma de la art. 25 alin. (1) a fost revizuită și nu utilizează termenii „sistem de comunicații electronice”. „mijloc de comunicații electronice” și „punct de acces la un sistem informatic”.

Referitor la procedura de autorizare și a informațiilor care urmează a fi furnizate, prevederile au fost redactate conform celor stabilite de grupul de lucru pe lângă Comisia parlamentară securitate națională, apărare și ordine publică.

<p><b>La art. 25 alin. (3)</b>, 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 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.</p>	<p><b>Se acceptă.</b> Acest aliniat a fost revizuit, iar termenul de 24 de ore stabilit a fost exclus.</p>
<p><b>3. La articolul 38.</b> 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.</p>	<p><b>Se acceptă.</b> Prevederile articolului au fost revizuite ținând cont de propunerile marilor operatori de comunicații electronice.</p>
<p><b>4. La articolul 41.</b> 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 trebui exclus sau mutat la articolul ce reglementează interceptarea. 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. La art. 41 alin. (1) pct. 4) și 5), este necesar de a defini clar ce se înțelege prin "date de identificare tehnice". La art. 41 alin. (1) pct. 7), este necesar de a exclude referința la codurile "IMSI"</p>	<p><b>Se acceptă.</b> Textul „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, precum și obținerea de la operatorii a” a fost exclus. Astfel, în redacția actuală sensul oferit măsurii de colectare a informației de la furnizorii de servicii de comunicații electronice nu se confundă cu măsura interceptării comunicărilor.  De asemenea, la art. 41 alin. (1), pct. 1 sintagmele „date de identificare tehnice”, „codurile IMSI”, „informația ce identifică</p>

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.

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.

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 conectate la echipamentul furnizorilor, ar trebui exclusă.

În hotărârile sale pe dosarele Digital Rights Ireland și 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.

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:

- să fie clar și precis;
  - 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;
  - 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.
- 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.

echipamentul comunicațional" din conținutul acestui articol, au fost excluse.

La alin. (2), litera b) a fost exclusă.

<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, 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>5. La articolul 44.</b> La art. 44, norma respectivă ar trebuie exclusă, deoarece este ineficientă. 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. Dacă prin mijloc de comunicații se înțelege 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 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><b>Se acceptă parțial.</b> Norma a fost revizuită iar termenul de „mijloc de comunicații” a fost exclus.</p> <p>Redacția actuală a acestui articol a fost revizuită conceptual și prevede clar modurile de blocare a accesului la rețelele de comunicații electronice.</p> <p><b>Se acceptă.</b> Acest articol a fost revizuit și a fost incluse modificări care prevăd expres ce informații trebuie să conțină în mod obligatoriu raportul, și anume: numărul total de măsuri, numărul dosarelor speciale inițiate, numărul persoanelor informate în privința cărora s-au desfășurat măsuri, date despre eventuale încălcări comise de către ofițerii de informații. La necesitate pot fi furnizate și alte date atâta timp cât se menționează doar datele care sunt prezentate în mod obligatoriu. Tot în acest sens, subcomisia parlamentară în mod obligatoriu va publica pe pagina web a</p>
	<p><b>6. La articolul 57.</b> 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 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”.</p>	

	<p>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>	<p>Parlamentului rezultatele controlului activității informative/contrainformative. Mai mult ca atât, ca o garanție a respectării legislației de către Serviciu, în cazul în care subcomisia va constata încălcări grave aceasta va putea solicita o anchetă parlamentară sau sesiza Procurorul General.</p>
<p><b>Procuratura Generală</b> Nr.4-1d/23-182 din 17 februarie 2023</p>	<p>1. Analiza proiectului de lege atestă că prevederile acestuia se intercalează cu prevederile Legii nr.59/2012 privind activitatea specială de investigații, iar în acest context procedura de dispunere și efectuare a măsurilor repetă obiectul de reglementare a ultimei.</p> <p>Totodată, se învederează inițiativa de a permite Serviciului de Informații și Securitate al Republicii Moldova (<i>în continuare SIS</i>) să efectueze măsuri speciale de investigații în afara procedurilor penale, care în proiectul de lege au fost denumite generic măsuri contrainformative.</p> <p>Măsurile contrainformative vor putea fi autorizate atât de directorul SIS sau directorul adjunct special împuternicit, dar și prin mandat judecătoresc. Se atestă însă faptul că, în cazul măsurilor autorizate de către directorul SIS sau directorul adjunct special împuternicit, prezentate ca fiind mai puțin intruzive în viața privată a persoanelor, nu sunt clar definite și reglementate mecanismele de control jurisdicțional, sfera și limitele controlului exercitat de procuror (art.58 din proiect).</p> <p>Prin urmare, este esențial să existe reguli clare și detaliate privind măsurile de supraveghere secrete, iar <b>legea internă trebuie să fie suficient de clară pentru a oferi cetățenilor o indicație adecvată cu privire la circumstanțele și condițiile în care autoritățile publice sunt împuternicite să recurgă la astfel de măsuri.</b></p> <p>Deși autoritățile și organele legislative naționale dispun de o anumită marjă de apreciere pentru a stabili cea mai bună politică în acest domeniu, statele contractante <b>nu beneficiază de o putere discreționară nelimitată</b> de a supune persoanele aflate în jurisdicția lor unor măsuri de supraveghere secretă.</p> <p>Curtea a afirmat că statele contractante nu pot adopta, în numele luptei împotriva spionajului și a terorismului, <b>orice măsură pe care o consideră adecvată</b>, ci, mai degrabă, indiferent de sistemul de supraveghere adoptat, acestea trebuie să asigure garanții adecvate și eficiente împotriva abuzurilor. Competențele de supraveghere secretă a cetățenilor sunt acceptabile numai în măsura strict necesară pentru protejarea instituțiilor democratice. O astfel de</p>	<p><b>Se acceptă</b> propunerea cu privire la constituirea grupului de lucru în scopul dezbaterii acestui proiect.</p>

ingerință trebuie susținută de motive pertinente și suficiente și trebuie să fie proporțională cu obiectivul sau obiectivele legitime urmărite.  
Subsidiar, potrivit principiilor dezvoltate în jurisprudența CtEDO cu privire la aplicabilitatea art.8 din Convenția europeană a drepturilor omului ce vizează dreptul la respectarea vieții private și de familie, a domiciliului și a corespondenței, legislația internă ar trebui să ofere garanții suficiente de precizie, eficiente și cuprinzătoare cu privire la **dispunerea și executarea măsurilor de supraveghere, precum și la posibilitățile de reparare a consecințelor acestora.**

Dreptul intern trebuie să ofere garanții adecvate pentru a împiedica orice utilizare a datelor cu caracter personal care ar putea fi incompatibilă cu garanțiile prevăzute art. 8 din Convenție. În virtutea celor expuse, considerăm că proiectul de lege nr.422 în redactarea prezentată spre avizare urmează a fi pus în dezbateri și revăzut în cadrul unui grup de lucru constituit în acest sens.

2. Trecând la o analiză punctuală a prevederilor proiectului de lege, formulăm următoarele obiecții.

Noțiunile utilizate în textul proiectului precum „pericol deosebit pentru securitatea statului, amenințări și riscuri la securitatea statului, acțiuni care periclitează securitatea statului, etc.” se prezintă a fi foarte vaste, vagi și lipsite de previzibilitate - cerință indispensabilă pentru respectarea standardului de calitate a legii.

Conform Strategiei securității naționale, aprobate prin Hotărârea Parlamentului nr. 153/15.07.2011, securitatea națională cuprinde acțiuni necesare în toate sectoarele de importanță majoră, precum: economie, sănătate, ecologie, educație, luptă împotriva corupției, mediu, migrațiune, etc.. Astfel, sfera de aplicare a proiectului de lege dat este foarte vastă și ușor interpretabilă, fapt care ar putea crea premise pentru abuzuri.

La fel, considerăm că din definiția „activitatea informativă externă” prevăzută la art.1 alin.(3) din proiect, necesită a fi excluse următoarele:  
- sintagma „sau ar putea constitui” — aceasta generează situații incerte/iluzorii care ar putea fi determinate doar de o presupunere fără existența unor circumstanțe obiective sau probe/materiale probatorii, substraturi factologice demonstrate și care stau la baza concluziei că o anumită persoană ar putea genera riscuri reale. Aceste prevederi creează un spațiu nelimitat de abuz în privința persoanelor în raport cu care ar putea să se creadă neîntemeiat că dețin potențiale riscuri în privința securității Republicii Moldova, fără existența unor bănueli rezonabile întemeiate; și - sintagma „precum și pentru obținerea informațiilor relevante pentru asigurarea

**Nu se acceptă.**

Versiunea redactată corespunde celor stabilite de către grupul de lucru de pe lângă Comisia parlamentară securitate națională, apărare și ordine publică.

<p><i>securității de stat sau pentru crearea condițiilor favorabile asigurării și promovării intereselor strategice și realizării cu succes a politicii de securitate națională a Republicii Moldova.</i> » - din motiv că prevederile acesteia sunt nedeterminate și neclare, iar în sensul art. 54 alin. (1) lit. a), b), f), h), i) din Legea nr. 100/2017 cu privire la actele normative, astfel de prevederi fie urmează a fi excluse, fie urmează a le fi atribuite denimiri clare.</p>	<p><b>Se acceptă.</b> Atricolul a fost completat corespunzător.</p>
<p>3. Titlul articolului 5 și alin. (1) al acestuia, după cuvântul „Drepturile” propunem completarea cu sintagma „și obligațiile”. Propunerea este înaintată în corespundere cu rigorile statuate la art. 46 alin. (2) lit. b) din Legea nr. 100/2017 cu privire la actele normative, care stabilește expres că actul normativ trebuie să prevadă nu doar drepturile subiecților (în cazul dat a ofițerilor de informații și securitate) dar și obligațiile acestora, care au fost propuse de a fi incluse în proiectul de lege, potrivit propunerii expuse în cadrul pct. 7 <i>infra</i> al prezentului aviz.</p> <p>4. La fel, cu privire la conținutul art. 5, considerăm oportun ca „Drepturile subiecților care efectuează activitatea informativă/contrainformativă”, să fie divizate în două articole separate, dintre care unul să prevadă „Drepturile și obligațiile subiecților care efectuează activitatea informativă” iar celălalt să prevadă în mod separat „Drepturile și obligațiile subiecților care efectuează activitatea contrainformativă”</p> <p>Această delimitare va asigura o claritate aferentă drepturilor și obligațiilor subiecților care efectuează aceste activități în mod separat pentru fiecare tip de activitate.</p> <p>O claritate în acest sens este deosebit de importantă din motiv că majoritatea activităților/măsurilor contrainformative necesită autorizarea judecătorului pe când cea informativă externă - nu. Prin urmare, în lipsa unei delimitări clare a drepturilor și obligațiilor subiecților în cadrul desfășurării activităților menționate, se creează o confuzie, existând riscul efectuării în temeiul drepturilor indicate - a unor acțiuni intruzive în lipsa unei autorizații corespunzătoare.</p>	<p><b>Se acceptă parțial.</b> Acest articol a fost revizuit și exclusă enumerarea concretă a drepturilor și obligațiilor ofițerilor de informații în domeniul activității contrainformative/informative externe, făcându-se trimitere la statutul juridic al ofițerului de informații reglementat de Legea nr. 170/2007 privind statutul ofițerului de informații și securitate precum și Legea privind Serviciul de Informații și Securitate al Republicii Moldova.</p>
<p>5. Având în vedere propunerea expusă <i>ante</i> cu privire la necesitatea reglementării a obligațiilor subiecților care efectuează activitatea informativă/contrainformativă, la articolul 5 din proiect după alin.(2), propunem completarea cu un alineat nou, cu următorul cuprins: „(3) în cadrul efectuării activității informative/contrainformative ofițerii de informații sunt obligați: a) să respecte drepturile și interesele legitime ale persoanei, să întreprindă, în limitele competenței, toate măsurile în vederea apărării drepturilor și libertăților omului, protecției tuturor formelor de proprietate ocrotite de lege</p>	<p><b>Nu se acceptă.</b> A se vedea argumentarea de mai sus.</p>

	<p>pentru asigurarea securității statului și a ordinii publice să asigure protecția vieții private în legătură cu prelucrarea datelor cu caracter personal, să asigure inviolabilitatea domiciliului, corespondenței și a regimului juridic al informațiilor cu accesibilitate limitată;</p> <p>b) să execute indicațiile legitime ale superiorilor sau ale procurorului;</p> <p>c) să informeze Procuratura, Instanța de judecată, Centrul Național pentru Protecția Datelor cu Caracter Personal cu privire la informațiile și faptele care sunt realizate cu încălcarea prezentei legi sau ale altor acte normative;</p> <p>e) să respecte proporționalitatea dintre scopul urmărit la realizarea activității informative/contrainformative și restrângerea drepturilor persoanelor vizate.”</p> <p>Normele de referință necesită a fi incluse în proiectul de lege având în vedere rigorile prevăzute de tehnica legislativă pentru proiecte de lege, în special care rezultă din prevederile art. 46 alin. (2) lit. b) din Legea nr. 100/2017 cu privire la actele normative, care stabilesc expres dispozițiile de conținut pe care trebuie să le conțină actul normativ.</p>
<p><b>Se acceptă.</b> Au fost excluse aliniatele respective.</p>	<p>6. La articolul 5, aliniatele (3) și (4) din proiect urmează a fi excluse, deoarece norme similare, dar mai extinse se regăsesc în art. 8 alin. (1) pct. 7) și pct. 9), pct. 11), pct. 20) din proiectul de Lege nr. 420 cu privire la Serviciul de Informații și Securitate al Republicii Moldova.</p>
<p><b>Se acceptă.</b> Articolul 6 a fost exclus.</p>	<p>7. La articolul 6 alin. (1) sintagma „sau verbal” urmează a fi exclusă. Norma vizată creează premise serioase pentru abuzuri sau evitarea responsabilității din partea ofițerilor de informații și securitate, în vederea declarării fictive cu privire la încheierea unor astfel de acorduri confidențiale.</p>
<p><b>Se acceptă.</b> Articolul 7 a fost exclus.</p>	<p>8. La articolul 7 alin. (2), după sintagma „comunicații electronice” se propune completarea cu sintagma „, în limita autorizăției”. Este de menționat că, activitatea informativă/contrainformativă nu presupune o activitate cu caracter permanent și nedeterminat, ci constituie o activitate specifică determinată și limitată de condițiile și termenele stabilite de lege.</p>
<p><b>Se acceptă.</b> Articolul 7 a fost exclus.</p>	<p>9. La articolul 7 alin. (2) pct. 3 din proiect, după textul „Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației” se propune completarea cu textul „și Centrul Național pentru Protecția Datelor cu Caracter Personal”.</p> <p>Propunerea rezultă din competențele funcționale atribuite Centrului Național pentru Protecția Datelor cu Caracter Personal prin Legea nr. 133/2011 privind protecția datelor cu caracter personal și art. 71 alin. (3) din Legea nr. 241/2007 privind comunicațiile electronice.</p> <p>Unul dintre obiectivele de bază prevăzute de proiectul de lege, este de a asigura proporționalitatea dintre scopul urmărit și restrângerea drepturilor fundamentale, în special dreptul la viața privată și protecția datelor cu caracter</p>

<p>personal, dar și asigurării unor mecanisme corespunzătoare de confidențialitate și de securitate în cazul realizării activității informative/contrainformative, opozabile acestor imperativități fiind inclusiv art. 4, art. 29 și art. 30 din Legea nr. 133/2011 privind protecția datelor cu caracter personal.</p>	<p><b>10.</b> La articolul 7 alin. (2) pct. 4), propunem ca cuvântul „toate” să fie exclus, iar după sintagma „comunicații electronice”, să fie completat cu cuvântul „necesare”. Or, redacția normei generează riscul de a solicita în exces informații, inclusiv atunci când acestea nu sunt justificate. Finalmente, considerăm oportun ca art.7 ce prevede „Asistența acordată la efectuarea activității informative/contrainformative” să fie divizat în două articole separate și independente, în care unul să prevadă „Asistența acordată la efectuarea activității informative” iar celălalt să prevadă în mod separat „Asistența acordată la efectuarea activității contrainformative”. Motivarea unei astfel de propuneri se prezintă a fi similară celei prezentate în raport cu art.5 din proiect, motiv pentru care facem trimitere la pct.4 al avizului.</p>	<p><b>Se acceptă.</b> Articolul 7 a fost exclus.</p>
<p>personal, dar și asigurării unor mecanisme corespunzătoare de confidențialitate și de securitate în cazul realizării activității informative/contrainformative, opozabile acestor imperativități fiind inclusiv art. 4, art. 29 și art. 30 din Legea nr. 133/2011 privind protecția datelor cu caracter personal.</p>	<p><b>11.</b> La articolul 9 alin. (1) propunem completarea la final cu textul: „și care va conține: data inițierii, ofițerii de informație și securitate desemnați; persoanele fizice și juridice vizate de activitatea informativă/contrainformativă; autorizațiile măsurilor informative/contrainformative; informațiile și documentele colectate în cadrul dosarului și temeiul legal; perioada de stocare, secretizare, resursele informaționale cu includerea tipului operațiunilor realizate: vizualizare, extragere; oricare alte date relevante. Dosarul special se consideră a fi inițiat din momentul efectuării măsurilor informative/contrainformative.”.</p> <p>Completarea în cauză este necesară pentru a determina clar momentul pomirii/inițierii dosarului special, de începere a curgerii termenelor dar și a respectării cerințelor prevăzute de proiectul de lege.</p>	<p><b>Se acceptă.</b> Articolul a fost completat cu prevederi ce vizează modul de inițierea dosarului, de înregistrare, de gestionare.</p>
<p>personal, dar și asigurării unor mecanisme corespunzătoare de confidențialitate și de securitate în cazul realizării activității informative/contrainformative, opozabile acestor imperativități fiind inclusiv art. 4, art. 29 și art. 30 din Legea nr. 133/2011 privind protecția datelor cu caracter personal.</p>	<p><b>12.</b> La articolul 10 după cuvintele „clasarea dosarului special,” propunem completarea cu cuvintele „ persoanele vizate se informează cu privire la prelucrarea acestor date, după care”.</p> <p>Considerăm că redacția actuală a proiectului nu asigură un echilibru asupra drepturilor restrânse în legătură cu activitatea informativă/contrainformativă. Este de menționat că, în cazul în care statul își creează mecanisme de eschivare de la informarea persoanei cu privire la prelucrarea informațiilor care s-au adevărit a fi irelevante, prin distrugerea acestora, creează de cealaltă parte context pentru imposibilitatea repunerii persoanelor în drepturi.</p> <p>Redacția proiectului poate genera precedente pentru ștergerea tuturor probelor în ceea ce privește eventualele colectări excesive și ilegale de date și</p>	<p><b>Se acceptă parțial.</b> Articolul 10 a fost expus într-o nouă redacție care stabilește doar locul și termenul de păstrare a dosarului special clasat, după caz, modalitatea de preluarea acestui termen sau desecretizarea. În ceea ce privește informarea persoanei despre măsurile realizate în privința sa, astfel de reglementări se regăsesc la art. 23 din proiectul legii.</p>

oferă posibilitatea Serviciului de a evita orice răspundere, or, norma vizată nu prevede care sunt criteriile după care informația va fi determinată ca fiind irelevantă și cine va decide în acest caz.

Mai mult, prevederile în cauză nu prevăd distincția dintre cazurile de colectare excesivă/ilegală și cazurile când informația s-a dovedit a fi irelevantă. În acest context, se evită orice mecanism de control și de verificare cu privire la faptul dacă datele sunt irelevante sau acumulate cu încălcarea legii.

Amintim la acest capitol despre statuările Curții Constituționale din Hotărârea nr.31 din 23 septembrie 2021, în care reiterând rațiunile CtEDO a indicat că printre garanțiile minime necesare pentru a se evita abuzul de putere se numără măsurile care trebuie luate pentru a comunica informațiile părților (*Big Brother Watch and Others v. Regatul Unit*, 25 mai 2021, § 335). Așadar, legea trebuie, în special, să detalieze măsurile de precauție care trebuie luate pentru a comunica în mod intact și complet înregistrările efectuate, în scopul unui eventual control al judecătorului și al apărării (*Huwig v. Franța*, 24 aprilie 1990, § 34; *Valenzuela Contreras v. Spania*, 30 iulie 1998, § 46; *Prado Bugallo v. Spania*, 18 februarie 2003, § 30; *Karabeyoglu v. Turcia*, 7 iunie 2016, § 88).

13. Articolul 11 conține un volum excesiv de atribuții acordate Serviciului și considerăm că urmează a fi exclus, pe motiv că contravine art. 3 alin. (1) lit. c) și f) din Legea nr. 100/2017 cu privire la actele normative.

În context, reținem că este contrar prevederilor legale ca efectul regulator al actului legislativ superior să fie detașat și echivalat cu puterea actelor normative departamentale ale Serviciului, care vor fi emise unilateral, fără o consultare publică, fără a se publica în Monitorul Oficial și fără a putea face cunoștință cu conținutul acestora.

Cel puțin, prevederile prezentului articol ar putea fi modificate, prin includerea la sfârșitul frazei a sintagmei „ , regulament, instrucțiune, coordonate cu Procuratura Generală”.

#### **Nu se acceptă.**

În redacția actuală articolul 11 nu conține un volum excesiv de atribuții ci reglementează faptul că toate activitățile Serviciului referitor la metodele efectuării măsurilor conținutive sau informative externe, procedurile interne de autorizare, regulile de întocmire a proceselor-verbale, modul de înregistrare a dosarelor speciale ș.a. se vor reglementa prin act normativ departamental. Tot în acest context, menționăm că reglementarea unor aspecte ce țin de exemplu: de tactica și metodele de activitate constituie informații atribuite la secretul de stat în conformitate cu prevederile Legii nr. 245/2008 cu privire la secretul de stat, respectiv publicarea acestor acte departamentale în Monitorul Oficial este ilegală.

Or, Serviciul are putere discreționară ca la

	<p>nivel departamental să-și organizeze propria activitate prin aprobarea unor acte normative departamentale ținând cont de actele normative ierarhic superioare. Corepunzător, actele interne nu vor depăși prevederile legale și nu vor stabili atribuții noi SIS -ului</p>
<p><b>14.</b> În Capitolul II secțiunea I din proiect, este reglementată procedura de autorizare a măsurilor contrainformative. Potrivit art. 12 alin.(1) din proiect: „(1) În cadrul activității contrainformative pot fi efectuate următoarele măsuri contrainformative: <b>1) cu autorizarea directorului Serviciului sau directorului adjunct special împuternicit:</b> <b>a) accesul la informația financiară sau monitorizarea tranzacțiilor financiare;</b> b) 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; c) urmărirea vizuală și/sau documentarea cu ajutorul metodelor și mijloacelor tehnice, precum și localizarea sau urmărirea prin sistemul de poziționare globală ori prin alte mijloace tehnice; d) controlul transmiterii banilor sau altor valori materiale sau nemateriale, precum și prestării serviciilor; e) investigația sub acoperire; f) livrarea supravegheată; g) colectarea mostrelor pentru cercetarea comparativă; h) cercetarea obiectelor și actelor; i) achiziția de control; j) cercetarea încăperilor, clădirilor, porțiunilor de teren sau a mijloacelor de transport, în cazul în care aceasta nu constituie o violare a domiciliului; k) experimentul operativ;” Se atestă astfel că, măsurile denumite în proiect „contrainformative” reprezintă potrivit Codul de procedură penală (art.1322 CPP), măsuri speciale de investigație. Spre deosebire de reglementările proiectului de lege supus avizării, în procesul penal, potrivit Codului de procedură penală, măsurile privind <i>accesul la informația financiară sau monitorizarea tranzacțiilor financiare; și documentarea cu ajutorul metodelor și mijloacelor tehnice, precum și</i></p>	<p><b>Se acceptă.</b> Acest articol a fost revizuit și expus într-o nouă redacție. Astfel, cu autorizarea directorului Serviciului sau directorului adjunct special împuternicit urmează să fie efectuată doar măsura contrainformativă - identificarea abonatului sau utilizatorului unei rețele de comunicații electronice sau a unui serviciu al societății informaționale. Referitor la celelalte măsuri, numărul de măsuri contrainformative a fost redus și urmează a fi realizate doar cu autorizarea judecătorului (mandat judecătoresc). În consecință, se garantează că restrângerea drepturilor și libertăților fundamentale ale omului, va fi efectuată doar în cadrul unui control jurisdicțional, de către un judecător și respectarea principiul echilibrului instituțional „<i>checks and balances</i>”.</p>

localizarea sau urmărirea prin sistemul de poziționare globală ori prin alte mijloace tehnice - se efectuează cu autorizarea judecătorului de instrucție. Totodată, măsurile privind 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; urmărirea vizuală; controlul transmiterii banilor sau altor valori materiale sau nemateriale, precum și prestării serviciilor; investigația sub acoperire; livrarea supravegheată; și achiziția de control — se efectuează cu autorizarea procurorului.

În acest registru, reținem statuările Comisiei de la Veneția din Avizul comun pe marginea proiectului de lege nr. 281 pentru modificarea și completarea legislației moldovenești cu privire la așa-numitul „mandat de securitate” adoptat de la cea de 110-a sesiune plenară din 10-11 martie 2017 (în continuare Avizul Comisiei de la Veneția din 10-11 martie 2017), în care Comisia a indicat următoarele:

„37. În Avizul din 2014, Comisia de la Veneția a considerat drept „**explicitabil**” faptul că Republica Moldova „*dorește să asigure un mecanism de investigații de securitate în afara cadrului anchetei penale*” (alin. 25). În același timp, **Comisia a subliniat faptul că introducerea mandatului de securitate comportă riscul subminării garanțiilor existente aplicabile investigării infracțiunilor, creând riscul ca garanțiile mai slabe care însoțesc investigațiile de securitate să poată fi utilizate pentru a ocoli garanțiile mai puternice pentru investigațiile penale obișnuite** (alin. 26).”

„42. Rămân în continuare preocupările cu privire la Articolul 7' (2) din proiectul de lege, care permite Serviciului accesul la toate tranzacțiile financiare și informațiile financiare, **în afara investigației penale**, tară un mandat de securitate și, prin urmare, **în lipsa oricărui control extern**. S-ar putea argumenta chiar că cerințele referitoare la transferul de date creează posibilitatea pentru supravegherea **în masă**, de fapt, chiar devine generalizată o astfel de supraveghere în cazul în care criteriile limitative pentru a permite accesul la aceste date sînt stabilite la nivel jos, iar datele personale ale multor persoane care nu sînt suspectate sînt, de fapt, accesate în acest context. Prevederea pare problematică și ar trebui revizuită avînd în vedere cerințele de proporționalitate prevăzute la Articolul 8 din CEDO (a se vedea Avizul din 2014, alin. 35 și recomandarea (b)). Opinem asupra pertinentei statuărilor Comisiei, și considerăm inacceptabilă modalitatea de autorizarea a măsurilor „contrainformative” de către directorului Serviciului sau directorului adjunct special împuternicit reglementată la 12 alin.(1) lit.a) -k) din proiect.

*Ab initio*, lipsa unor garanții suficiente precum și ignorarea instituirii unor garanții mai înalte chiar și decât cele prevăzute de Codul de procedură penală (având în vedere că sunt efectuate în afara unui proces penal) este inadmisibilă și creează premise pentru încălcarea art.8 CEDO.

Mai mult, unica reglementare privind aprecierea **necesității stricte** de efectuare a măsurilor 12 alin.(1) pct.l) lit.a) - k) din proiect, se regăsește în art.14 alin.(4) potrivit căruia, „(4) *Directorul Serviciului, directorul adjuncț special împuternicit, vor refuza autorizarea măsurii contrainformative dacă constată că demersul înaintat este neîntemeiat și neargumentat.*

Astfel, Directorul Serviciului, directorul adjuncț special împuternicit urmează să aprecieze temeinicia demersului privind autorizarea măsurilor contrainformative în lipsa unor criterii/condiții expres definite pentru autorizarea acestora.

Mai mult decât atât, considerăm în mod justificat că efectuarea testului de proporționalitate a scopului acțiunii/măsurii în raport cu restrângerea drepturilor și libertăților fundamentale ale omului, poate fi efectuată doar în cadrul unui control jurisdicțional, de către un judecător, fiind o prerogativă exclusivă a puterii judecătorești. Chiar și așa însă, implicarea judecătorului de instrucție, urmează a nu fi una formală.

Sub acest aspect însă, mai reținem și statuările Comisiei de la Veneția din 10-11 martie 2017, în special pct.41 din Aviz, care a invocat că:

*41. [...] efectul și valoarea practică a implicării instanțelor, în astfel de chestiuni, depind foarte mult de natura condițiilor juridice care urmează să fie verificate. Dacă se mențin niște criterii limitative atît de joase și nu este prevăzut niciun test eficient de proporționalitate, impactul real al implicării instanței pare a fi destul de dubios (a se vedea alin. 32 din Avizul din 2014, în care se face referire la problema proporționalității, inclusiv critica dură formulată în acest sens în hotărîrea CEDO în cazul lordachi).7 \* Subsecvent, în pct.25 din Aviz, Comisia de la Veneția, a mai statuat că: „Fără îndoială, agenția de securitate ar trebui să poată colecta și analiza informații referitoare la fenomenele periculoase pentru societate din surse deschise în mod relativ liber. Cu toate acestea, atunci cînd agenția dorește să meargă mai departe și stochează informații cu privire la persoanele fizice sau inițiază o anchetă împotriva unei persoane fizice cu ajutorul unei măsurii de constrîngere prin care se încalcă drepturile omului (supraveghere, etc.), în conformitate cu practica stabilită a CEDO9, trebuie să fie îndeplinite niște standarde mult mai stricte.”*

In aceste condiții, considerăm imperios necesar ca măsurile contrainformative

care aduc atingere/ingerințe dreptului la viața privată, să fie evaluate de către un judecător fiind asigurate standarde și garanții mult mai înalte pentru autorizarea acestora.

Considerentele expuse vor asigura respectarea principiului echilibrului instituțional, cunoscut astăzi sub denumirea „*checks and balances*” care stă la baza democrației și presupune echilibrul puterilor și controlul lor reciproc, astfel încât puterile statale să aibă aproximativ aceeași pondere, adică să fie echilibrate, pentru a se putea limita reciproc, evitând astfel ca puterea statală să fie folosită în mod abuziv.

Acest sistem [...] reprezintă o condiție *sine qua non* a democrației moderne, împiedicând omnipotența legislativului, pe cea a executivului sau a judiciarului.

Prin urmare, propunem autorizarea măsurilor contrainformative prevăzute la art.12 alin.(l), cu excepția celor de la art.12 alin.(l) pct.g), h), j) și k), de către judecătorul de instrucție la demersul procurorului desemnat din cadrul Procuraturii Generale.

Măsurilor contrainformative prevăzute la art.12 alin.(l) pct.g), h), j) și k), ar putea fi autorizate de Directorul Serviciului sau adjunctul special împuternicit, din motiv că sunt mai puțin intruzive în drepturile persoanei, drepturi protejate de art.8 CEDO.

În această ordine de idei, pentru operarea modificărilor conceptuale propuse, urmează a fi revizuit și ajustat textul proiectului în special al art.12, 15, 16, 18, 19, 23, 24, 25, 36, 39, 49, ș.a., enumerarea efectuată nefiind una exhaustivă.

În acest context, art.art. 15, 18, 19 alin.(l) și (2), art.23 alin.(4), (5), (6), și art.39 alin.(4) reieșind din propunerile conceptuale iterate, textul „Directorul Serviciului sau directorul adjunct special împuternicit”, „directorului Serviciului”, „Serviciului”, urmează a fi substitute la forma gramaticală corespunzătoare cu textul „procurorul desemnat din cadrul Procuraturii Generale” sau după caz, norma urmează a fi completă cu acest text.

La art.24 alin.(3), art.36 alin.(4) textul „ordonanța directorului Serviciului sau directorului adjunct special împuternicit” urmează a fi substitute cu textul „mandatul judecătoresc”.

La art.25 alin.(3), art.36 alin.(4) textul „ordonanța directorului Serviciului sau directorului adjunct special împuternicit” și textul „directorului Serviciului sau directorului adjunct special împuternicit” urmează a fi substitute cu textul „mandatul judecătoresc” și respectiv cu textul „judecătorului de instrucție”.

La reconceptualizarea proiectului de lege potrivit propunerii respective, și

### **Se acceptă parțial.**

Toate măsurile contrainformative a căror desfășurare este necesară mandatul judecătoresc se vor autoriza la demersul scris al directorului Serviciului sau directorul adjunct special împuternicit. A nu se confunda activitatea specială de investigații unde este necesar demersul procurorului cu activitatea contrainformativă care se detașează de la prevederile Codului de procedură penală, care prevede un alt mecanism de autorizare.

### **Se acceptă.**

Toate articolele menționate au fost revizuite.

<p>anume implicarea judecătorului la autorizarea măsurilor contrainformative la demersul procurorului, întru evitarea unei inadvertențe legislative, autorul proiectului urmează să revizuiască întreg proiectul de lege fără a se limita la articolele menționate <i>supra</i>.</p>	<p>15. În acord cu propunerea iterată <i>supra</i> în pct.14 al avizului, art.14 ce se referă la „Procedura autorizării măsurilor contrainformative de către directorul Serviciului sau directorului adjunct special împuternicit”, urmează să se refere doar la măsurile contrainformative prevăzute la art.12 alin.(l) pct.g), h), j) și k).</p>	<p><b>Se acceptă.</b>          Articolul 14 a fost expus într-o nouă redacție.</p>
<p>16. Cu privire la temeiurile pentru efectuarea măsurilor contrainformative prevăzute de art.13 din proiect, reiterăm criticile Comisiei de la Veneția din 10-11 martie 2017 statuate în pct. 24 al Avizului potrivit căruia:          „24. O agenție de securitate deține deseori mandatul de a preveni amenințările la adresa securității statului, de ex., atacurile teroriste. Astfel, o <b>agenție de securitate este, în mod inevitabil, tentată să investigheze ceea ce poate fi numit „pre-infracțiune”</b>. Cu toate acestea, într-o democrație bazată pe statul de drept, dreptul penal are scopul nu doar de a proteja societatea, ci și de a impune limite fundamentale privind puterea coercitivă a statului. Infracțiunile trebuie să fie formulate în mod clar și restrictiv, stabilind, în termeni obiectivi și generali, comportamentul interzis. Comportamentul interzis ar trebui să fie astfel, în mod rezonabil, previzibil. De asemenea, nu este suficient, într-un stat democratic guvernat de statul de drept, ca organele de aplicare a legii sau de securitate să considere cu adevărat că o anumită persoană este angajată într-un comportament interzis. <b>Trebuie să existe indicii concrete înainte de a putea iniția investigația vreunei infracțiuni sau, cel puțin, o activitate infracțională</b>. Aceste indicii concrete, împreună cu alte informații, trebuie să atingă un anumit standard, o <b>suspiciune rezonabilă, care trebuie să fie testată de către o instanță de judecată înainte de a putea dispune o măsură sub acoperire care încalcă drepturile omului</b>.</p>	<p><b>Se acceptă.</b>          Articolul respectiv a fost revizuit, unele temeiuiri au fost excluse, altele detaliate.</p>	<p><b>Se acceptă.</b>          Mandatul judecătoresc urmează să fie eliberat de către un judecător din cadrul Curții de Apel Chișinău <u>special împuternicit</u>. Totodată, la art. 61 a fost stabilit expres că președinții Curții de Apel Chișinău și Curții Supreme de Justiție vor stabili numărul concret de judecător ce vor fi abilitați cu competența de a elibera</p>
<p>17. La art.15 alin.(2) și respectiv alin.(16) pentru asigurarea obiectivității și excluderii riscurilor de influențare a judecătorilor care vor examina demersurile privind autorizarea măsurilor contrainformative și respectiv a recursurilor împotriva încheierilor de respingere a demersului privind eliberarea mandatului judecătoresc, precum și încheierilor privind declararea ca fiind ilegale a măsurii și dispunerea distrugerii informațiilor acumulate, considerăm just ca demersurile să fie repartizate judecătorilor sau, după caz, completului de judecată în mod aleatoriu, prin intermediul programului informațional automatizat de gestionare a dosarelor.</p>		<p><b>Se acceptă.</b>          Mandatul judecătoresc urmează să fie eliberat de către un judecător din cadrul Curții de Apel Chișinău <u>special împuternicit</u>. Totodată, la art. 61 a fost stabilit expres că președinții Curții de Apel Chișinău și Curții Supreme de Justiție vor stabili numărul concret de judecător ce vor fi abilitați cu competența de a elibera</p>

	<p>mandate judiciare și de examinare a recursurilor, vor desemna judecătorii respectivi și vor organiza procesul de repartizare aleatorii a demersurilor/recursurilor Serviciului.</p> <p><b>Nu se acceptă.</b></p> <p>Articolul respectiv a fost expusă într-o nouă redacție, și prevede că „La declararea măsurilor ca fiind ilegale, măsura se sistază.”. La articolul 23 al proiectului se reglementează modul de informare a persoanei despre măsurile contrainformative înfăptuite în privința sa.</p> <p><b>Se acceptă.</b></p> <p>Articolul 16 a fost revizuit integral și excluse „faptele ce prezintă pericol deosebit pentru securitatea statului”.</p>	<p>18. La art. 15 alin. (14) după cuvintele „judecătorul dispune” se completează cu sintagma „cu informarea în prealabil a persoanelor vizate de măsurile ilegale și punerea la dispoziție a unei copii a informațiilor”. Completările în cauză sunt necesare pentru restabilirea drepturilor persoanelor vizate și după caz realizarea acțiunii în regres prin obținerea despăgubirilor în cazul activităților ilegale.</p> <p>19. Prevederile articolului 16 „Condițiile speciale de efectuare a măsurilor contrainformative autorizate prin eliberarea mandatului judecătoresc” - urmează a fi revizuit <i>in integrum</i> deoarece faptele invocate ca fiind <b>pericol deosebit pentru securitatea statului</b> constituie în esență fapte infracționale prevăzute de Codul penal al Republicii Moldova, depistarea, investigarea și cercetarea cărora este prevăzută de Codul de procedură penală și Legea nr.59/2012 privind activitatea specială de investigații. Totodată, urmează a fi menționat că, așa cum raționalizează CtEDO, măsurile care limitează drepturile persoanelor trebuie să fie proporționale și adecvate gravității faptelor și valorilor sociale protejate de lege. Anume din acest considerent, măsurile intruzive realizate de către organele statului și care limitează esențial drepturile fundamentale ale persoanei, urmează să fie autorizate de judecător.</p> <p>Procedura de dispunere și efectuare a măsurilor repetă obiectul de reglementare a Legii nr. 59/2012 privind activitatea specială de investigație, dar și scopul legii penale prevăzut la art. 2 alin. (1) din Codul penal, care stabilește expres că Legea penală apără, împotriva infracțiunilor, persoana, drepturile și libertățile acesteia, proprietatea, mediul înconjurător, orânduirea constituțională, suveranitatea, independența și integritatea teritorială a Republicii Moldova, pacea și securitatea omenirii, precum și întreaga ordine de drept, aspecte reflectate expres în mai multe prevederi ale Codului penal, de exemplu:</p> <ul style="list-style-type: none"> <li>- Art. 337 Trădarea de patrie;</li> <li>- Art. 338 Spionajul;</li> <li>- Art. 339 Uzurparea puterii de stat;</li> <li>- Art. 340 Rebeliunea armată;</li> </ul>
--	--	---

<p>- Art. 342 Atențarea la viața Președintelui Republicii Moldova, a Președintelui Parlamentului sau a Prim-ministrului;</p> <p>- Art. 343 Diversiunea;</p> <p>- Art. 344 Divulgarea secretului de stat;</p> <p>- Art. 351 Uzurparea de calități oficiale;</p>	<p><b>Nu se acceptă.</b></p> <p>Versiunea redactată corepsunde celor stabilite de către grupul de lucru de pe lângă Comisia securitate națională, apărare și ordine publică.</p>
<p>- Art. 342 Atențarea la viața Președintelui Republicii Moldova, a Președintelui Parlamentului sau a Prim-ministrului;</p> <p>- Art. 343 Diversiunea;</p> <p>- Art. 344 Divulgarea secretului de stat;</p> <p>- Art. 351 Uzurparea de calități oficiale;</p>	<p><b>20.</b> Cu privire la termenul pentru care se autorizează măsurile contrainformative prevăzute de art. 17 din proiectul legii, menționăm următoarele.</p> <p>Termenul de autorizare pentru 90 zile a măsurilor contrainformative prevăzute la art. 12 alin.(1), (2), cu posibilitatea de prelungire pe perioade succesive îl considerăm excesiv de mare, devind astfel de la standardele instituite chiar și pentru măsurile special de investigație prevăzute de Codul de procedură penală (art.1324) alin.(7) CPP.</p> <p>Și comisia de la Veneția în Avizul său din 10-11 martie 2017 a apreciat limitarea duratei de autorizare a măsurilor la termenul de 30 zile.</p> <p>Astfel, în pct.43 din Aviz, Comisia a reținut următoarele:</p> <p><i>„Durata termenului minim inițial de autorizare a măsurilor speciale a fost limitată la 30 de zile, în comparație cu cele 6 luni propuse anterior, iar preocupările privind posibilitatea unor prelungiri nedefinite ale autorizării au fost abordate stabilind un termen de cel mult doi ani cumulativ (noul Art. 11(9)). Ambele prevederi reprezintă evoluții pozitive.</i></p> <p>În context, reieșind din reglementările Codului de procedură penală, propunem posibilitatea autorizării măsurilor contrainformative pentru o perioadă de 30 de zile cu posibilitatea de a fi prelungită întemeiat pentru aceeași perioadă, până la termenul maxim 6 luni. Respectiv, fiecare prelungire a duratei măsurii nu poate depăși 30 de zile.</p> <p>Astfel, la art. 17 alin. (1) și (2) cifrele „90” urmează să fie substituie cu cifrele „30”.</p> <p>La art. 17 alin. (3) cuvintele „ , cu posibilitatea de prelungire pe perioade succesive precum și pe perioade care nu se succed, de până la 6 luni” se exclud. Aceste prevederi le apreciem ca fiind abuzive și generează posibilitatea nejustificată de a aplica repetat prelungirea termenului, or, includerea unor mecanisme repetate de prelungire a termenului la infinit, încalcă grav dreptul la viața privată prin asigurarea urmării continue a persoanelor.</p> <p>La art. 17 alin. (5) textul „2 ani” se substituie cu cuvintele „ 6 luni”. Termenul de 2 ani este unul și mai excesiv și limitează nejustificat pe o perioadă extrem de mare drepturile și libertățile fundamentale.</p> <p>Menționăm că, termenul stabilit în cadrul activităților contrainformative/informative nu poate depăși termenul stabili în cadrul</p>

<p>procesului penal de Legea nr. 59/2012 privind activitatea specială de investigație.</p> <p><b>21.</b> Cu privire la art.23 din proiect urmează a fi menționate următoarele. Actuala redacție a proiectului de lege, art.23 alin.(3) prevede faptul că informarea persoanei nu va avea loc dacă „<i>există motive întemeiate de a considera că acest fapt ar putea constitui un risc sporit pentru viața sau sănătatea oamenilor, ar periclita o altă investigație desfășurată, ar dăuna securității statului sau ar aduce prejudicii scopului pentru care au fost efectuate măsurile contrainformative</i>”.</p> <p>Această formulare lasă spațiu de interpretare cu privire la „<i>motivele întemeiate</i>”. Alai mult, în cazul în care își consideră drepturile lezate, subiecții care au fost vizați în cadrul măsurilor contrainformative nu pot contesta procedura de efectuare a acestora atâta timp cât nu vor cunoaște despre aplicarea măsurilor în privința lor, lucru valabil mai ales pentru măsurile contrainformative autorizate de către conducerea Serviciului.</p> <p>În cauza <i>Klass c. Germaniei</i>, Curtea aceasta a accentuat și faptul că, acolo unde urmărirea secretă a instituțiilor statului rămâne necunoscută persoanelor supuse controlului, circumstanța conduce la ideea existenței inevitabile a unei asemenea urmăriri, și aplicarea extensivă a articolului 8 poate fi redusă la zero. În această situație există probabilitatea ca un individ să fie tratat într-o manieră contrară articolului 8, sau să fie privat de dreptul conferit de acest articol, tară să fie în cunoștință de cauză și prin urmare să fie în imposibilitate de a obține o remediere atât la nivel național așa și în fața instituțiilor Convenției.</p> <p>Prin urmare, în cazul în care un stat instituie o măsură de supraveghere secretă, a cărei existență nu este cunoscută de persoanele care fac obiectul controlului, având drept consecință faptul că respectiva supraveghere nu poate fi contestată, este posibil ca anumite persoane să fie private de drepturile pe care le au în temeiul art. 8 CEDO.</p> <p>Acest lucru este valabil în special într-un context în care progresele tehnologice au permis evoluția metodelor de supraveghere și în care statul poate avea interese legitime să apere ordinea, să prevină faptele penale sau să combată actele de terorism.</p> <p>Simpla existență a unei legislații care permite unui sistem de monitorizare secretă a comunicațiilor implică un risc de supraveghere pentru toate persoanele cărora li se poate aplica legislația.</p> <p>În acest context, reținem statuările Comisiei de la Veneția din 10-11 martie 2017 potrivit cărora ultima a statuat următoarele:</p> <p>49. Totuși, condiția care urmează a fi îndeplinită este că există „motive</p>	<p><b>Nu se acceptă.</b></p> <p>Considerăm că sintagma „motive întemeiate” nu lasă careva spațiu de interpretare deoarece autorul proiectului a menționat „<i>motive întemeiate de a considera că acest fapt ar putea constitui un risc sporit pentru viața sau sănătatea oamenilor, ar periclita o altă investigație desfășurată, ar dăuna securității statului sau ar aduce prejudicii scopului pentru care au fost efectuate măsurile contrainformative</i>”. Respectiv, sunt enumerate patru motive întemeiate în baza cărora poate fi dispusă neinformarea. Mai mult ca atât, neinformarea persoanei nu se va face la discreția Serviciului. Temeinicia motivelor va fi apreciată de către un judecător abilitat cu dreptul de a elibera mandat judecătoresc. Prin urmare, aceste motive vor fi supuse controlului din partea judecătorului care va decide asupra ne/informării persoanei. Tot în acest sens, în cazul în s-a dispus neinformarea iar temeiurile (motivele întemeiate) au dispărut persoana urmează a fi informată despre măsurile contrainformative realizate în privința sa.</p>
---	---

<p><b>Avocatul Poporului</b> <b>OMBUDSMAN</b> 04-03/11-403 din 20 februarie 2023</p>	<p>întemeiate” de a considera că înștiințarea ar periclita, de exemplu, o altă investigație destășurată (noul Articol 72(3)). Acest lucru pare a reprezenta un <b>criteriu restrictiv foarte jos</b>, deoarece, după cum este evidențiat în Avizul din 2014 (alin. 46), lipsa de înștiințare poate însemna că încălcarea drepturilor nu va fi descoperită niciodată. <b>Un astfel de efect ar veni ca o încălcare a Articolului 8 din CEDO.</b> În acest context, Comisia a propus următoarele sugestii, care ar oferi garanții:</p> <ul style="list-style-type: none"> <li>- Includerea, așa cum sugerează recomandarea (h) din Avizul din 2014, a unei proceduri prin care un avocat care reprezintă interesele persoanei afectate poate contesta aceste decizii.</li> <li>- Demersul pentru amânarea înștiințării ar putea fi examinat (eventual) de către un alt judecător decât cel care a autorizat mandatul de securitate prima dată. Acest lucru ar permite o nouă perspectivă asupra faptelor.</li> </ul> <p>O altă opțiune ar fi atribuirea sarcinii de a stabili dacă înștiințarea poate avea loc sau nu unui organism independent de supraveghere, în cazul în care ar fi creat un astfel de organism (a se vedea Avizul din 2014, alin. 79).</p>	<p><b>Se acceptă.</b> Au fost excluse alineatele care prevăd aceste sintagme.</p>
<p><b>Se acceptă.</b></p>	<p>1. Sintagmele „probabilitate sporită” și „probabilitate înaltă” ar trebui de clarificat/revizuit pentru a nu admite limitarea abuzivă a drepturilor și libertăților omului (art. 5 alin. (2), art. 15 alin. (7)).</p>	<p><b>Se acceptă.</b> Articolul 6 a fost exclus.</p>
<p>2. Prevederile cu privire la persoanele care colaborează în secret cu Serviciul ar trebui revizuite, deoarece sunt tratate diferit persoanele care colaborează cu Serviciul, în funcție de forma încheierii acordului în scris sau verbal. Tratarea diferită se observă și în cazul sprijinului acordat Serviciului ce poate fi cu titlu gratuit sau remunerat. Or, orice persoană care colaborează cu Serviciul trebuie să beneficieze de aceleași garanții (art.6).</p>	<p>3. Nu este clar cum se va face distincția între dosarele speciale administrate în condițiile proiectului și dosarele speciale administrate în temeiul art. 21 din Legea nr. 59 din 29.03.2012 privind activitatea specială de investigații. Considerăm că astfel de norme concurente ar trebui clarificate în scopul evitării abuzurilor (art. 9).</p>	<p><b>Nu se acceptă.</b> Dosarele speciale inițiate în temeiul prevederilor art. 9 al prezentului proiect se inițiază în cadrul activității contrainformative/informative externe, activitate care este distinctă de activitatea specială de investigații (subiecți, temeuri, procedură de autorizare, diferite ș.a.).</p>
<p>4. O mare parte din măsurile contrainformative constituie, în esență, măsuri speciale de investigații, în condițiile descrise la art. 18 din Legea nr. 59 din 29.03.2012. Se vor crea mecanisme paralele de autorizare a unor măsuri. Aceasta ar putea crea anumite confuzii și diminuarea din previzibilitatea legii, fapt care ar putea conduce la încălcarea drepturilor omului (art.12).</p>	<p>5. Normele care prevăd efectuarea măsurilor contrainformative cu autorizarea</p>	<p><b>Se acceptă.</b> Articolul 12 a fost revizuit, astfel încât a fost modificat mecanismul de autorizare.</p>
<p><b>Se acceptă.</b></p>	<p></p>	<p><b>Se acceptă.</b></p>

<p>Articolul 12 a fost revizuit, în redacția actuală directorul Serviciului sau directorul adjunct special împuternicit autorizează doar măsura identificarea abonatului sau utilizatorului unei rețele de comunicații electronice sau a unui serviciu al societății informaționale.</p>	<p><b>Nu se acceptă.</b>          Autorul proiectului nu poate stabili exhaustiv care sunt acele consecințe nefavorabile deoarece acestea pot să difere de la persoană la persoană. Există riscul nereglementării unor situații care ar putea fi catalogate ca consecințe nefavorabile și la apariția lor să nu poată fi dispuse măsurile contrainformative pentru a proteja persoana.</p>
<p>directorului Serviciului sau directorul adjunct reprezintă riscuri majore de abuz și ar trebui înlocuite cu autorizarea exclusivă a instanței de judecată pentru a exclude orice arbitriu din partea conducătorilor Serviciului, persoane oficiale exponente ale unui interes politic (art.12 lit.c), 14) (urmărirea vizuală și/sau documentarea cu ajutorul metodelor și mijloacelor tehnice, precum și localizarea sau urmărirea prin sistemul de poziționare globală ori prin alte mijloace tehnice).</p>	<p>6. Sugerăm concretizarea expresiei „consecințe nefavorabile” care este una neclară (art. 16 alin. (3)).</p>
<p>7. Considerăm că ar trebui de evitat utilizarea unor termeni, precum „în cel mai scurt timp posibil” și „termen cât mai restrâns posibil”. Sugerăm redactarea sau precizarea unui termen mai concret (art.25, alin.(3), art.36 alin.(5)).</p>	<p><b>Nu se acceptă.</b>          Referitor la art. 25 alin. (3), menționăm că inițial a fost stabilit un termen concret de 24 de ore, care ulterior a fost exclus. Aceasta s-a făcut în scopul de a nu pune furnizorul de comunicații electronice în imposibilitatea de a acționa.          Referitor la art. 36 alin. (5) evidențiem că demontarea aparatului nu poate fi restrânsă de careva termeni, existând riscul punerii în pericol a ofițerilor de informații care au desfășurat măsura.</p>
<p>8. Considerăm că prelucrarea datelor cu caracter personal în cadrul activității informative/contrainformative ar trebui să constituie obiectul legislației cu privire la datele cu caracter personal. Or, Centrul pentru protecția datelor cu caracter personal are drept obiectiv apărarea drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viață privată în legătură cu prelucrarea și transmiterea transfrontalieră a datelor cu caracter personal (art.55).</p>	<p><b>Se acceptă.</b>          Articolul respectiv a fost revizuit, iar prelucrarea datelor cu caracter personal se va efectua în condiții generale ținându-se cont de particularitățile prevăzute de prezenta lege și nu în exclusivitate de aceasta.</p>
<p>9. Similar sugestiei descrise supra la proiectul nr.420 reiterăm lipsa reglementărilor clare privind controlul judiciar efectiv al măsurilor întreprinse de Serviciul de Informații și Securitate. Aceasta ar trebui să includă</p>	<p><b>Se acceptă.</b>          Au fost operate modificările corespunzătoare la temeiurile de</p>

	<p>autorizarea judiciară prealabilă pentru a desfășura anumite activități operative/de investigație cu un potențial ridicat de a încălca drepturile omului, precum și o formă de control ulterioară care verifică dacă sunt îndeplinite condițiile.</p> <p>În legătură cu mandatul de securitate, Comisia de la Veneția a recomandat Republicii Moldova:</p> <p>a) prevederea condițiilor suficient de clare și precise pentru autorizarea judiciară a mandatului de securitate, solicitând, printre altele, indicii concrete privind activitatea criminală, suspiciuni rezonabile și o definiție mai îngustă a categoriilor</p> <p>de persoane vizate de investigația specială în baza mandatului de securitate;</p> <p>b) specificarea circumstanțelor pentru autorizarea de urgență și prevederea termenului rezonabil pentru revizuirea ulterioară de către judecător;</p> <p>c) specificarea mai corespunzătoare a motivelor de amânare a înștiințării persoanei vizate de un mandat de securitate și consolidarea garanțiilor aferente, inclusiv prin mecanisme adecvate pentru revizuire periodică a deciziei de neînștiințare și a unui drept efectiv de a contesta această decizie, precum și decizia de a emite mandatul de securitate.</p>	<p>autorizare, procedura de autorizare, procedura de autorizare pentru cazurile ce nu suferă amânare și controlul legalității post autorizării, precum și specificarea concretă a motivelor de amânare, condițiile de neinformare, toate aceste mecanisme sunt supuse controlului de către judecătorul special împuternicit.</p>
<p><b>Centrul Național pentru Protecția Datelor cu Caracter Personal (CNPDCP)</b> Nr. 04-06/245 din 27 ianuarie 2023</p>	<p>1. La art. 1: Având în vedere că legea trebuie să stabilească inclusiv garanțiile minime de protecție a persoanelor împotriva abuzurilor și arbitrarului, art. 1 alin. (1) din proiect, care reglementează domeniul de aplicare, se propune de completat cu sintagma <i>„garanțiile minime de protecție a persoanelor supuse măsurilor contrainformative, garanțiile procedurale de contestare a acestora”</i>.</p>	<p><b>Se acceptă.</b> Art. 1 alin. (1) a fost completat cu sintagma „garanții minime de protecție a persoanelor supuse măsurilor contrainformative”. Complementar, este de notat faptul că garanțiile minime de protecție a persoanelor supuse măsurilor contrainformative, includ inclusiv garanțiile procedurale de contestare a acestora. Suplimentar, prin art. 20<sup>1</sup> din proiectul de lege s-a prevăzut expres procedura de control a legalității efectuării măsurilor contrainformative de către judecător, care reprezintă o garanție importantă pentru subiecții în privința cărora s-au efectuat măsurile respective.</p>
	<p>2. Se propune la articolul 2, la enumerarea principiilor, de completat suplimentar cu o nouă literă: <i>i) contestării efective în fața unei autorități judiciare independente a legalității acțiunilor/inacțiunilor subiecților care</i></p>	<p><b>Nu se acceptă.</b> În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate</p>

<p>efectuează activitatea informativă/contrainformativă;</p>	<p>națională, apărare și ordine publică s-a decis redarea art. 2 în forma respectivă, fără a include respectivul principiu. Suplimentar este de notat faptul că, art. 58 alin. (2) din proiect stabilește procedura de control exercitată de către procuror, în baza plângerilor despuse de către persoane ale căror drepturi și interese legitime se presupune că au fost încălcate sau din oficiu, fapt care permite contestarea acțiunilor subiecților care efectuează măsurile contrainformative.</p>
<p>3. Se propune completarea art. 3 cu două alineate noi:  <i>(4) Rezultatele activității informative/contrainformative, inclusive rezultatele măsurilor speciale de investigații efectuate cu încălcarea legii sunt nule de drept și nu pot fi stocate pentru utilizare în cadrul altor dosare speciale</i>  <i>(5) Persoanele vizate de activitatea informativă/contrainformativă efectuată cu încălcarea legislației dispun de dreptul de a solicita achitarea unor despăgubiri pentru repararea prejudiciului material și moral cauzat și pentru repararea consecințelor cauzate.</i></p>	<p><b>Se acceptă parțial.</b>  Articolul 3 a fost exclus.  Cu toate acestea, propunerea privind declararea rezultatelor măsurilor contrainformative efectuate cu încălcarea vădită a drepturilor și libertăților persoanei să fie declarate nule a fost inserată în cadrul art. 20<sup>1</sup> alin. (4) din proiect.  Referitor la celelalte propuneri, menționăm că în cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică nu au fost acceptate propunerile respective.</p>
<p>4. După articolul 5 din proiect care stabilește Drepturile subiecților care efectuează activitatea informativă/contrainformativă, se propune completarea legii cu un articol nou care să reglementeze Obligațiile și restricțiile subiecților care efectuează activitatea informativă/contrainformativă, care să conțină cel puțin următoarele obligații și restricții:  Obligații:  a) să respecte drepturile și interesele legitime ale persoanei;  b) să întreprindă, în limitele competenței, toate măsurile în vederea apărării drepturilor și libertăților omului, protecției tuturor formelor de proprietate ocrotite de lege pentru asigurarea securității statului și a ordinii publice;  c) să respecte confidențialitatea datelor cu caracter personal ce au devenit cunoscute în timpul efectuării măsurii speciale de investigații;</p>	<p><b>Se acceptă parțial.</b>  La art. 5 alin. (1) a fost menționat expres că Serviciul și ofițerii de informații dispun de drepturile și au obligațiile stabilite în Legea privind Serviciul de Informații și Securitate al Republicii Moldova și Legea nr. 170/2007 privind statutul ofițerului de informații și securitate, fapt care acoperă juridic propunerile respective, iar în parte ace vizează activitatea informativă externă, prin alin. (1)<sup>1</sup> au fost reglementate inclusiv drepturile și obligațiile de care</p>

<p>d) să respecte proporționalitatea dintre dreptul lezat și necesitatea măsurii ce se efectuează;</p> <p>e) să asigure documentarea și arhivarea fără excepții a materialelor privind desfășurarea activității informative și contrainformative.</p> <p>Restricții:</p> <p>(1) Subiecților care efectuează activitatea informativă/contrainformativă li se interzice:</p> <p>a) să provoace comiterea de infracțiuni;</p> <p>b) să antreneze în activitatea informativă/contrainformativă, în calitate de persoane care colaborează <i>confidential</i> cu Serviciul, deputați, judecători, procurori, ofițeri de urmărire penală și avocați.</p>	<p>dispune Ministerul Apărării și Militarii.</p>
<p>5. Sintagma „în condițiile prezentei legi” de la alin. (1) a art. 7 considerăm că are un caracter general, lăsând loc de interpretări și crează circumstanțe pentru acțiuni abuzive din partea subiecților care efectuează activitatea informativă/contrainformativă, fiind necesar a specifica în baza căror articole din lege revin obligațiile descrise la acest articol persoanelor fizice și juridice, or, eventual, doar invocarea obligației statuate la art. 7 în solicitarea de acordare a asistenței nu este suficientă.</p> <p>Suplimentar, se propune completarea articolului cu un nou alineat cu următorul conținut:</p> <p>(4) <i>Serviciul va asigura documentarea permanentă și fără excepții a informațiilor obținute în cadrul procesului de acordare a asistenței la efectuarea activității informative și contrainformative de către persoanele și entitățile de drept public sau privat enumerate la alin. (1).</i></p>	<p><b>Se acceptă parțial.</b></p> <p>Articolul 7 a fost exclus în întregime, dispărând necesitatea efectuării modificărilor propuse.</p>
<p>6. La Articolul 8 „Utilizarea mijloacelor tehnice la efectuarea activității informative/contrainformative” se propune completarea articolului cu un nou alineat cu următorul conținut:</p> <p><i>La efectuarea activității informative/contrainformative pot fi utilizate doar mijloace tehnice speciale destinate pentru obținerea ascunsă a informației, aparate de înregistrare video, audio sau a alte mijloace tehnice care se află exclusiv la balanța Serviciului și sunt înregistrate în mod corespunzător.</i></p>	<p><b>Se acceptă.</b></p> <p>Articolul 8 a fost redat într-un alineat unic, care inserează propunerea formulată.</p>
<p>7. La Articolul 9 „Dosarul special” se propune completarea articolului cu noi alineate cu următorul conținut:</p> <p><i>Activitatea informativă/contrainformativă efectuată în afara urmării penale este permisă doar în condițiile inițierii unui dosar special, în limitele acestuia, și exclusiv în baza temeiurilor prevăzute la art.13 din lege.</i></p> <p><i>Activitatea informativă/contrainformativă efectuată în afara urmării penale și în afara unui dosar special este nulă de drept și atrage răspunderea</i></p>	<p><b>Nu se acceptă.</b></p> <p>Normele din articolul 9 în redacția respectivă au fost examinate în cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică, astfel încât s-a decis redare articolului în forma expusă. Cu toate acestea, ideile propuse sunt</p>

<p>înglobate inclusiv în prevederile de la art. 9.</p> <p>Suplimentar, în redacția existentă, s-a sporit controlul în vederea inițierii dosarului special, or, în propunerile din aviz dosarul special se coordona de către conducătorul subdiviziunii specializate, pe când proiectul prevede un mecanism mai riguros de coordonare, și anume de către directorul sau directorul adjunct al Serviciului.</p>	<p><b>Nu se acceptă.</b></p> <p>În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică au fost discutate subiectele respective și s-a decis expunerea art. 10 în forma redată.</p> <p>Suplimentar, este de notat faptul că art. 23 din proiect stabilește expres procedura de informare a persoanei despre măsurile contrainformative înfăptuite în privința sa.</p>	<p>disciplinară,</p> <p>contravențională și/sau penală prevăzută de legislație.</p> <p>Conducătorul subdiviziunii specializate este responsabil de legalitatea inițierii dosarului special și a acțiunilor efectuate în cadrul acestuia.</p> <p>Ofițerul de informație nu poate iniția un dosar special fără coordonarea conducătorului subdiviziunii specializate.</p>	<p>8. La Articolul 10 „Gestionarea materialelor irelevante pentru activitatea informativă/contrainformativă” se propune completarea articolului cu două alineate cu următorul conținut:</p> <p><i>Rezultatele activității informative/contrainformative efectuate cu încălcarea legislației nu pot fi sususe ștergerii/distrugerii fără notificarea persoanei a cărei drepturi au fost încălcate.</i></p> <p><i>Informația cu privire la fapte de încălcare a drepturilor și libertăților fundamentale ale omului se desecretizează în modul stabilit de legislația cu privire la secretul de stat, cu notificarea obligatorie a persoanelor vizate de acestea.</i></p>	<p><b>Precizare.</b> Actele departamentale care vor detalia toate procesele necesare realizării activității contrainformative/informative vor avea ca scop implementarea legii, astfel încât acestea vor fi în strictă conformitate cu prevederile expuse în proiect și vor urmări nemijlocit scopul expus în lege, fără a reglementa careva norme care să excedă acesteia. În context, o asemenea normă de precizare în lege este irelevantă.</p> <p>Totodată, art. 1 alin. (3)<sup>1</sup> stabilește expres că desfășurarea activității informative/contrainformative în alte scopuri decât cele menționate de prezenta lege nu se admite, astfel încât, nici actele departamentale nu vor putea deține</p>	<p>9. La art. 11 Reglementarea departamentală a activității informative/contrainformative :</p> <p>Deși legea nu poate să prevadă o reglementare detaliată a activității informative/contrainformative din varii motive (prin lege e posibilă reglementarea unor aspecte generale, asigurarea caracterului secret/confidențial al activităților etc), pentru întrunirea criteriilor de claritate și previzibilitate pe care trebuie să le întrunească o lege, se propune completarea articolului cu anumite prevederi detaliate pe care trebuie să le respecte reglementările departamentale.</p> <p>Astfel, se propune introducerea interdicției exprese ca reglementările departamentale să excedeze domeniul de aplicare a legii sau să vină în contradicție.</p>
---	---	---	---	--	--

<p>reglementări contrare legii și scopului acesteia.</p> <p><b>Se acceptă.</b> Potrivit art. 12 alin. (1) pct. 2) din proiect, măsurile conținutive vor fi efectuate în baza mandatului judecătoresc, care le va autoriza, fiind un organ judiciar independent de organul care va efectua aceste măsuri.</p>	<p><b>Nu se acceptă.</b> În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică aceste aspecte au fost discutate, fiind acceptată formularea respectivă.</p>	<p>Având în vedere riscurile înalte de abuzuri care reies din acordarea posibilității de a autoriza măsurile conținutive în mod independent de către aceeași autoritate care este competentă să le efectueze, se propune ca autorizarea măsurilor prevăzute la art. 12 alin. (1) pct. 1) lit. a), lit. b), lit. c) și lit. e) să fie efectuată de către un organ judiciar independent (procuror sau instanța de judecată).</p> <p>10. La Articolul 13 „Temeiurile pentru efectuarea măsurilor conținutive”: Pentru asigurarea clarității și previzibilității legii, se necesită excluderea temeiurilor legale precum: - informațiile devenite cunoscute. Se propune de reformulat cu - <i>informațiile veridice care pot fi probate</i>; 11. În aceeași ordine de idei, se propune excluderea sau reformularea temeiului prevăzut la alin. (1) pct. 5, care stabilește temei - <i>necesitatea de a obține date informative</i>.</p> <p>12. La Articolul 14 „Procedura autorizării măsurilor conținutive de către directorul Serviciului sau directorului adjunct special împuternicit”: Având în vedere riscurile înalte de abuzuri care reies din acordarea posibilității a autoriza măsurile conținutive în mod independent de către aceeași autoritate care este competentă să le efectueze, se propune ca autorizarea măsurilor prevăzute la alin. (1) pct. 1) lit. a), lit. b), lit. c) și lit. e) să fie efectuată de către un organ judiciar independent (procuror sau instanța de judecată). Suplimentar, se propune reformularea alin. (4) pentru ca și în cazul autorizării măsurilor conținutive de către conducerea Serviciului să fie stabilită obligația verificării în prealabil dacă: a) <i>acțiunea solicitată urmărește un scop legitim</i>; c) <i>acțiunea va fi proporțională cu dreptul sau libertatea persoanei garantată de lege și necesitatea apărută</i>.</p> <p>13. La Articolul 20 „Consemnarea măsurilor conținutive”: Se propune completarea articolului cu două alineate noi cu următorul conținut: (4) <i>Rezultatele activității informative/conținutive efectuate cu încălcarea legislației nu pot fi ștergerii/distrugerii fără notificarea persoanei lezate în drepturi</i>.</p>	<p><b>Se acceptă.</b> Măsurile conținutive nominalizate vor fi autorizate prin mandat judecătoresc, fiind asigurat un control în acest sens de către un organ judiciar independent de autoritatea care efectuează măsurile respective. Suplimentar, la alineatul (3) al articolului 14 din proiect s-a inclus propuneri formulate.</p>	<p><b>Nu se acceptă.</b> În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică aceste aspecte au fost discutate, fiind acceptată formularea articolului în redacția propusă, din motive obiective.</p>
--	---	--	--	--

<p>(5) <i>La dosarul special se păstrează obligatoriu informațiile obținute de la prestatorii de servicii de comunicații electronice în cadrul procesului de acordare a asistenței la efectuarea activității informative și conținuturile informative de către persoanele și entitățile de drept public sau privat enumerate la art. 7 alin. (1) al legii.</i></p>	<p>Totodată, ideile respective se regăsesc în proiect la art. 9, care stabilește expres că toate informațiile culese se păstrează în dosarul special și acestea nu pot fi distruse.</p>
<p>14. La Articolul 21 „Utilizarea rezultatelor măsurilor conținuturilor informative”: Se propune completarea articolului cu un alineat nou cu următorul conținut: (6) <i>Rezultatele măsurilor conținuturilor informative obținute cu încălcarea legii și alte informații cu privire la fapte de încălcare a drepturilor și libertăților fundamentale ale omului se desecretizează în modul stabilit de legislația cu privire la secretul de stat, cu notificarea obligatorie a persoanelor vizate de acestea.</i></p>	<p><b>Nu se acceptă.</b> În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică aceste aspecte au fost discutate, fiind acceptată formularea articolului în redacția propusă, din motive obiective.</p>
<p>15. La Articolul 23 „Informarea persoanei despre măsurile conținuturilor informative înfăptuite în privința sa”: În vederea asigurării unei notificări veridice funcționale, se propune completarea articolului cu un alineat nou: (8) <i>Informarea persoanei se efectuează după încetarea situației care afectează considerabil atingerea scopurilor de asigurarea a securității naționale urmărite în cadrul activității efectuate în temeiul prezentei legi, dar nu mai târziu de 5 ani de la data prelucrării datelor cu caracter personal pentru fiecare caz în parte.</i> (9) <i>Neinformarea persoanei contrar prevederilor prezentului articol atrage răspunderea disciplinară, contravențională și/sau penală prevăzută de legislație.</i></p>	<p><b>Nu se acceptă.</b> Articolul 23 prevede expres procedura de informare sau neinformare a persoanelor în privința cărora au fost efectuate măsuri conținuturilor informative. Respectiv, neinformarea persoanei are loc în cazul existenței unor temeuri obiective în acest sens, fiind supusă unei duble autorizări, în mod primar de către directorul Serviciului, și ulterior, de către judecătorul care a eliberat mandatul judecătoresc. Aceste temeuri sunt supuse unor reevaluări anuale, iar în momentul în care temeuriile de neinformare decad, persoana imdeiat va fi informată despre efectuare în privința acesteia a măsurilor conținuturilor informative.</p>
<p>16. La Articolul 55 „Controlul asupra prelucrării datelor cu caracter personal în cadrul activității informative/conținuturilor informative”: În forma actuală, prevederile acestui articol, în special alin. (2) nu sunt compatibile cu prevederile Legii nr. 271/2013 privind formularea declarațiilor în privința modului de aplicare a Convenției 108, și contravine cu Decretul Președintelui Republicii Moldova nr. 757 din 22 decembrie 2022, prin care s-a aprobat semnarea Protocolului de amendare a Convenției pentru protecția persoanelor referitor la prelucrarea datelor cu caracter personal, care face referire inclusiv la prelucrarea datelor în scopul asigurării securității naționale,</p>	<p><b>Se acceptă.</b> Alin. (2) al art. 55 a fost exclus. Complementar alin. (1) al art. 55 din proiect a fost ajustat, astfel încât s-a prevăzut expres că controlul asupra prelucrării datelor cu caracter personal în cadrul activității informative/conținuturilor informative se efectuează în condiții generale.</p>

<p>din care motiv urmează a fi excluse.</p> <p>De asemenea trezește semne de întrebare cum va fi efectuat controlul prelucrării datelor cu caracter personal dacă proiectul pus în discuție nu conține prevederi privind condiții generale de prelucrare a datelor cu caracter personal, modul de realizare a drepturilor subiecților de date cu caracter personal, care sunt prevăzute de Legea nr. 133/2011 privind protecția datelor cu caracter personal. De altfel, urmează a menționa că Legea nr. 133/2011 prevede posibilitatea aplicării excepțiilor și restricțiilor la prelucrarea datelor cu caracter personal în anumite cazuri, situație care poate fi aplicată și în raport cu activitățile efectuate în cadrul activității informative/contrainformative.</p>	<p>Prevederile de la art. 56 lasă loc de abuzuri, or, în situația în care Serviciul șterge datele colectate în cadrul activității informative/contrainformative, în circumstanțele descrise la alin. (1), persoanele nu vor cunoaște despre colectarea datelor ce îi vizează, circumstanțele în care au fost colectate și nu vor avea temeii pentru a se adresa procurorului sau instanței de judecată pentru a contesta legalitatea acestor acțiuni, or, unul din subiectele ce trezesc semne de întrebare este cum se asigură informarea persoanelor în legătură cu prelucrarea datelor cu caracter personal în cadrul activității informative/contrainformative.</p>	<p><b>Se acceptă.</b></p> <p>Articolul 56 a fost exclus, astfel fiind remediată problema.</p>
<p>17. La Articolul 57 „Controlul parlamentar”:</p> <p>În vederea eficientizării acestui tip de control, se propune:</p> <p><i>(7) În baza informațiilor din Raportul general privind activitatea informative /contrainformativă prezentat de către Serviciu și a altor informații relevante, Subcomisia parlamentară va publica un Raport public privind rezultatele efectuării controlului parlamentar asupra activității informative/contrainformative. Raportul subcomisiei parlamentare va conține cel puțin:</i></p> <p><i>a) informații despre numărul total al măsurilor contrainformative efectuate pe parcursul anului, comunicat de Serviciu;</i></p> <p><i>b) informații privind numărul măsurilor contrainformative pentru care s-a eliberat mandat judecătoresc și numărul celor refuzate de a fi autorizate;</i></p> <p><i>c) informații privind numărul de cazuri în care s-a constatat încălcarea prevederilor legislației la efectuarea activității informative/contrainformative;</i></p> <p><i>d) informații privind numărul de proceduri disciplinare/penale pornite și numărul de cazuri de aplicare a sancțiunilor disciplinare, contravenționale, după caz penale;</i></p> <p><i>e) informații privind numărul de sesizări înaintate în adresa organelor de</i></p>	<p><b>Se acceptă.</b></p> <p>Articolul 57 a fost completat cu alin. (7) și (8) care vin să implementeze ideile propuse, astfel încât problemele semnalate au fost înlăturate.</p>	<p><b>Se acceptă.</b></p> <p>Articolul 57 a fost completat cu alin. (7) și (8) care vin să implementeze ideile propuse, astfel încât problemele semnalate au fost înlăturate.</p>

	<p><i>drept sau în instanța de judecată pe fapte de încălcare a legislației la efectuarea activității informative/contrainformative.</i></p> <p>18. Totodată, considerăm că în condițiile statuate la acest articol, controlul parlamentar nu este unul efectiv, or, controlul parlamentar se limitează la rapoarte ce conțin date statistice și nu se expune asupra legalității acțiunilor întreprinse de SIS pe un caz concret.</p> <p>19. La Articolul 58 „Controlul exercitat de către procuror”:      Având în vedere propunerea făcută pe marginea art. 12 din proiect în scopul diminuării riscurilor de abuzuri care reies din acordarea posibilității a autoriza măsurile contrainformative în mod independent de către aceeași autoritate care este competentă să le efectueze, se propune ca autorizarea măsurilor prevăzute la alin.(1) pct. 1) lit.a), lit. b), lit. c) și lit. e) să fie efectuată de către un organ judiciar independent (procuror sau instanța de judecată), se propune ca articolul dat să facă trimitere expres la controlul legalității măsurilor de investigație autorizate de procuror.      Suplimentar, se propune completarea cu alineat nou:  <i>(5) Controlul exercitat de procuror se efectuează în privința activității contrainformative realizate din momentul dispunerii măsurilor de investigații până la încetarea acestora și se extinde inclusiv asupra constatării și sancționării faptelor de neinformare a persoanei despre măsurile contrainformative înfăptuite în privința sa, contrar prevederilor art. 23 din proiect cu completările propuse.</i></p> <p>20. La Articolul 60 „Controlul exercitat de către magistrați”:      Se propune completarea articolului cu un alineat nou:  <i>„Orice persoană este în drept să se adreseze în instanță pentru repunerea în drepturile încălcate la efectuarea activității contrainformative și să solicite repararea prejudiciilor materiale și morale cauzate în legătură cu aceasta.”</i></p>	<p><b>Se acceptă parțial.</b>      Luând în considerare faptul că măsurile contrainformative, în cea mai mare parte a lor se autorizează de către judecător, respectiv acesta va verifica temeinicia înfăptuirii măsurilor contrainformative la eliberarea mandatului judecătoresc sau va aprecia legalitatea acțiunilor efectuate în absența mandatului judecătoresc.      Respectiv, ideile propuse au fost luate în considerare, doar că în cadrul controlului exercitate de către magistrați.</p>
		<p><b>Nu se acceptă.</b>      În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică aceste aspecte au fost discutate, menținându-se poziția propusă.</p>
		<p><b>Nu se acceptă.</b>      Considerăm oportună menținerea articolului în propunerea redată.</p>
		<p><b>Se acceptă.</b>      Articolul 4 a fost competat cu alineatul (1)<sup>1</sup> care stipulează că activitatea informativă externă în domeniul militar este efectuată</p>
<p><b>Guvernul Republicii Moldova</b></p>	<p>Recomandăm divizarea art. 1 al proiectului de lege în 2 articole separate: unul care ar stabili domeniul de reglementare al legii și altul care ar indica principalele noțiuni utilizate în conținutul legii și semnificatia acestora.</p> <p>La art. 4 menționăm că prin proiect se exclude orice implicare a altei autorități, cu excepția Serviciului de Informații și Securitate al Republicii Moldova, în înfăptuirea măsurilor contrainformative și informative externe.      Respectiv, considerăm necesară includerea în proiect a prevederilor</p>	

<p>de către Ministerul Apărării.</p>	<p><b>Precizare.</b> Alineatul (2) al articolului 5 din proiectul de lege a fost exclus în întregime.</p>
<p>referitoare la realizarea activității de informații de către alte entități ce fac parte din sistemul organelor securității statului – Ministerul Afacerilor Interne, Serviciul de Protecție și Pază de Stat, Serviciul Vamal, precum și Ministerul Apărării, conform competențelor legale atribuite.</p> <p>Amintim că, în temeiul pct. 6 subpct. 3) din Regulamentul cu privire la organizarea și funcționarea Ministerului Apărării, aprobat prin Hotărârea Guvernului nr. 692/2017, Ministerul Apărării realizează funcții în domeniul analizei și informațiilor militare.</p> <p>În conformitate cu prevederile art. 6 din Legea nr. 59/2012 privind activitatea specială de investigații, Ministerului Apărării îi este atribuită calitatea de subiect cu drept de efectuare a măsurilor speciale de investigații, având drept sarcină de bază în temeiul art. 2 lit. d), colectarea de informații despre posibile evenimente și/sau acțiuni ce ar putea pune în pericol securitatea militară a statului.</p> <p>Astfel, pentru prevenirea și contracararea riscurilor și amenințărilor interne și externe, cu caracter politico-militar, la adresa securității statului, Ministerul Apărării, prin intermediul structurilor de informații militare, desfășoară activitate informativă în domeniul apărării pentru decidenții politici.</p> <p>Activitatea informativă în domeniul militar reprezintă măsuri de culegere, prelucrare, verificare, protecție și valorificare a informațiilor necesare cunoașterii, prevenirii și contracarării oricăror acțiuni care constituie, potrivit legii, amenințare pentru independența, suveranitatea, unitatea, integritatea teritorială și a democrației constituționale, asigurarea apărării naționale prin prevenirea, contracararea și înlăturarea amenințărilor și agresiunilor cu caracter military îndreptate împotriva țării.</p> <p>Respectiv, se vor revizui prevederile art. 4 prin prisma celor expuse.</p> <p>La art. 5 alin. (2) lit. b), d) și e) menționăm următoarele:</p> <ul style="list-style-type: none"> <li>- lit. b), după cuprinsul său, reglementează ca un drept al ofițerului de informații ceea ce în activitatea specială de investigații reprezintă măsură specială de investigații „Chestionarea”, fără a o cataloga ca pe o măsură contrainformativă, prin analogie cu cea specială de investigații. Astfel, art. 34 din Legea nr. 59/2012 privind activitatea specială de investigații prevede că „chestionarea constă în comunicarea nemijlocită a ofițerului de investigații și a altor persoane împuternicite de către acesta cu persoanele care posedă sau care dispun de informații despre fapte, evenimente, circumstanțe sau persoane care prezintă interes”;</li> <li>- lit. d), după cuprinsul său, reglementează ca un drept al ofițerului de informații ceea ce în activitatea specială de investigații reprezintă măsură specială de investigații „Culegerea de informații despre persoane și fapte”, fără</li> </ul>	<p>informații ceea ce în activitatea specială de investigații reprezintă măsură specială de investigații „Chestionarea”, fără a o cataloga ca pe o măsură contrainformativă, prin analogie cu cea specială de investigații. Astfel, art. 34 din Legea nr. 59/2012 privind activitatea specială de investigații prevede că „chestionarea constă în comunicarea nemijlocită a ofițerului de investigații și a altor persoane împuternicite de către acesta cu persoanele care posedă sau care dispun de informații despre fapte, evenimente, circumstanțe sau persoane care prezintă interes”;</p> <ul style="list-style-type: none"> <li>- lit. d), după cuprinsul său, reglementează ca un drept al ofițerului de informații ceea ce în activitatea specială de investigații reprezintă măsură specială de investigații „Culegerea de informații despre persoane și fapte”, fără</li> </ul>

a o cataloga ca pe o măsură contrainformativă, prin analogie cu cea specială de investigații.

Astfel, art. 35 din Legea nr. 59/2012 privind activitatea specială de investigații prevede că „culegerea de informații despre persoane și fapte constă în dobândirea informațiilor despre persoane fizice și juridice, despre faptele, evenimentele și circumstanțele care prezintă interes, prin studierea nemijlocită a documentelor, a materialelor, a bazelor de date, prin întocmirea de solicitări adresate persoanelor fizice și juridice care posedă sau care dispun de informații”;

- lit. e), după cuprinsul său, reglementează ca un drept al ofițerului de informații ceea ce în activitatea specială de investigații reprezintă măsură specială de investigații „Identificarea persoanei”, fără a o cataloga ca pe o măsură contrainformativă, prin analogie cu cea specială de investigații. Astfel, art. 36 din

Legea nr. 59/2012 privind activitatea specială de investigații prevede că „identificarea persoanei constă în stabilirea persoanei după semnalmentele statice [...] și dinamice [...], precum și prin intermediul fotorobotului și al altor metode ce dau posibilitate de a stabili persoana cu o probabilitate sporită”.

Reiese că, prin exercitarea acestor drepturi, ofițerii de informații vor efectua niște măsuri contrainformative analoge celor speciale de investigații, chiar dacă potrivit prevederilor propuse în proiectul de lege asemenea acțiuni nu constituie măsuri contrainformative, în acest fel fiind evitată parcurgerea procedurii de dispunere, autorizare, efectuare, prelungire, încetare și consemnare, cu toate că aceste acțiuni comportă ingerințe semnificative în viața privată a persoanei.

Mai mult decât atât, în condițiile în care rezultatele, adică informațiile obținute prin asemenea acțiuni nu se consemnează într-un proces-verbal în conformitate cu prevederile art. 20, nu este clar cum acestea vor fi valorificate, inclusiv utilizate prin prisma art. 21, de exemplu – pentru efectuarea altor măsuri contrainformative (art. 21 alin. (1) lit. b)), fiind puse la baza demersurilor privind autorizarea efectuării altor măsuri contrainformative.

Suplimentar, notăm că, textul „cu sau fără înregistrarea discuției cu ajutorul mijloacelor tehnice” conținut în cuprinsul dispoziției normei juridice prevăzute de art. 5 alin. (2) lit. b) nu reprezintă altceva decât o interceptare și înregistrare a comunicărilor ambientale purtate între ofițer și persoană, posibilitatea reproducerii acestora constituind o imixtiune gravă în viața privată a persoanei.

Așadar, reglementarea acestei acțiuni ca pe un drept al ofițerului de informații și nu ca pe o măsură contrainformativă pentru care este necesară

	<p>autorizația unui judecător de instrucție, în calitate de magistrat independent, poate duce la eventualele abuzuri.</p> <p>Reieșind din cele expuse mai sus, insistăm asupra excluderii lit. b), d) și e) de la art. 5 alin. (2) și completării, în capitolul II, secțiunea 2, cu un articol nou, intitulat „Culegerea de informații”, cu următorul cuprins „Culegerea de informații constă în dobândirea informațiilor despre persoane fizice și juridice, bunuri mobile și imobile, fapte, evenimente și circumstanțe care prezintă interes, prin comunicare nemijlocită cu alte persoane, prin studiere de documente, materiale, baze de date, sisteme informaționale și surse deschise, prin adresare de solicitări persoanelor fizice și juridice care posedă sau care dispun de informații care prezintă interes, precum și după semnalamentele statice și dinamice, prin intermediul fotorobotului și al altor metode ce oferă posibilitatea de a identifica o persoană cu o probabilitate sporită”. În acest fel, acțiunile respective vor fi reglementate ca măsură contrainformativă, așa cum se cuvine, ținând cont de ingerințele pe care le comportă.</p>
<p><b>Precizare.</b> Alineatul 4 al articolului 5 și alineatul (1) al articolului 7 din proiectul de lege au fost excluse.</p>	<p>Art. 5 alin. (4) se va revedea în scopul instituirii posibilității organelor de ocrotire a normelor de drept, ale autorităților publice și persoanelor juridice indiferent de tipul de proprietate, de a cere compensare, în cazurile în care folosirea acestor servicii au implicat cheltuieli, or, obligarea de oferire pe gratis a unor servicii nu va putea fi mereu justificată. De asemenea, în corelație cu prevederile de la art. 7 alin. (1), menționăm că persoanele private nu pot fi constrânse să ofere toată informația de care dispun, ci doar informația pe care acestea sunt obligate să o prezinte Serviciului conform legii.</p>
<p><b>Precizare.</b> Alineatul (2) și (3) al articolului 5 din proiectul de lege au fost excluse în întregime.</p>	<p>Art. 5 alin. (2) lit. d) se va aduce în concordanță cu noțiunile utilizate în Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, prin substituirea textului „sisteme informaționale, baze de date” cu cuvintele „să acceseze date deținute în sisteme și resurse informaționale”.</p> <p>Totodată, luând în considerare dispozițiile art. 2 alin. (1), art. 6 alin. (2) și (4) din Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate și faptul că schimbul de date dintre autoritățile și instituțiile publice este reglementat prin legea în cauză și Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MCConnect), propunem de completat lit. d), după cuvintele „platformei de interoperabilitate” cu cuvintele „în conformitate cu prevederile cadrului normativ care reglementează domeniul schimbului de date și al interoperabilității”.</p> <p>Suplimentar, la același alin. (2) lit. d), considerăm necesar de exclus ultimul enunț, or, regulile de acces la bazele de date se stabilesc de cadrul normativ prin care au fost instituite sistemele informaționale respective, precum și de posesorul acestora, nicidecum de către Serviciul de Informații și Securitate.</p>

	<p>Alternativ, propunem expunerea enunțului respectiv cu următorul cuprins:  „Posesorii sistemelor informaționale colaborează cu Serviciul în vederea asigurării respectării regulilor și a procedurilor de ținare a evidenței accesului la datele puse la dispoziția Serviciului.”</p> <p>În conformitate cu art. 72 și art. 73 alin. (2) din Legea nr. 467/2003, la alin.(3) lit. a) recomandăm substituirea textului „să achiziționeze, creeze, mențină, perfecționeze, administreze sisteme informaționale” cu textul „să asigure condițiile juridice, financiare și organizatorice și să asigure crearea, administrarea, mentenanța și dezvoltarea de sisteme informaționale”.</p>
<p><b>Precizare.</b> Alineatul (8) și (9) al articolului 6 din proiectul de lege au fost excluse.</p>	<p>Prevederile art. 6 alin. (8) și (9) urmează a fi revizuite, deoarece se încearcă de a institui o tratare diferită a persoanelor care colaborează cu Serviciul, în funcție de forma încheierii acordului (scrisă sau verbală). Astfel, este inadmisibilă acordarea unor recompense persoanelor care și-au exprimat în scris consimțământul de a colabora cu Serviciul de Informații și Securitate al Republicii Moldova și neacordarea recompensei celor care tot colaborează cu Serviciul, dar care și-au exprimat consimțământul printr-un acord verbal. De fapt, recompensele acordate nu au legătură directă cu forma încheierii acordului, dar cu urmările survenite în urma colaborării cu Serviciul (deces, mutilări), or, orice persoană care colaborează cu Serviciul trebuie să beneficieze de aceleași garanții.</p>
<p><b>Precizare.</b> Articolul 7 din proiectul de lege a fost exclus în întregime.</p>	<p>La art. 7 referitor la colectarea informațiilor, în pct. 15 din Avizul Comisiei de la Veneția se menționează că colectarea informațiilor, inclusive a informațiilor cu privire la persoane constituie un amestec asupra drepturilor individuale, îndeosebi a dreptului la respectarea vieții private și de familie, a domiciliului și corespondenței, consacrat în articolul 8 al CEDO, dar și a altor drepturi fundamentale. Prin urmare, este absolut necesar ca rolul, funcțiile, puterile și îndatoririle agențiilor de securitate să fie clar definite și delimitate de legislație sau Constituție. În mod egal, aceste agenții trebuie să fie supravegheate îndeaproape.</p>
<p><b>Precizare.</b> Articolul 7 din proiectul de lege a fost exclus în întregime.</p>	<p>La prevederile art. 7 alin. (3) se va ține cont de prevederile art. 10 alin. (1) lit. o) din Legea nr. 753/1999 privind Serviciul de Informații și Securitate și art. 26 alin. (1) din Legea nr. 170/2007 privind statutul ofițerului de informații și securitate. În conformitate cu normele menționate, detașarea ofițerilor deinformații și securitate în cadrul autorităților publice și a structurilor organizaționale din sfera lor de competență se realizează fie în temeiul unei hotărâri a Parlamentului, la decizia Președintelui, în temeiul unei hotărâri a Guvernului ori a unui tratat internațional, fie cu acordul instituției interesate, pentru îndeplinirea unor funcții în interesul securității naționale, iar nu la simpla solicitare din partea Serviciului.</p>

	<p>Prin urmare, se vor revizui prevederile art. 7 alin. (3) în scopul evitării apariției unor norme conflictuale și a armonizării actelor normative, dar și a excluderii posibilității de aplicare nejustificată și abuzivă a normei juridice.</p> <p>Art. 8, propunem a fi expus în următoarea redacție: „La efectuarea activității informative/contrainformative se permite, în cazurile și condițiile stabilite de lege, utilizarea mijloacelor tehnice, cum ar fi aparatele de fotografiat și cele de supraveghere și/sau de înregistrare audio și/sau video, inclusiv mijloacelor tehnice speciale, precum și a sistemelor informaționale”. Pe această cale se va face distincție între: 1) mijloacele tehnice, printre care și aparatele de fotografiat și cele de supraveghere și/sau de înregistrare audio și/sau video aflate în circulație nerestricționată; și 2) mijloacele tehnice speciale, printre care și aparatele de fotografiat și cele de supraveghere și/sau de înregistrare audio și/sau video aflate în circulație restricționată, utilizate pentru obținerea în secret a informațiilor.</p> <p>În prevederile art. 10 necesită a se specifica cine apreciază care materiale sunt relevante sau irelevante pentru cauza cercetată. Considerăm oportună referirea la un act normativ care va reglementa strict modul și ordinea de gestionare a materialelor menționate, este necesar de specificat un termen concret, reglementat la nivel de lege organică și nu prin act departamental, la expirarea căruia se purcede la distrugerea propriu-zisă a rezultatelor efectuării măsurilor informative/contrainformative, fie în decursul căruia, după clasarea dosarului informativ/contrainformativ, sunt distruse acestea. Totodată, se va prevedea controlul legalității măsurilor întreprinse de Serviciul de Informații și Securitate al Republicii Moldova până la distrugerea materialelor considerate irelevante,</p> <p>La art. 11 Comisia de la Veneția a menționat că prevederile acestuia de delegare oferă o vastă reglementare a unor aspecte specifice prin acte departamentale ale Serviciului. În opinia Curții Europene a Drepturilor Omului, este crucial ca aspectele care presupun amestecul în exercitarea drepturilor omului să fie stabilite în legea formală. Curtea a considerat că deși procedurile detaliate și condițiile care trebuie respectate nu este necesar să fie incorporate în dreptul substanțial, „o lege care oferă putere de discreție trebuie să indice obiectul acelei puteri” și ar fi contrar statului de drept ca o discreție legală să ia expresia unei puteri nelimitate. „În consecință, legea trebuie să indice obiectul unei atare discreții acordate autorităților competente și modalitatea exercitării acesteia cu suficientă claritate, luând în considerare scopul legitim al măsurii respective, pentru a-i oferi persoanei protecția cuvenită împotriva amestecului arbitrar” (a se vedea pct. 22 din Avizul Comisiei de la Veneția).</p>
<p><b>Nu se acceptă.</b></p> <p>În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică a fost abordat în detaliu subiectul respectiv și s-a ajuns la concluzia de a păstra norma în redacția propusă.</p>	
<p><b>Se acceptă parțial.</b></p> <p>Aceste aspecte au fost discutate în cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică și s-a expus articolul 10 într-o nouă redacție, care soluționează problemele abordate în aviz.</p>	
<p><b>Precizare.</b> În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică aceste aspecte au fost discutate și a fost argumentată necesitatea menținerii articolului în redacția propusă.</p>	

La art. 12 referitor la măsurile conținutative efectuate cu autorizarea directorului Serviciului de Informații și Securitate, Comisia de la Veneția, a menționat că norma indicată prevede un număr mare de măsuri care, în mod vădit, aduc atingere drepturilor fundamentale pot fi aplicate la simpla autorizare a Directorului Serviciului de Informații și Securitate, fără condiții de necesitate sau proporționalitate, fără control judiciar sau alte forme de control extern, nici ex ante nici ex post, fără obligația de a informa persoana vizată, chiar și după încheierea operațiunii și fără limitări clare sau cerințe privitoare la modalitățile de aplicare.

O atare putere discreționară nu corespunde certitudinii juridice, proporționalității și dreptului de acces la instanță și este vădit contrară supremăției legii, unul dintre principiile de bază ale societății democratice (pct. 23 din Avizul Comisiei de la Veneția).

La pct. 48 din Avizul Comisiei de la Veneția se menționează că măsurile conținutative care pot fi efectuate cu autorizarea exclusivă a Directorului Serviciului constituie o ingerință gravă în dreptul la viață privată (a se vedea, în special, ancheta sub acoperire, sau urmărirea vizuală și urmărirea prin sistemul global de poziționare). Comisia de la Veneția a reamintit că, potrivit jurisprudenței Curții Europene a Drepturilor Omului, este, în principiu, de dorit să se încredințeze controlul de supraveghere unui judecător; în mod alternativ, supravegherea de către organele nejudiciare poate fi considerată compatibilă cu Convenția, cu condiția ca organul de supraveghere să fie independent de autoritățile care efectuează supravegherea și să fie învestit cu puteri și competențe suficiente pentru a exercita un control eficient și continuu.

Prin urmare, Comisia de la Veneția a subliniat necesitatea de a asigura un control de supraveghere de către un judecător sau un organism independent.

Revizuirea și supravegherea măsurilor informative trebuie să existe la trei etape: înainte de acțiune (autorizare ex ante), în timpul acțiunii (supraveghere continuă) și după finalizarea acțiunii (control ex post) (a se vedea pct. 49 din Avizul Comisiei de la Veneția).

La art. 12, menționăm că, în conformitate cu prevederile propuse în proiectul de lege pentru modificarea unor acte normative (privind activitatea specială de investigații) (inițiativa legislativă nr. 451 din 08.12.2022), care, în prezent, se examinează de către Parlamentul Republicii Moldova și urmează a fi promovat în viitorul imediat următor, varietățile măsurilor speciale de investigații sunt altele decât cele stipulate în proiectul de lege privind activitatea conținutativă și activitatea informativă externă (inițiativa legislativă nr. 422 din 17.11.2022), deși natura măsurilor speciale de

## Se acceptă.

Articolul 12 alineatul (1) punctele 1) și 2) au fost modificate și stabilesc expres care măsuri conținutative sunt autorizate de către directorul sau directorul adjuncț special împuternicit ai Serviciului și care sunt autorizate de către judecător, fiind practic toate măsurile autorizate prin mandat judecătoresc, cu o singură excepție.

Urmează a se ține cont de faptul că acest aspect a fost discutat în detaliu în cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică și s-a decis redarea normelor în formula respectivă.

investigații și a măsurilor contrainformative este similară sau chiar identică, despre ce vorbește și faptul că unele măsuri contrainformative coincid sută la sută cu unele măsuri speciale de investigații fapt ce în practică ar putea trezi neclarități. Așadar, în corespundere cu dispozițiile art. 27 alin. (1) pct. 1)-3) din Legea nr. 59/2012 privind activitatea specială de investigații, în redacția propusă în proiectul de lege, în afara procesului penal pot fi efectuate următoarele măsuri speciale de investigații:

„1) cu autorizarea judecătorului de instrucție la demersul procurorului:

- a) supravegherea tehnică;
  - b) interceptarea și înregistrarea comunicărilor și/sau imaginilor;
  - c) reținerea, cercetarea, predarea sau ridicarea trimerilor poștale;
  - d) monitorizarea sau controlul tranzacțiilor financiare și/sau accesul la informațiile financiare;
  - e) colectarea de informații de la furnizorii de servicii de comunicații electronice;
  - f) accesarea, interceptarea și înregistrarea datelor informatice;
- 2) cu autorizarea procurorului la demersul conducătorului subdiviziunii specializate:
    - a) identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice ori al unui punct de acces la un sistem informatic;
    - b) achiziția de control;
    - c) investigația sub acoperire;
    - d) colectarea mostrelor pentru cercetarea comparată;
  - 3) cu autorizarea conducătorului subdiviziunii specializate la demersul ofiterului de investigații:
    - a) cercetarea obiectelor și documentelor;
    - b) urmărirea vizuală;
    - c) culegerea de informații.”

În acest context, subliniem că proiectul de lege pentru modificarea unor acte normative (privind activitatea specială de investigații) (inițiativa legislativă nr.451 din 8 decembrie 2022) a fost elaborat cu participarea membrilor grupului de lucru printre care ofițeri de investigații, ofițeri de urmărire penală, procurori, judecători, avocați, reprezentanți ai societății civile și doctrinari ai mediului academic, inclusiv colaboratori ai subdiviziunilor specializate care exercită activitate specială de investigații și colaboratori ai organelor de urmărire penală constituite în cadrul Ministerului Afacerilor Interne (inclusiv în cadrul autorităților din subordine – Inspectoratul General al Poliției, Inspectoratul General al Poliției de Frontieră, Serviciului Protecție Internă și Anticorupție, Biroului Migrație și Azil etc.), Ministerului

Apărării, Centrului Național Anticorupție, Serviciului Fiscal de Stat, Serviciului Vamal, Serviciului de Protecție și Pază de Stat și Administrației Naționale a Penitenciarelor, dar și în cadrul Serviciului de Informații și Securitate.

Varietățile și esența măsurilor speciale de investigații prevăzute de proiectul de lege prenotat, precum și atribuirea competenței autorizării efectuării acestora diferitor subiecți reprezentă, mai mult sau mai puțin, rezultatul unui consens al tuturor membrilor grupului de lucru și reflectă inclusiv poziția reprezentanților Serviciului de Informații și Securitate.

În această ordine de idei, considerăm absolut necesar și insistăm asupra:

1) uniformizării varietăților măsurilor conținutive cu cele ale măsurilor speciale de investigații specificate de proiectul de lege pentru modificarea unor acte normative (privind activitatea specială de investigații) (inițiativa legislativă nr. 451 din 08.12.2022), cu unele excepții; și

2) atribuirii competenței autorizării efectuării măsurilor conținutive prin analogie cu cea a efectuării măsurilor speciale de investigații.

La fel, este relevant că măsura conținutivă „Colectarea de informații de la furnizorii de servicii de comunicații electronice” și măsura conținutivă „Accesul la informațiile financiare sau monitorizarea tranzacțiilor financiare”, care, aparent, reprezintă măsuri inofensive din punct de vedere al ingerințelor aduse în viața privată a persoanei, de fapt, constituie măsuri ce presupun imixțiuni grele în viața privată a persoanei, or, prin intermediul acestora poate fi stabilit întregul profil social (personal și profesional) și financiar al persoanei. Aspectele semnalate dictează necesitatea încredințării competenței de autorizare a respectivelor măsuri unei persoane cu un grad mai înalt de independență decât directorul Serviciului de Informații și Securitate sau procurorul, adică judecătorului de instrucție, în calitate sa de magistrat independent, care dispune de garanții suplimentare în acest sens, așa cum este prevăzut de proiectul de lege pentru modificarea unor acte normative (privind activitatea specială de investigații) (inițiativa legislativă nr. 451 din 08.12.2022).

La art. 12 propunem ca pct. 1) și 2) să fie expuse în următoarele redacții:

- „1) cu autorizarea, prin ordonanță, a directorului Serviciului sau a directorului adjunct special împuternicit al Serviciului: [...]”;

- „2) cu autorizarea, prin încheiere, a judecătorului de instrucție: [...]”.

În redacția propusă în proiectul de lege, la pct. 1) se indică subiectul care autorizează – „directorul Serviciului sau directorul adjunct special împuternicit”, iar la pct. 2) se indică actul prin care se autorizează – „mandatul judecătoresc”.

<p>Astfel, propunem specificarea, atât la pct. 1), cât și la pct. 2), a subiecților competenți să autorizeze efectuarea măsurii contrainformative, precum și a actelor emise de către aceștia în scopul respectiv. Totodată, în sine, mandatul judecătoresc nu reprezintă un act prin care se dispune autorizarea, acesta fiind emis ca supliment la încheierea judecătorească pentru a fi înmănat persoanei supuse măsurii sau terțelor persoane ca dovadă a faptului că ofițerii de investigații/informații posedă autorizația judecătorului de instrucție.</p>	<p>Cu privire la art. 13 alin. (1) pct. 1) lit. c) subliniem că, o asemenea formulare largă ar putea deschide calea pentru încălcarea drepturilor și libertăților fundamentale ale omului. Astfel, pentru a permite efectuarea măsurilor speciale, potentialul risc trebuie să fie legat de o anumită faptă, or, nu există riscuri în lipsa faptelor.</p>	<p>La art. 15, cuvintele „îi pot fi prezentate” din cuprinsul alin. (6) se vor substitui cu cuvintele „i se prezintă”, deoarece redacția actuală lasă loc pentru interpretări. Mai mult, legea trebuie să prevadă expres materialele necesare pentru a fi prezentate judecătorului sau categoria acestora, și conceptual ar putea să se prevadă faptul, că o parte din material nu se anexează la dosar. Însă, chiar și în acest caz, în dosar trebuie să existe mențiuni despre toate materialele care au fost examinate de judecător.</p> <p>În partea ce ține de „nedezvăluirea identității persoanelor”, menționăm că ar fi nejustificabil ca judecătorul să nu cunoască identitatea persoanelor a căror depoziii sunt puse la eliberarea mandatului.</p>	<p>La art. 16 alin. (2) referitor la utilizarea cuvintelor „suspiciuni rezonabile” se va ține cont că Codul de procedură penală operează cu noțiunea de „bănuială rezonabilă”, care potrivit art. 6 subpct. 43 reprezintă suspiciunea care rezultă din existența unor fapte și/sau informații care ar convinge un observator obiectiv că sa comis ori se pregătește comiterea unei infracțiuni imputabile unei anumite ori anumitor persoane și că nu există alte fapte și/sau informații care înlătură caracterul penal al faptei ori dovedesc neimplicarea persoanei.</p>	<p>Norma art. 17 se va revedea în scopul excluderii textului „perioade succesive, precum și perioade care nu se succed”, care este una ambiguă și urmează a fi stabilită cu claritate perioada pentru care se dispune o măsură contrainformativă indiferent de succesiunea acțiunilor întreprinse. Mai mult, prin perioadă se înțelege interval de timp în cursul căruia se desfășoară un fenomen sau se petrece un eveniment.</p> <p>Redacția actuală permite realizarea măsurilor contrainformative în cazul perioadelor care nu se succed, într-un interval de timp care cu siguranță va depăși termenul de 30 zile sau, după caz, 6 luni din data începerii. Astfel,</p>
	<p><b>Se acceptă.</b> Litera c) alineatul (1) al articolul 13 a fost exclus.</p>	<p><b>Se acceptă parțial.</b> În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică problemele respective au fost discutate în detaliu și s-a ajuns la formularea alin. (6) în redacția modificată.</p>	<p><b>Precizare.</b> Alineatul (2) al articolului 16 a fost expus într-o nouă redacție.</p>	<p><b>Nu se acceptă.</b> În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică norma respectivă a fost discutată, astfel încât s-a ajuns la redacția modificată propusă.</p>

<p>norma dată trebuie să stabilească intervalul de timp concret pentru care se autorizează efectuarea măsurilor contrainformative, pentru a exclude abuzurile și ingerința nemotivată în drepturile și interesele legitime ale persoanelor vizate.</p>	<p>La art. 23 referitor la informarea persoanei despre măsurile contrainformative înfăptuite în privința sa, Comisia de la Veneția a atras atenția că, pentru măsuri aprobate de către Directorul Serviciului de Informații și Securitate, nu este prevăzut niciun sistem de notificare a persoanei vizate. Deși recunoscând constatarea Curții Europene a Drepturilor Omului precum că o cale de atac efectivă „trebuie să însemne o cale de atac care este cât se poate de eficientă având în vedere sfera restrânsă de recurs inerentă în orice sistem de supraveghere secretă”, Comisia de la Veneția a reiterat observația conform căreia nu este permisă prevederea posibilității de a nu informa niciodată o persoană vizată cu privire la măsurile speciale. „Persoana vizată ar trebui să fie informată când măsura se încheie, cu excepția cazului în care informațiile ar dăuna (nu doar să afecteze) securității naționale, legat în care ar putea fi prevăzut un sistem de amânări temporare cu un test legat de amenințarea continuă la adresa securității naționale (pct. 51 din Avizul Comisiei de la Veneția).</p> <p>Art. 23 alin. (1) după textul „alin. (1)” se va completa cu textul „pct. 1 și”, dat fiind faptul că persoana trebuie să fie informată și despre măsurile întreprinse în privința ei, autorizate de directorul Serviciului sau directorul adjunct special împuternicit.</p> <p>Recomandăm în cuprinsul art. 23 alin. (3) precizarea faptului cine va aprecia existența motivelor întemeiate enunțate.</p>	<p>La art. 24 (precum și la art. 12 alin. (1) pct. 1) lit. a)), privind măsura „Accesul la informația financiară sau monitorizarea tranzacțiilor financiare”, propunem următorul cuprins:</p>
	<p><b>Se acceptă parțial.</b></p> <p>În cadrul ședințelor grupului de lucru de lucru au fost discutate problemele respective și s-a luat decizia ca practic toate măsurile contrainformative să fie autorizate de către judecător, cu excepția uneia, fapt care va asigura un mecanism de control cu privire la temeinicia efectuării acestora, astfel încât, în redacția propusă în proiect, persoana va fi informată despre efectuarea măsurilor respective în raport cu aceasta, astfel încât, problemele semnalate au fost înlăturate.</p> <p>Suplimentar, a fost prevăzut mecanismul de neinformare din motive întemeiate despre efectuarea măsurilor în privința unei persoane, care din nou a fost asigurat împotriva abuzurilor, prin instituirea mecanismului de control al judecătorului asupra temeiniciei amânării informării, dar cu ulterioara informare.</p> <p>Complementar, cu referire la propunerea ce vizează alineatul (3) al articolului 23, este de notat că aprecierea existenței motivelor întemeiate de neinformare a persoanei, va fi efectuată de către persoana care întocmește raportul, fapt prevăzut la alineatul (4). Acest raport, ulterior, va fi supus unui mecanism dublu de control, din partea directorului Serviciului și ulterior din partea judecătorului.</p>	<p><b>Se acceptă.</b></p> <p>Propunerea expusă a fost luată în considerare la redactarea normei</p>

<p>prevăzute la art. 24 din proiectul de lege.</p>	<p><b>„Articolul 24.</b> Monitorizarea sau controlul tranzacțiilor financiare și/sau accesul la informațiile financiare</p> <p>Monitorizarea sau controlul tranzacțiilor financiare și/sau accesul la informațiile financiare reprezintă operațiunile prin care se asigură cunoașterea conținutului tranzacțiilor financiare, în regim de timp real sau după realizarea acestora, efectuate de către persoanele fizice și juridice prin intermediul băncilor sau al altor persoane/organizații care intermediază tranzacțiile financiare ori obținerea de la entitățile respective a înscrisurilor sau a informațiilor aflate în posesia acestora referitoare la depunerile, conturile sau tranzacțiile unei persoane.”</p> <p>Remarcăm că redenumirea măsurii contrainformative respective, precum și reglementarea unui alt cuprins al acesteia rezidă în faptul că efectuarea acesteia presupune trei operațiuni distincte, după cum urmează:</p> <ol style="list-style-type: none"> <li>1) monitorizarea tranzacțiilor financiare, care constă în cunoașterea conținutului tranzacțiilor financiare în regim de timp real;</li> <li>2) controlul tranzacțiilor financiare, care constă în cunoașterea conținutului tranzacțiilor financiare ulterior realizării acestora; și</li> <li>3) accesul la informațiile financiare, care constă în solicitarea și obținerea informațiilor și documentelor cu privire la conturile/tranzacțiile persoanelor.</li> </ol> <p>La fel, atenționăm că noțiunea „instituții financiare” este depășită pentru că reglementările Legii instituțiilor financiare nr. 550/1995 au fost substitute cu reglementările Legii nr. 202/2017 privind activitatea băncilor, cea dintâi lege organică fiind redenumită în Legea nr. 550/1995 cu privire la lichidarea băncilor, conținând, la momentul actual, doar normele juridice care reglementează procedura de lichidare a băncilor.</p>
<p><b>Se acceptă.</b></p> <p>Măsura contrainformativă prevăzută la art. 26 din proiectul de lege va fi autorizată prin mandatul judecătoresc, fiind operate modificări în acest sens.</p>	<p>La art. 26 (precum și la art. 12 alin. (1) pct. 1) lit. c)), privind măsura „Urmărirea vizuală și/sau documentarea cu ajutorul metodelor și mijloacelor tehnice, precum și localizarea sau urmărirea prin sistemul de poziționare globală ori prin alte mijloace tehnice”, menționăm că aceasta reprezintă o combinație între măsura „Urmărirea vizuală” (art. 1346 din Codul de procedură penală), care se autorizează de către procuror și măsura „Documentarea cu ajutorul metodelor și mijloacelor tehnice, precum și localizarea sau urmărirea prin intermediul sistemului de poziționare globală (GPS) ori prin alte mijloace tehnice” (1343 din Codul de procedură penală), care se autorizează de către judecătorul de instrucție.</p> <p>Notăm că, efectuarea documentării cu ajutorul metodelor și mijloacelor tehnice este atribuită în competența judecătorului de instrucție la autorizare, iar efectuarea urmării vizuale este atribuită în competența procurorului la autorizare deoarece, deși ambele presupun relevarea și fixarea acțiunilor</p>

<p>persoanelor, imobilelor, mijloacelor de transport și a altor obiecte, în primul caz acestea pot fi reproduse datorită utilizării aparatelor tehnice de înregistrare, astfel încât gravitatea ingerințelor în viața privată a persoanei este sporită, iar în al doilea caz acestea nu pot fi reproduse datorită folosirii doar a organelor vizuale ale omului. Unificarea celor două măsuri într-o singură măsură contrainformativă și atribuirea acesteia în competența directorului Serviciului de Informații și Securitate la autorizare nu este proporțională cu imixtiunea admisă în viața privată a persoanei.</p>	<p>La art. 36 (precum și la art. 12 alin. (1) pct. 2) lit. a)), privind măsura „Cercetarea domiciliului și/sau, după caz, instalarea în el a aparatelor ce asigură supravegherea audio, video, de fotografiat, de constatare a unor situații de fapt, cu sau fără efectuarea înregistrărilor”, menționăm că aceasta comportă cea mai gravă imixtiune în viața privată a persoanei. Notăm că, în conformitate cu prevederile proiectului de lege pentru modificarea unor acte normative (privind activitatea specială de investigații), această măsură (specială de investigații, analoagă celei contrainformative) nu poate fi dispusă și efectuată în afara procesului penal, deoarece este prea intruzivă. Prin urmare, insistăm asupra excluderii acesteia din proiectul de lege privind activitatea contrainformativă și activitatea informativă externă (inițiativa legislativă nr. 422 din 17.11.2022). În același registru, evidențiem că, în ipoteza în care ar exista suficiente temeiuri factice pentru dispunerea și efectuarea respectivei măsuri în afara procesului penal, cel mai probabil, bănuiala rezonabilă cu privire la pregătirea sau la săvârșirea unei infracțiuni ar fi conturată demult, astfel încât ar fi posibilă inițierea cauzei penale prin începerea urmăririi penale și cercetarea domiciliului și/sau instalarea în el a aparatelor ce asigură fotografierea sau supravegherea și înregistrarea audio și video în cadrul procesului penal.</p>
	<p><b>Nu se acceptă.</b> În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică a fost discutată problematica respectivă și s-a demonstrat necesitatea existenței măsurii contrainformative respective, articolul 36 fiind supus unor modificări.</p>

<p><b>Nu se acceptă.</b> Măsura contrainformativă în redacția propusă în aviz diferă de scopul măsurii reglementate la art. 37, or, în sensul normei propuse în proiectul de lege, se urmărește scopul de a supraveghea din exterior și a obține date și informații despre situațiile care se petrec în interiorul domiciliului, și nicidecum în exteriorul acestuia. În redacția propusă în aviz, scopul urmărit ar fi asimilat cu scopul măsurii contrainformative – urmărirea vizuală, iar prin art. 37 s-a intenționat obținerea altor rezultate, prenotate.</p>	<p><b>Se acceptă.</b> Măsura contrainformativă prevăzută la art. 27 din proiectul de lege a fost exclusă.</p>	<p><b>Precizare.</b> În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică a fost abordat în detaliu subiectul respectiv, ajungându-se la un consens în acest sens inclusiv cu operatorii. Respectiv, optăm pentru menținerea formulării propuse.</p>
<p>La art. 37 (precum și la art. 12 alin. (1) pct. 2) lit. b)), privind măsura „Supravegherea domiciliului prin utilizarea mijloacelor tehnice cu sau fără efectuarea înregistrărilor”, propunem următorul cuprins: „<b>Articolul 37.</b> Supravegherea tehnică Supravegherea tehnică reprezintă utilizarea mijloacelor tehnice pentru relevarea și fixarea cronologică a acțiunilor/inacțiunilor, poziționărilor, mișcărilor și contactelor (legăturilor) persoanelor, supravegherea imobilelor, urmărirea și localizarea mijloacelor de transport și a altor obiecte.” Remarcăm că supravegherea domiciliului prin utilizarea mijloacelor tehnice ce asigură înregistrarea (art. 1327 din Codul de procedură penală) și documentarea cu ajutorul metodelor și mijloacelor tehnice, localizarea sau urmărirea prin sistemul de poziționare globală (GPS) ori prin alte mijloace tehnice (art. 1343 din Codul de procedură penală) implică procedee, metode și tehnici de aceeași natură, precum și utilizarea mijloacelor tehnice, inclusiv speciale, de același fel. Din aceste considerente, pledăm pentru optimizarea prin comasare și reglementare unitară a măsurilor respective.</p>	<p>Prevederile art. 39 se vor analiza prin prisma art. 135 din Codul de procedură penală nr. 122/2003, care presupune că controlul transmiterii banilor sau a altor valori materiale extorcate poate fi efectuat doar de către organele de urmărire penală ale Ministerului Afacerilor Interne și de Centrul Național Anticorupție. De altfel, controlul transmiterii banilor sau a altor valori materiale se efectuează în cadrul urmăririi penale ca măsură specială de investigații, și nu este clară necesitatea efectuării aceluiași măsură în cadrul activității informative sau contrainformative. Mai mult, scopul proiectului dat este delimitarea măsurilor speciale de investigație efectuate de organele de urmărire penală de cele informative sau contrainformative efectuate de Serviciu.</p>	<p>La art. 40 (precum și la art. 12 alin. (1) pct. 2) lit. d)), privind măsura „Accesul la informația ce se află sau se prelucrează într-un sistem informațional și/sau monitorizarea acesteia cu sau fără efectuarea înregistrărilor”, propunem următorul cuprins: „<b>Articolul 40.</b> Accesarea, interceptarea și înregistrarea datelor informatice Accesarea și/sau interceptarea datelor informatice constă în folosirea unor metode și/sau mijloace tehnice pentru obținerea datelor informatice stocate pe un suport informațional, fără înștiințarea proprietarului sau utilizatorului acestuia și/sau pentru colectarea în timp real a datelor informatice asociate comunicărilor prin intermediul unui sistem informatic, iar înregistrarea datelor informatice constă în stocarea informațiilor obținute în urma accesării</p>

	<p>și/sau interceptării pe un suport informațional.”</p> <p>Informațiile traficate prin intermediul rețelelor de comunicații electronice, cele ce se regăsesc într-un sistem informațional și cele care sunt stocate pe un suport magnetic nu constituie altceva decât date informatice, în caz de necesitate, acestea urmând a fi accesate, interceptate și înregistrate de către reprezentanții organelor de drept.</p>
<p><b>Se acceptă.</b></p> <p>Măsura contrainformativă prevăzută la art. 41 din proiectul de lege va fi autorizată prin mandatul judecătoresc, care va examina temeinicia efectuării acesteia, și ulterior legalitatea.</p>	<p>La art. 41 Comisia de la Veneția la pct. 54 din aviz a menționat că, 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, Serviciul de Informații și Securitate 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 măsură necesită un mandat judiciar, dacă Serviciul de Informații și Securitate 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.</p> <p>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.</p>
<p><b>Se acceptă.</b></p> <p>Au fost operate modificările necesare, iar alineatul (5) a fost exclus.</p>	<p>La art. 46 alin. (4) prin prisma prevederilor art. 54 din Legea nr. 100/2017 urmează a fi revăzute prevederile în vederea eliminării tuturor ambiguităților.</p> <p>Astfel, din prevederile punctului menționat nu este clar care sunt „instituțiile Republicii Moldova de peste hotare”, or, potrivit dispozițiilor Legii nr. 761/2001 cu privire la serviciul diplomatic, reprezentarea Republicii Moldova în relațiile ei cu alte state și cu organizațiile internaționale este realizată de către misiunile diplomatice, inclusiv reprezentanțele permanente de pe lângă organizațiile internaționale, delegațiile și misiunile ad-hoc și oficiile consulare (obiecție valabilă și pentru art. 46, pct. 5) din proiect).</p> <p>De asemenea, este echivoc textul „misiunilor și reprezentanțelor diplomatice externe ...”, precum și cetățenilor aflați peste hotarele republicii” întrucât această formulare poate fi interpretabilă și duce în eroare.</p>
<p><b>Nu se acceptă.</b></p> <p>Considerăm oportună menținerea normei în redacția propusă, pentru a nu afișa în legea bugetară anuală a sumei care necesită a fi alocată pentru activitatea</p>	<p>La art. 50 alin. (1) din proiect urmează a fi expus în următoarea redacție:  „Desfășurarea activităților informative/contrainformative se realizează din contul și în limita alocațiilor bugetare aprobate în acest sens prin legea bugetară anuală, precum și din alte surse în modul stabilit de legislație”.</p>

<p>informativă/ contrainformativă.</p> <p><b>Nu se acceptă.</b></p> <p>Considerăm oportun a fi specificate datele respective, pentru a spori certitudinea în raportul de constatare tehnico-științifică, nefiind un aspect negativ.</p>	<p><b>Se acceptă.</b></p> <p>Au fost operate modificările necesare, astfel încât au fost luate în considerare obiectivele înaintate. Complementar, art. 56 din proiectul de lege a fost exclus în totalitate.</p>
<p>La art. 54 alin. (6) lit. b) nu considerăm justificat ca raportul de constatare tehnico-științifică să conțină date cu privire la studiile sau calificările deținute de specialist pentru efectuarea cercetărilor, precum și experiența în domeniu, deoarece specialistul trebuie să aibă studii în domeniu, pregătirea respectivă în domeniu și să fi obținut calificarea de specialist. În acest context, această prevedere devine inutilă.</p>	<p>La art. 55 alin. (2) referitor la prevederea că prelucrarea datelor cu caracter personal în cadrul activității informative/contrainformative nu constituie obiectul legislației privind protecția datelor cu caracter personal, Comisia de la Veneția a menționat că, abordarea ar trebui să fie mai degrabă inversă, legislația privind protecția datelor fiind regula, cu excepții restrâns definite. Comisia de la Veneția a reamintit, de asemenea, că, potrivit jurisprudenței Curții Europene a Drepturilor Omului, nerespectarea ordinului unei autorități de protecție a datelor/libertății informațiilor de a dezvălui informații de către o agenție de informații conduce la încălcarea art. 6 și 10 ale CEDO (pct. 60 din Avizul Comisiei de la Veneția).</p> <p>Art. 55 și 56 necesită a fi aduse în concordanță cu prevederile art. 15 din Legea nr. 133/2011 privind protecția datelor cu caracter personal. Astfel, prelucrarea datelor cu caracter personal de către Serviciu se va realiza cu respectarea normelor Legii nr. 133/2011, iar reglementarea prin prezentul proiect a prelucrării și protecției datelor respective se va limita doar la acele situații care sunt indicate ca excepții de la regulile generale stabilite prin art. 15 al legii prenotate.</p> <p>De asemenea, la art. 55 recomandăm completarea acestuia cu reglementarea/constituirea unui mecanism care ar statua procedura de urmat în cazul în care Centrul pentru Protecția Datelor cu Caracter Personal constată anumite operațiuni de prelucrare a datelor cu caracter personal efectuate în cadrul activităților reglementate de această lege. În acest caz apare întrebarea logică care entitate va prelua controlul legalității acestor operațiuni și în care circumstanțe, precum și ce măsuri urmează a fi întreprinse de Centru. În acest context, ar fi necesară instituirea unui mecanism legal de colaborare între Centru, Procuratura Generală și Serviciul de Informații și Securitate, în special în situațiile în care activitatea de control efectuată de Centru se intersectează cu activitățile efectuate de Serviciul de Informații și Securitate ce vizează operațiunile de prelucrare a datelor cu caracter personal, precum și reieșind din norma care statuează că activitatea reglementată de proiect poate fi efectuată și public.</p> <p>La cap. VI „Controlul Activității Informative/Contrainformative” se va ține</p>
	<p><b>Se acceptă.</b></p>

<p>Articolul 57 a fost completat cu alineatele (7) și (8) care soluționează problemele semnalate.</p> <p>Complementar, odată ce Subcomisia parlamentară stabilește anumiți indici de suspiciune că au fost săvârșite încălcări grave în activitatea Serviciului, aceasta poate sesiza Procurorul General, care la rândul său va întreprinde acțiuni ce se impun.</p>	<p>cont de prevederile pct. 71 din Avizul Comisiei de la Veneția.</p> <p>În cadrul controlului parlamentar, Serviciul de Informații și Securitate ar trebui să fie obligat să furnizeze toate datele privind numărul și tipurile de măsuri efectuate, iar Subcomisiei ar trebui să i se solicite să publice un raport anual cu privire la aceste date statistice. Subcomisia ar trebui să poată emite un raport special pentru a atrage atenția publicului și Parlamentului asupra activităților care necesită un răspuns urgent. Ar trebui luată în considerare și posibilitatea de a iniția anchete parlamentare, care ar putea rezulta în anchete judiciare, atunci când există suspiciuni de nereguli grave, supuse unor cerințe de securitate a statului.</p> <p>În plus, Comisia de la Veneția a reamintit recomandarea sa anterioară de a completa sau înlocui „sistemul actual de supraveghere parlamentară cu o anumită formă de organ independent de supraveghere/contestare”.</p> <p>Referitor la controlul din partea procurorilor, Comisia de la Veneția a menționat că, controlul efectuat de procurori ar trebui să fie relevant doar în materie penală. Serviciul de informații și Securitate nu ar trebui să aibă o putere absolută în acordarea dreptului de acces la secretul de stat procurorilor însărcinați cu controlul activităților Serviciului de Informații și Securitate. Informațiile privind organizarea, formele, tacticile, metodele și mijloacele de funcționare ale Serviciului de Informații și Securitate nu ar trebui excluse din vizorul controlului procurorilor, dacă implică o răspundere penală.</p> <p>Cât privește controlul judiciar, Comisia de la Veneția a menționat că, pentru măsurile supuse mandatului judiciar, ar trebui revizuită prevederea care stipulează că un judecător nespecializat decide de sine stătător, în scurt timp, asupra unor chestiuni extrem de complexe. Măsurile prevăzute la art. 12 alin. (1) subpct. 1) ar trebui supuse automat controlului judiciar efectiv, cu excepția cazurilor justificate corespunzător stabilite de lege. În plus, controlul legalității <i>ex post</i> prevăzut la art. 60 din proiectul de lege privind activitatea informativă ar trebui revizuit pentru a deveni efectiv.</p>	<p><b>Precizare.</b> În redacția actuală, este indicat că legea intră în vigoare după 90 de zile de la data publicării acesteia în Monitorul Oficial al Republicii Moldova.</p>
<p>La art. 61 alin. (1) menționăm că norma repetă regula generală de intrare în vigoare a actelor normative stipulată la art. 56 alin. (1) din Legea nr. 100/2017, potrivit căreia, actele normative intră în vigoare peste o lună de la dat publicării în Monitorul Oficial al Republicii Moldova sau la data indicată în textul actului normativ, care nu poate fi anterioară datei publicării.</p> <p>În același timp, atragem atenția că proiectul de lege privind activitatea contrainformativă și activitatea informativă externă nu prevede exceptarea de la efectuarea măsurilor contrainformative împotriva avocaților în exercitarea profesiei și, implicit, nu stabilește interdicția de a efectua măsuri contrainformative cu privire la raporturile legale de asistență juridică dintre</p>	<p><b>Se acceptă.</b></p> <p>Proiectul a fost completat și incluse prevederile literei b)¹ al alineatului 5 și literei a) al alineatului (7)¹ ale articolului 15 din proiectul de lege, care oferă o</p>	

<p>reglementare în partea ce vizează raporturile de asistență juridică dintre avocat și clientul acestuia, în procesul de autorizare și efectuare a măsurilor contrainformative.</p>	<p>avocat și clientul său. La fel, proiectul nu prevede interdicția de a cerceta biroul sau domiciliul avocatului în exercitarea profesiei și/sau, după caz, instalarea în ele a aparatelor ce asigură supravegherea audio, video, de fotografiat, de constatare a unor stări de fapt, cu sau fără efectuarea înregistrărilor, precum și interdicția de a stenografia comunicările dintre avocat și persoana pe care o apără. Acest fapt pune în pericol grav garantarea independenței exercitării profesiei de avocat, consfințită la art. 52 și 53 din Legea nr. 1260/2002 cu privire la avocatură și la art. 26 alin. (4) din Constituția Republicii Moldova.</p>
<p><b>Se acceptă.</b></p>	<p><b>Pe plan redacțional în raport cu normele de tehnică legislativă, comunicăm următoarele.</b></p> <p>Se va ține cont că prevederile generale privind survenirea răspunderii poartă un caracter declarativ și necesită a fi excluse. Răspunderea juridică trebuie să fie prevăzută de normele materiale ce stabilesc tipul concret de răspundere (penală sau contravențională), determină faptele și sancțiunile pentru comiterea acestora.</p>
<p><b>Se acceptă.</b></p>	<p>La art. 15 se vor revizui trimerile de la alin. (12), (16) și (19). Obiecție valabilă și la art. 23 alin. (5) și la art. 61 alin. (2).</p>
<p><b>Se acceptă.</b></p>	<p>Referința la actul normativ se va expune conform prevederilor art. 55 alin.(5) din Legea nr. 100/2017 cu privire la actele normative, astfel încât la indicarea datei de adoptare a actului normativ să se indice numărul de ordine, ca element de identificare, la care să se adauge anul în care a fost adoptat, aprobat sau emis acesta, fiind despărțite de o bară „/”.</p>
<p><b>Se acceptă.</b></p>	<p>Numerotarea secțiunilor se va revizui prin prisma prevederilor art. 53 alin.(1) lit. a) din Legea nr. 100/2017.</p>
<p><b>Se acceptă</b></p>	<p>Relevăm necesitatea redactării textului prin excluderea acronimului „etc.”, deoarece semnificația acestuia este periculoasă sub aspect de interpretare extensivă.</p>
<p><b>Se acceptă</b></p>	<p>Din sintagma „legislația în vigoare”, cuvintele „în vigoare” se vor exclude, ca fiind inutile. Regula generală este că referințele la actele normative prezintă referințe la legislația în vigoare și doar pentru excepțiile de la regulă se va specifica dacă este vorba despre legislația aplicabilă la un anumit moment.</p>
<p>Se acceptă în limita admisibilă. Obiecțiile și propunerile neacceptate au fost contraargumentate.</p>	<p>În sensul celor enunțate mai sus, proiectul Legii privind activitatea contrainformativă și activitatea informativă externă se susține cu condiția că urmează a fi luate în considerare obiecțiile, propunerile și recomandările menționate <i>supra</i>.</p>

	<p>Normele art. 6 alin. (8) și alin. (9) reglementează unele garanții sociale acordate persoanelor care și-au exprimat consimțământul scris de a colabora cu Serviciul.</p>	<p><b>Precizare.</b> Articolul 6 din proiectul de lege a fost exclus.</p>
<p><b>Centrul de la Geneva pentru Guvernarea Sectorului de Securitate – DCAF</b></p>	<p>1. Cele două proiecte de lege <b>necesită o analiză mai atentă și o modificare aprofundată</b> pentru a asigura fundamentul juridic al unui serviciu de informații și de securitate care este (1) <b>eficient în descurajarea amenințărilor la adresa securității naționale și (2) responsabil în mod democratic în îndeplinirea misiunii sale.</b></p> <p>2. Cele două proiecte de lege sunt complexe și <b>prea ambițioase în ceea ce privește definirea competențelor SIS și a responsabilităților operaționale, dar oferă puține detalii și dispoziții clare privind controlul și supravegherea.</b></p> <p>4. Ambele proiecte de lege atât supra detaliate, cât și complicate și totuși vagi cu privire la unele dintre cele mai importante aspecte. Niciuna dintre legi nu reflectă legi similare în democrațiile europene în care legile sunt simple (rareori peste 6 pagini), mai puțin detaliate cu privire la activitatea operațională, dar definesc mai detaliat problema importantă a supravegherii în toate formele sale (executivă, parlamentară și judiciară).</p>	<p>Proiectele de lege vizate au parcurs etapa de consultări publice, fiind îmbunătățite semnificativ ca urmare a dezbatărilor din cadrul grupului de lucru de pe lângă Comisia parlamentară securitate națională, apărare și ordin publică.</p> <p><b>Se acceptă.</b> Proiectele conțin prevederi privind controlul exercitat de către parlament, procuror și instanțele judecătorești. Totodată, în cadrul grupului de lucru de pe lângă Comisia Securitate Națională, Apărare și Ordin publică s-a revăzut proiectul prin prisma eficacității mecanismelor de control și supraveghere a activității conținutive.</p>
	<p>5. Decizia de a elabora <b>2 legi separate</b> (de asemenea, o a treia lege privind rolul ofițerului de informații) ar trebui analizată în continuare, împreună cu posibilitatea de a combina proiectele într-o singură lege. O lege unică ar evita repetițiile, ar oferi o mai mare claritate și ar fi un singur punct de referință. Dacă se păstrează două legi, trebuie asigurată claritatea și armonizarea, în special în ceea ce privește sarcinile și competențele serviciului.</p> <p>14. Capitoul III din Legea CI ar trebui să ia în considerare în continuare implicațiile operațiilor externe, legalitatea acestora și implicațiile pentru ofițerii individuali. Proiectul nu ia în considerare ofițerii SIS care comit acte ilegale (cum ar fi mita) atunci când își desfășoară activitatea în străinătate. Acest lucru ar face ca ofițerii SIS să fie urmăriți penal nu numai în țări străine, ci și în Moldova, dacă legislația moldovenească este extraterritorială, adică fapta este pasibilă de urmărirea penală a unui cetățean moldovean în Republica Moldova, chiar dacă este comisă în străinătate. Alte servicii similare evită acest lucru prin anumite părți ale legislației lor. De exemplu, în Regatul Unit, acest lucru este reglementat de secțiunea 7 din ISA, unde este necesară aprobarea ministerială pentru a încălca legea în străinătate, dar oferă o</p>	<p><b>Nu se acceptă.</b> Argumentul nu poate fi reținut dat fiind faptul că, ambele proiecte au domenii de reglementare distincte/separate. Respectiv, adoptarea concomitentă a ambelor legi este indispensabilă.</p> <p>Versiunea redactată corespunde celor stabilite de către grupul de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică. Totodată reglementări detaliate privind statutul juridic (inclusiv cu răspunderea juridică) al ofițerilor SIS se regăsesc în Legea nr. 170/2007 privind statutul ofițerului de informații și securitate.</p>

<p>imunitate efectivă de urmărire penală în Regatul Unit. În SUA, acest lucru se încadrează în diferite decrete prezidențiale.</p> <p>15. Proiectele de legi tac cu privire la multe aspecte care implică răspunderea (penală) a ofițerilor. Câteva exemple sunt cazurile de influențare, susținere sau adoptare a unor decizii contrare interesului național; ordine ilegale, degradarea sau distrugerea resurselor economice de interes național. De asemenea, nu este clar dacă ofițerii sau colaboratorii pot participa sau contribui la infracțiuni sau pot acționa ca agent provocator. Oligafia privind raportarea infracțiunilor este prea restrânsă – trebuie raportată chiar și infracțiuni minore.</p>	<p>Reglementări detaliate privind statutul juridic (inclusiv cu răspunderea juridică) al ofițerilor SIS se regăsesc în Legea nr. 170/2007 privind statutul ofițerului de informații și securitate. Totodată, eventualele încalcări săvârșite de ofițeri de informații atrag răspunderea juridică în condiții generale, nefiind necesară o normă specială în acest sens.</p> <p><b>Se acceptă.</b></p> <p>Proiectul vizează expres că spocul activității informative/conatrinformative este culegerea de informații pentru prevenirea faptelor ce pot afecta securitatea statului, iar informațiile culese nu pot constitui probe într-o cauză penală.</p>
<p>16. Esența activității de intelligence este <b>colectarea de informații utile</b> în procesul decizional al autorităților statului. Scopul este de a obține cunoștințe fiabile, <b>prevăzătoare despre amenințările și riscurile la adresa securității naționale</b>, în vederea prevenirii și neutralizării acestora. Eficacitatea activității de intelligence este determinată de acuratețea, fiabilitatea și punctualitatea informațiilor furnizate factorilor de decizie și nu de valoarea probatorie a informațiilor colectate.</p> <p>17. Informațiile colectate prin metode acoperite care încalcă drepturile și libertățile omului și, în special, dreptul la viață privată (cum ar fi supravegherea secretă, interceptarea comunicațiilor) sunt menite să furnizeze elemente interioare care să permită serviciului de informații să prevină și să descurajeze amenințările la adresa securității naționale. În majoritatea țărilor europene, serviciile de informații utilizează astfel de metode intruzive de colectare a informațiilor în următoarele circumstanțe:</p> <ul style="list-style-type: none"> <li>➤ Un mandat / un ordin este autorizat de o autoritate externă serviciului</li> <li>➤ Mandatul este emis în afara cadrului procesului penal, deoarece se referă adesea la aspecte care nu fac obiectul evaluării penale; prin urmare, procesul de autorizare este reglementat de alte legi decât Codul de procedură penală (Legea legală a serviciului de informații sau o lege specială privind măsurile speciale de investigare)</li> <li>➤ Cererea de folosire a unor astfel de măsuri poate fi declanșată de standarde / motive de suspiciune mai scăzute decât utilizarea unor măsuri intruzive în cadrul anchetelor penale al căror scop este de a colecta probe privind infracțiunile care au fost deja săvârșite.</li> <li>➤ Fac obiectul unor mecanisme diferite de control și supraveghere față de cele privind agențiile de aplicare a legii: aprobarea directorului de serviciu pentru fiecare solicitare este urmată de un mandat judiciar emis de o curte la nivel înalt sau de o curte specializată; o comisie parlamentară specială de</li> </ul>	<p><b>Se acceptă.</b></p> <p>Versiunea redactată corespunde celor stabilite de către grupul de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică, în cadrul căruia au fost dezbătute și principiile enunțate.</p> <p>Astfel, redacția finală a proiectului prevede un mecanism concret de autorizare a măsurilor contrainformative (de către judecătorul de instrucție) ce constituie imixțiuni serioase în viața privată a persoanei.</p>

<p>supraveghere sau un organism independent de supraveghere să exercite un control post-facto asupra legalității, legitimității și proporționalității acestor măsuri.</p> <p>➤ În majoritatea țărilor europene, procurorul nu joacă un rol în aprobarea mandatului de securitate.</p> <p>➤ Principiile definite de jurisprudența Curții Europene a Drepturilor Omului (cum ar fi legalitatea, necesitatea, legitimitatea, proporționalitatea, subsidiaritatea sau ultima ratio) ar trebui să aibă caracter obligatoriu pentru autoritățile implicate în inițierea, autorizarea și punerea în aplicare a unor metode intruzive – ofițeri de informații, director al serviciului de informații, instanță.</p>	<p>18. Una dintre condițiile fundamentale pentru eficacitatea serviciilor de informații este <b>secretul</b> atât al persoanelor și structurilor, cât și al metodelor, formelor și mijloacelor de desfășurare a activităților desfășurate. În timp ce activitățile de aplicare a legii se desfășoară sub rigoarea mult mai mică a secretului și adesea în condiții de deschidere, menținerea secretului de informații dă naștere la o serie de cerințe legate de organizarea activităților unui astfel de serviciu, atât în țară, cât și în străinătate. Acesta este un alt motiv pentru care ar trebui evitată implicarea personalului de serviciu și a infrastructurii în sarcini care nu sunt de informații.</p>	<p><b>Se acceptă.</b>  Versiunea redactată corespunde celor stabilite de către grupul de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică au fost abordate în detaliu subiectele respective, conceptele date regăsindu-se în textul final al proiectului.</p>
<p>supraveghere independent de supraveghere să exercite un control post-facto asupra legalității, legitimității și proporționalității acestor măsuri.</p> <p>➤ În majoritatea țărilor europene, procurorul nu joacă un rol în aprobarea mandatului de securitate.</p> <p>➤ Principiile definite de jurisprudența Curții Europene a Drepturilor Omului (cum ar fi legalitatea, necesitatea, legitimitatea, proporționalitatea, subsidiaritatea sau ultima ratio) ar trebui să aibă caracter obligatoriu pentru autoritățile implicate în inițierea, autorizarea și punerea în aplicare a unor metode intruzive – ofițeri de informații, director al serviciului de informații, instanță.</p>	<p>19. Ar trebui create garanții eficiente pentru a împiedica serviciile de informații să se implice în activități și în colectarea de informații în alte scopuri decât prevenirea amenințărilor la adresa securității naționale. Un sistem eficient de responsabilizare vizează în principal prevenirea (1) utilizării abuzive a fondurilor statului și (2) a abuzului de putere (cum ar fi ingerința în situația politică, restricționarea libertăților civile, persecutarea cetățenilor, utilizarea ilegală și/sau nejustificată a măsurilor intruzive pentru colectarea de informații și manipularea informațiilor obținute în scopuri contrare atribuțiilor serviciului, inclusiv desfășurarea de activități infracționale de către ofițerii serviciului.</p>	<p><b>Se acceptă.</b>  În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică au fost abordate în detaliu subiectele respective, conceptele date regăsindu-se în textul final al proiectului.</p>

<p>20. Există diferite niveluri de control și supraveghere care contribuie la responsabilizarea serviciilor de informații. Acestea sunt complementare și se consolidează reciproc, astfel încât deficiențele de la un nivel au potențialul de a afecta întregul sistem.</p> <p>21. Sistemele de control intern transpun dispozițiile legale abstracte în instrucțiuni administrative și operaționale "de zi cu zi" și servesc scopului identificării și neutralizării cazurilor de abuz de putere și a altor nereguli din partea personalului de serviciu. Funcționalitatea și eficiența sistemului de control intern ar trebui să facă obiectul unei evaluări de către organismele de control externe. Împreună cu membrii de rang înalt ai SIS, Guvernul și Parlamentul ar trebui să analizeze ce controale interne ar trebui instituite pentru a se asigura că cultura și metodologiile de lucru reflectă normele democratice și societale moldovenești. Controalele și cultura sunt la fel de importante ca și legislația.</p> <p><b>Mecanismele de control intern din cadrul SIS nu sunt suficient de detaliate în cele două proiecte.</b> Responsabilitatea asigurării controlului intern este consacrată în legi (într-un mod laconic și general) ca intrând în subordinea directorului SIS (Legea SIS art.18 i) și a legii CI art. 59), însa ambele legi tac asupra principiilor de stabilire și funcționare a mecanismelor de control intern. Proiectele de lege nu menționează modul în care directorul ar trebui să îndeplinească această responsabilitate și modul în care sistemul de control intern va fi supravegheat de executiv și legislativ. Legea ar trebui să dea în mod specific directorului responsabilitatea de a stabili orientări etice în cadrul serviciului care să reflecte valorile societății moldovenești.</p>	<p><b>Se acceptă.</b></p> <p>Proiectele conțin prevederi privind controlul exercitat de către parlament, procuror și instanțele judecătorești.</p> <p>Totodată, în cadrul grupului de lucru de pe lângă Comisia Securitate Națională, Apărare și Ordin publică s-a revăzut proiectul prin prisma eficacității mecanismelor de control și supraveghere a activității contrainformative.</p>
<p>22. Mecanismele de control intern din cadrul SIS nu sunt suficient de detaliate în cele două proiecte. Responsabilitatea asigurării controlului intern este consacrată în legi (într-un mod laconic și general) ca intrând în subordinea directorului SIS (Legea SIS art.18 i) și a legii CI art. 59), însa ambele legi tac asupra principiilor de stabilire și funcționare a mecanismelor de control intern. Proiectele de lege nu menționează modul în care directorul ar trebui să îndeplinească această responsabilitate și modul în care sistemul de control intern va fi supravegheat de executiv și legislativ. Legea ar trebui să dea în mod specific directorului responsabilitatea de a stabili orientări etice în cadrul serviciului care să reflecte valorile societății moldovenești.</p> <p>23. Legea ar trebui completată cu dispoziții clare care să definească obiectivul, domeniul de aplicare, mecanismele, normele sistemului de control intern, precum și formele și mijloacele de atingere a obiectivului. Controlul intern ar trebui să fie un sistem integrat în procesul de gestionare a serviciului la toate nivelurile. Activitățile subunității de control intern [articolul 59 alineatul (1)] sunt doar o parte a așa-numitului control instituțional intern. Parte a sistemului de control intern sunt, de asemenea, instrumente de control operațional, cum ar fi deciziile directorului de a autoriza măsuri de contrainformații (articolul 14) și activitatea de informații externe (articolul 49).</p> <p>24. Mecanismele de control intern clare și puternice sunt o condiție prealabilă esențială a auto-reținerii în utilizarea metodelor intruzive. Prin urmare, ar trebui să se acorde o atenție deosebită elaborării statutului, reglementărilor, standardelor profesionale, codurilor de conduită și formării personalului, în urma adoptării pachetului legislativ.</p>	<p><b>Se acceptă.</b></p> <p>Scopul, domeniul de reglementare, procedura de autorizare a măsurilor contrainformative și controlul intern au fost revăzute și reformulate expres în art. 1, 12, 59.</p>

<p><b>Se acceptă.</b> Normele prevăzute la art. 10 și art. 56 alin. (2) au fost excluse.</p> <p><b>Nu se acceptă.</b> SIS nu este supus controlului executiv, fiind o autoritate administrativă autonomă (nefiind în subordinea organului executiv central).</p>	<p>25. Dispoziția privind distrugerea materialelor care s-au dovedit a fi irelevante pentru cazul investigat este confuză și contrară principiilor controlului intern [articolul 10 și articolul 56 alineatul (2) din legea CI].</p> <p><b>26. Controlul executiv este neclar – în special atribuirea sarcinilor SIS.</b> Sarcina de intelligence este procesul de stabilire a cerințelor și priorităților cheie de intelligence care definesc cheltuielile agențiilor de informații și colectarea și analiza informațiilor. În democrații, sarcina serviciilor de informații este responsabilitatea ramurii executive a guvernului și reflectă politicile externe, de securitate și de apărare ale unui stat. Rezultatele procesului de lucru, denumit în mod obișnuit "declarația priorităților serviciilor de informații", sunt de obicei rezumate într-un document care este aprobat de miniștrii guvernului sau de șeful executivului. Parlamentul nu atribuie sarcini direct agențiilor de informații, deoarece executivul este cel care controlează politicile, planificarea strategică, precum și acțiunile din sectorul public.</p>
<p><b>Se acceptă.</b> Cadru juridic al activității contrainformative și activității informative externe, realizate de către Serviciul de Informații și Securitate al Republicii Moldova, modalitatea și condițiile de dispunere și efectuare a măsurilor contrainformative și măsurilor informative externe, precum și de efectuare a controlului asupra legalității acestora au fost reglementate expres în proiect.</p>	<p>27. Ambele proiecte de legi nu au detalii (dacă există vreo definiție) cu privire la modul în care sunt atribuite sarcinile SIS. Atunci când se organizează activități de informații, este necesar să se ia în considerare crearea unui sistem efectiv și eficient de atribuire a sarcinilor serviciilor de informații de către autoritățile executive desemnate cu precizie. Acest lucru este esențial pentru a se asigura că SIS desfășoară ceea ce guvernul consideră a fi prioritățile și activitățile lor în concordanță cu interesele naționale și cu nevoile reale ale autorităților statului. De asemenea, o sarcină clară este esențială pentru a menține SIS responsabil împotriva unui set clar de obiective, ceea ce permite o supraveghere semnificativă de către comisia parlamentară.</p>
<p><b>Nu se acceptă.</b> SIS nu este supus controlului executiv, fiind o autoritate administrativă autonomă.</p>	<p>28. Sarcina revine puterii executive și, în mod ideal, ar fi mai degrabă un cabinet decât o responsabilitate prezidențială să evite sarcini care ar fi numai benefice pentru președinte. În orice țară, acest lucru este făcut de Consiliul național de securitate, care este format din președinte, precum și din înalți miniștri și înalți funcționari din domeniul apărării și securității.</p> <p><b>29. Controlul executiv ar trebui să fie mai transparent și mai clar, în ceea ce privește responsabilitățile, și să fie deschis supravegherii într-un mod general.</b></p>

<p><b>Se acceptă.</b> Articolul 12 alin. (1) pct.1) și art.15 alin. (2) din proiect au fost revăzute.</p> <p>Totodată, potrivit art. 12 alin. (1) pct. 2) din proiect, măsurile contrainformative vor fi efectuate în baza mandatului judecătoresc, care le va autoriza, fiind un organ judiciar independent de organul care va efectua aceste măsuri. Proiectul a fost completat cu mecanism de control judecătoresc ex-post.</p>	<p>30. Controlul judiciar constă în <b>autorizarea ante-facto/ex ante</b> a utilizării metodelor de colectare a informațiilor (emiterea unui mandat) și în revizuirea post-facto/ex post (monitorizarea continuă) a aplicării mandatului. În majoritatea țărilor europene este, de obicei, o instanță la nivel înalt (Curtea Supremă sau Curtea de Apel) prin conducerea sa (președinte al Curții sau un judecător desemnat de președinte) care are dreptul legal de a autoriza utilizarea unor metode intruzive de către serviciile de informații. Nivelul înalt al Curții și vechimea judecătorului (judecătorilor) care au autoritatea de a emite un mandat sunt menite să <b>prevină orice influență nejustificată</b> a serviciului de informații asupra deciziilor lor.</p> <p>31. Proiectul de lege al SIS nu prevede mecanisme de control judiciar. Legea CI oferă detalii cu privire la rolul sistemului judiciar și emiterea de mandate. Soluția avută în vedere de proiectul de <b>lege diferă de bunele practici europene în două moduri:</b> (1) judecătorul care emite mandatul este un judecător de instrucție, nu un judecător superior de la o instanță de nivel înalt; (2) un număr semnificativ de măsuri intruzive (11 din 20 definite de legea CI) scapă de sub controlul judiciar, fiind aprobate de directorul SIS [articolul 12 alineatul (1) punctul 1)].</p>
<p><b>Se acceptă parțial.</b> Proiectul a fost completat cu un articol nou (art. 20<sup>1</sup>), care prevede controlul legalității efectuării măsurilor contrainformative de către judecător.</p> <p>Cât privește prelungirea termenului de efectuare a măsurii contrainformative, aceasta se realizează de judecătorul care examinează minuțios circumstanțele care justifică această prelungire, iar în cazul în care apreciază că solicitarea nu este motivată, refuză prelungirea.</p> <p>Totodată, versiunea redactată corespunde celor stabilite de către grupul de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică.</p>	<p>32. Nu este clar modul în care mandatele de punere în aplicare sunt monitorizate/revizuite de către instanță, deoarece art.18 pare să se refere doar la informațiile directorului SIS cu privire la rezultatele unei măsuri contrainformative. Mai multe detalii ar putea fi furnizate cu privire la prelungirea mandatului: tipul de informații care trebuie furnizate judecătorului și criteriile de acordare a prelungirii mandatului [articolul 17 alineatul (5)].</p> <p>33. Ar trebui să fie clar că judecătorul, atunci când i se solicită permisiunea de supraveghere, nu decide pur și simplu o problemă da/nu, ci are control deplin (în cadrul legii) asupra întinderii supravegherii permise. Cu alte cuvinte, judecătorul poate și ar trebui să fie în măsură să modifice ordinea, să stabilească condiții suplimentare de supraveghere, să limiteze cercul de suspecți care pot fi supuși supravegherii, solicitând solicitantului să raporteze frecvent cu privire la rezultatele supravegherii. Legea trebuie să încurajeze un control informat, independent și critic al cererilor de către judecător.</p>
<p>Capitolul VI (CONTROLUL ACTIVITĂȚII INFORMATIVE/CONTRAINFORMATIVE) a fost revizuit în cadrul grupului de lucru</p>	<p>34. Proiectul de lege al CI la art. 58 este mai detaliat cu privire la controlul procurorilor, dar încă vag, lăsând multe întrebări fără răspuns. De exemplu, alineatul (1) indică faptul că se referă la activitatea contrainformativă, lăsând</p>

<p>la o parte activitățile de informații externe. Alineatul (2) limitează domeniul de aplicare al rolului de procuror la soluționarea plângerilor împotriva SIS în cazurile care pot implica o încălcare a legii de către ofițerii serviciului. Aceasta este o restrângere semnificativă a domeniului de aplicare al controlului de procuror. În plus, proiectul de lege nu abordează aspecte precum instrumentele, procedurile și mijloacele pe baza cărora urmează să se desfășoare procedurile de urmărire penală. De asemenea, nu există indicii cu privire la procedura de tratare a rezultatelor unei astfel de proceduri.</p>	<p>creat pe lângă Comisia securitate națională, apărare și ordine publică</p>
<p>35. Legislația ar fi îmbunătățită prin simplificarea articolelor și prin acoperirea întregii responsabilități judiciare într-o singură secțiune. Acest lucru ilustrează, de asemenea, modul în care existența unei singure legi în loc de două ar părea benefică, în ceea ce privește claritatea, concizia și previzibilitatea legii.</p>	<p><b>Nu se acceptă.</b> Argumentul nu poate fi reținut dat fiind faptul că, ambele proiecte au domenii de reglementare distincte/separate. Respectiv, adoptarea concomitentă a ambelor legi este indispensabilă.</p>
<p>36. Parlamentele sunt principalul organism însărcinat cu exercitarea supravegherii implementării priorităților de securitate națională de către agențiile de informații. În forma sa actuală, textul proiectului de lege abordează subiectul pe scurt și superficial. Dispozițiile legii ar trebui să fie supuse unei extinderi suplimentare și definirii instrumentelor de supraveghere parlamentară. În timp ce dezbaterile declanșate de raportul anual de activitate al SIS este bine prezentată la articolul 57 din proiectul CI, acesta este doar un instrument și un exemplu atunci când puterea de supraveghere a Parlamentului este exercitată. Alte instrumente, cum ar fi audierile comisiilor, rapoartele specifice solicitate de comisie, aprobarea bugetului și supravegherea execuției bugetare, inspecțiile în teren, întrebările și interpellările în plen, ar trebui menționate în lege, pentru a preveni o interpretare minimalistă a dispozițiilor legilor și a puterii constituționale de supraveghere a Parlamentului.</p>	<p><b>Se acceptă parțial.</b> Prevederile au fost redactate conform celor stabilite de grupul de lucru pe lângă Comisia securitate națională, apărare și ordine publică.</p>
<p>37. Supravegherea eficientă se bazează pe autoritatea reală a unei comisii parlamentare de a convoca funcționarii la reuniunile comisiilor, de a solicita accesul la informații, documente și explicații cu privire la activitățile serviciului. Aceasta înseamnă că membrii comisiei au acces la informații clasificate, iar legea prevede sancțiuni (care pot include răspunderea penală) pentru obstrucționarea accesului comisiei la informații sau pentru furnizarea de informații neadevărate comisiei. Accesul parlamentarilor la informații clasificate referitoare la SIS ar trebui menționat prin lege.</p>	<p><b>Se acceptă</b> Versiunea redactată corespunde celor stabilite în cadrul ședințelor grupului de</p>
<p>38. Pentru o supraveghere eficientă a informațiilor, mandatul de supraveghere <b>trebuie să fie clar și precis</b> (detaliat într-un document precum Regulamentul de procedură al comisiei), deoarece accesul la informații</p>	<p><b>Se acceptă</b> Versiunea redactată corespunde celor stabilite în cadrul ședințelor grupului de</p>

<p>lucru de pe lângă Comisia securitate națională, apărare și ordine publică.</p>	<p><b>Se acceptă.</b>          Articolul 57 a fost completat cu alineatele (7) și (8) care soluționează problemele semnalate.</p> <p>Controlul parlamentar asupra activității informative/contrainformative este exercitat nmijlocit atât de către Comisia securitate națională, apărare și ordine publică, cât și prin intermediul Subcomisiei pentru exercitarea controlului parlamentar asupra activității Serviciului de Informații și Securitate al Republicii Moldova (art. 57 alin. (1) din proiect).</p> <p>Serviciul de Informații și Securitate al Republicii Moldova este direct sub control parlamentar, în acest sens fiind relevante prevederile art. 57 din proiect.</p>
<p>clasificate este întotdeauna condiționat de principiul "necesității de a cunoaște", care, la rândul său, este definit de mandatul comisiei. În cazul în care Parlamentul nu își definește în mod clar mandatul de supraveghere (prin urmare, "necesitatea de a ști"), acest lucru va fi definit de SIS, în mod informal, ceea ce va fi în mod inerent restrictiv. Legea ar putea menționa că comisia/subcomisia își va defini mandatul de supraveghere și modus operandi într-un <b>Regulament al Comisiei</b>.</p>	<p>39. Legea ar trebui să prevadă, de asemenea, un Raport anual elaborat de comisie/sau de subcomisie și prezentat Parlamentului în plen, care să analizeze activitățile de supraveghere ale comisiei și principalele concluzii și recomandări ale acestora referitoare la activitatea SIS (fără a se referi la informații sensibile sau clasificate). În cele din urmă, ar putea fi avute în vedere două versiuni ale acestor rapoarte: una restrânsă (doar pentru Biroul Parlamentului) și una publică (pentru plen și pentru public).</p> <p>40. Experiența țărilor europene a arătat că este întotdeauna mai bine ca serviciile de securitate și de informații să aibă o <b>comisie parlamentară permanentă separată</b> pentru supraveghere, mai degrabă decât o subcomisie. Supravegherea credibilă și eficientă depinde de legitimitatea democratică solidă a comisiei și cvorumul fezabil. Comisia pentru securitate națională, apărare și ordine publică al Parlamentului ar trebui să-și păstreze responsabilitatea generală pentru supravegherea informațiilor, să ia în considerare adoptarea unor proceduri care să sporească funcționalitatea subcomisiei SIS și să o încurajeze să funcționeze ca instrument de canalizare a punctelor de vedere și inițiativelor opoziției; ar trebui avută în vedere o eventuală împărțire a sarcinilor/instrumentelor și oportunităților de supraveghere între comisie și subcomisie.</p> <p>41. Deși parlamentele nu sunt direct implicate în atribuirea sarcinilor agențiilor de informații, acestea joacă totuși un rol esențial în supravegherea procesului. Acest rol este dublu: supravegherea procesului prin care executivul definește prioritățile de intelligence; și, în al doilea rând, supravegherea executării de către agențiile de informații a acestor priorități. Comisia ar trebui să analizeze cu atenție faptul dacă implicarea directă a Parlamentului în atribuirea sarcinilor agențiilor de informații ar putea submina capacitatea executivului de a governa. În plus, acest lucru ar putea crea un conflict de interese: parlamentele nu pot efectua o supraveghere sau un control independent și eficient al agențiilor de informații, fiind în același timp responsabile pentru atribuirea sarcinilor acestora.</p> <p>42. Problema <b>interceptării</b> tuturor comunicațiilor personale este întotdeauna un subiect dificil și are nevoie de o direcție și o supraveghere</p>
	<p><b>Se acceptă.</b>          Prevederile au fost redactate conform celor</p>

<p>stabilite de grupul de lucru pe lângă Comisia securitate națională, apărare și ordine publică.</p>	<p>clare. Acest lucru este deosebit de important, având în vedere că o mare parte din informațiile cu caracter personal ale unei persoane sunt transportate în date. Legea CI este ușor confuză și ar beneficia de o secțiune separată dedicată protocoalelor de interceptare care ar include stocarea, ștergerea materialelor care nu sunt relevante, termenii și ștergerea materialelor operaționale, materiale privilegiate, adică medicale, avocat / client etc. și alte aspecte legate de viața privată. În majoritatea țărilor democratice există legi separate și specifice referitoare la acest subiect, astfel încât toate agențiile care trebuie să efectueze interceptări să respecte aceleași reguli.</p>
<p><b>Se acceptă.</b> Dispozițiile privind protecția datelor personale au fost revăzute stabilindu-se aplicabilitatea regulilor generale de prelucrare și control asupra datelor personale în cadrul activității informative/contrainformative.</p>	<p>44. Este posibil ca dispozițiile privind <b>protecția datelor</b> din cele două proiecte să nu îndeplinească standardele europene.</p>
<p><b>Se acceptă.</b> Prevederile art. 58 din proiect, stabilesc responsabilitatea și competența procurorului din cadrul Procuraturii Generale de a exercita controlul asupra activității contrainformative și se efectuează în baza plîngerilor depuse de către persoane ale căror drepturi și interese legitime se presupune că au fost încălcate sau din oficiu (art. 58 (alin. 2)).</p>	<p>45. <b>Plângeri.</b> Nu pare să existe o procedură oficială de depunere a plîngerilor împotriva SIS din partea publicului. Responsabilitatea pentru investigarea plîngerilor revine Procuraturii Generale, dar pare să se limiteze la utilizarea unor metode intruzive (art.58 din legea CI). Cu toate acestea, sistemul public de reclamații ar trebui să fie mai transparent, mai clar și mai accesibil și ar trebui să includă trimiterea la măsurile și liniile de responsabilitate pentru corectarea neregulilor descoperite în urma investigării plîngerilor.</p>
<p><b>Se acceptă.</b> Articolul 23 prevede expres procedura de informare, inclusiv, temeiurile obiective de neinformare de persoanelor în privința cărora au fost efectuate măsurile contrainformative.</p>	<p>47. <b>Informarea persoanei cu privire la măsurile CI întreprinse împotriva sa (articolul 23).</b> O serie de țări democratice desfășoară această practică, cu toate acestea, procedura trebuie analizată cu atenție, deoarece ar putea alerta persoanele cu privire la metodele utilizate de SIS, făcându-le astfel dificil de utilizat în viitor. De asemenea, are implicația serioasă de a alerta actorii străini cu privire la interesele SIS și ar putea afecta, de asemenea, capacitatea SIS de a lucra cu parteneri internaționali care ar putea fi precauți referitor la eventuala expunere a informațiilor și tehnicilor partajate.</p>
<p><b>Se acceptă.</b> Articolul 6 din proiect a fost exclus.</p>	<p>1. <b>Art. 6 alin. (8) și alin. (9)</b> – Normele reglementează unele garanții sociale acordate persoanelor care și-au exprimat consimțământul scris de a colabora cu Serviciul. Norma alin. (1) al aceluiași articol (art. 6) prevede că: persoanele care colaborează confidențial cu Serviciul sunt persoane fizice care, printr-un acord</p>
<p><b>Centrul Național Anticorupție al Republicii Moldova</b></p>	

<p>(nr. 06/2-7236 din 06.12.2022)</p>	<p>scris sau verbal, și-au dat consimțământul să ofere confidențial informații Serviciului, să participe confidențial la pregătirea și efectuarea activității informative/contrainformative, precum și să contribuie într-un alt mod, neinterzis de lege, la activitatea informativă/contrainformativă.</p> <p>Astfel, persoanele care colaborează confidențial cu Serviciul își exprimă consimțământul fie printr-un acord scris, fie printr-un acord verbal.</p> <p>În redacția propusă de autor, garanțiile urmează a fi acordate la survenirea cazurilor asigurate doar pentru persoanele care și-au exprimat consimțământul scris de a colabora cu Serviciul.</p> <p>Astfel, suntem în prezența reglementării juridice doar a unei categorii de cetățeni, or, ambele pot avea aceleași obligații și îndatoriri în ceea ce privește colaborarea confidențială cu Serviciul.</p> <p>Considerăm tratarea într-o manieră justă și echitabilă a tuturor persoanelor care colaborează confidențial cu Serviciul.</p> <p>Recomandăm autorului completarea normei cu prevederi care ar asigura instituirea unor garanții sociale și pentru persoanele care colaborează în mod confidențial cu Serviciul în baza acordurilor verbale.</p> <p>În acest sens, dacă autorul consimte că angajamentul scris presupune o colaborare în baza altor criterii/condiții, respectiv și asigurarea socială urmează să fie diferențiată în raport cu persoanele care colaborează în baza angajamentelor verbale.</p>
<p><b>Se acceptă.</b></p> <p>Normele privind acordarea dreptului Serviciului de a distruge materiale, prevăzute la art. 9 alin. (3) și art. 15 alin. (14) a fost excluse.</p> <p>Totodată, menționăm că, propunerea expusă a fost luată în considerare la redactarea normei prevăzute la art. 10 din proiectul de lege.</p>	<p><b>2. Normele art. 9 alin. (3), art. 10 și 15 alin. (14) reglementează în fond distrugerea materialelor care s-au dovedit a fi irelevante pentru cauza examinată de către Serviciu.</b></p> <p>Normele privind acordarea dreptului Serviciului de a distruge materiale urmează să fie corelate cu prevederile art. 23 care statuează obligația Serviciului de a informa persoana despre măsurile contrainformative înfăptuite în privința sa, precum și cu prevederile art. 58 prin care se asigură efectuarea controlului asupra activității contrainformative de către procuror în baza plângerilor depuse de către persoane ale căror drepturi și interese legitime se presupune că au fost încălcate.</p> <p>Astfel, considerăm că atribuirea în mod unilateral a dreptului Serviciului de a distruge careva materiale care consideră că nu au relevanță cauzei și scopului examinat riscă să prejudicieze în unele cazuri drepturile persoanelor asupra cărora au fost desfășurate careva măsuri contrainformative.</p> <p>În acest sens, Serviciul va avea puterea decizională de a considera care fapte, materiale, documente sunt sau nu sunt relevante speței, existând riscul luării unor decizii subiective în dependență de interes.</p> <p>Pornind de la ideea că normele legii stabilesc obligativitatea inițierii unui</p>

<p>dosar special, care este supus înregistrării, considerăm oportun ca toate documentele să fie păstrate/arhivate cel puțin până la expirarea termenului în care orice persoană lezată să fie în drept de a contesta acțiunile considerate a fi ilegale din cadrul măsurilor contrainformative desfășurate, termen care urmează a curge după data informării persoanei în condițiile art. 23 privind măsurile contrainformative înfăptuite în privința sa.</p> <p>Propunem autorului excluderea normelor care ar permite Serviciului distrugerea materialelor, documentelor și altor obiecte ce au relevanță cauzei desfășurate prin includerea acestora în dosarul special inițiat și remis pentru arhivare conform procedurii legale.</p>	<p>Norma art 15 alin. (6) stabilește în mod confuz asigurarea judecătorului cu prezentarea materialelor ce confirmă necesitatea efectuării măsurilor contrainformative.</p> <p>Textul „îi pot fi prezentate” denotă o ambiguitate administrativă în privința acțiunilor ce urmează a fi întreprinse de către Serviciu.</p> <p>Astfel, în anumite cazuri, Serviciul va putea refuza prezentarea cărorva acte/documente/materiale ce sunt necesare judecătorului pentru argumentarea măsurii contrainformative solicitate.</p> <p>În aceste condiții, norma va permite în mod legal Serviciului de a nu prezenta aceste materiale.</p> <p>Propunem autorului substituirea textului „îi pot fi prezentate materialele” cu textul „îi sunt prezentate materialele”.</p>	<p><b>Se acceptă.</b></p> <p>Norma a fost modificată corespunzător. Astfel, propunerea expusă a fost luată în considerare la redactarea normei prevăzute la art 15 alin. (6) din proiect.</p>
<p>dosar special, care este supus înregistrării, considerăm oportun ca toate documentele să fie păstrate/arhivate cel puțin până la expirarea termenului în care orice persoană lezată să fie în drept de a contesta acțiunile considerate a fi ilegale din cadrul măsurilor contrainformative desfășurate, termen care urmează a curge după data informării persoanei în condițiile art. 23 privind măsurile contrainformative înfăptuite în privința sa.</p> <p>Propunem autorului excluderea normelor care ar permite Serviciului distrugerea materialelor, documentelor și altor obiecte ce au relevanță cauzei desfășurate prin includerea acestora în dosarul special inițiat și remis pentru arhivare conform procedurii legale.</p>	<p>Norma art 15 alin. (6) stabilește în mod confuz asigurarea judecătorului cu prezentarea materialelor ce confirmă necesitatea efectuării măsurilor contrainformative.</p> <p>Textul „îi pot fi prezentate” denotă o ambiguitate administrativă în privința acțiunilor ce urmează a fi întreprinse de către Serviciu.</p> <p>Astfel, în anumite cazuri, Serviciul va putea refuza prezentarea cărorva acte/documente/materiale ce sunt necesare judecătorului pentru argumentarea măsurii contrainformative solicitate.</p> <p>În aceste condiții, norma va permite în mod legal Serviciului de a nu prezenta aceste materiale.</p> <p>Propunem autorului substituirea textului „îi pot fi prezentate materialele” cu textul „îi sunt prezentate materialele”.</p>	<p><b>Se acceptă parțial.</b></p> <p>Menționăm că, art. 1 din proiect a fost revizuit în contextul dezbaterilor publice, iar măsurile contrainformative care pot fi efectuate cu autorizarea directorului Serviciului sau directorului adjunct special împuternicit, au fost reduse și urmează a fi realizate doar cu autorizarea judecătorului. Respectiv, art.12 alin. (1) pct.1) și 2) au fost modificate și stabilesc expres care măsuri contrainformative sunt autorizate de către directorul sau directorul adjunct special împuternicit ai Serviciului (doar una) și care sunt autorizate de către judecător.</p> <p>De asemenea, au fost operate modificari la art.17 alin. (5) din proiect privind durata</p>
<p>dosar special, care este supus înregistrării, considerăm oportun ca toate documentele să fie păstrate/arhivate cel puțin până la expirarea termenului în care orice persoană lezată să fie în drept de a contesta acțiunile considerate a fi ilegale din cadrul măsurilor contrainformative desfășurate, termen care urmează a curge după data informării persoanei în condițiile art. 23 privind măsurile contrainformative înfăptuite în privința sa.</p> <p>Propunem autorului excluderea normelor care ar permite Serviciului distrugerea materialelor, documentelor și altor obiecte ce au relevanță cauzei desfășurate prin includerea acestora în dosarul special inițiat și remis pentru arhivare conform procedurii legale.</p>	<p>Norma art 15 alin. (6) stabilește în mod confuz asigurarea judecătorului cu prezentarea materialelor ce confirmă necesitatea efectuării măsurilor contrainformative.</p> <p>Textul „îi pot fi prezentate” denotă o ambiguitate administrativă în privința acțiunilor ce urmează a fi întreprinse de către Serviciu.</p> <p>Astfel, în anumite cazuri, Serviciul va putea refuza prezentarea cărorva acte/documente/materiale ce sunt necesare judecătorului pentru argumentarea măsurii contrainformative solicitate.</p> <p>În aceste condiții, norma va permite în mod legal Serviciului de a nu prezenta aceste materiale.</p> <p>Propunem autorului substituirea textului „îi pot fi prezentate materialele” cu textul „îi sunt prezentate materialele”.</p>	<p><b>1. ATRIBUȚII PEA LARGI PENTRU SIS ÎN LIPSA UNOR GARANȚII SUFICIENTE</b></p> <p>Proiectul de lege nu definește clar ce înseamnă activitatea informativă și contrainformativă. <b>Sub descrierile lungi și vagi din art. 1 din proiect poate fi încadrat orice.</b> Acest lucru este inadmisibil pentru o lege atât de intrusivă în viața privată, efectuată de o agenție secretă. De asemenea, așa cum este scris art. 16 din proiect, aceste măsuri pot fi aplicate, în esență, și pentru documentarea infracțiunilor. Aceasta de fapt poate fi folosit pentru eludarea procedurii penale, ce de asemenea nu este admisibil.</p> <p>Proiectul propune ca SIS să poată efectua măsuri speciale de investigații (redenumite de fapt ca măsuri contrainformative) fără ca o cauză penală să fie inițiată. Se mai propune posibilitatea autorizării unor măsuri fără acordul judecătorului de instrucție. O varietate de acțiuni vor putea fi aplicate de către SIS după o autorizare internă a directorului SIS sau a adjunctului desemnat, <b>în afara vreunui control extern.</b> Conform autorilor, ideea proiectului era de a delimita măsurile de investigație efectuate de organele de urmărire penale și cele efectuate de SIS. În esență, proiectul reproduce în mare parte</p>

prevederile Codului de procedură penală și a Legii privind activitatea specială de investigații, **instituirea mecanismelor paralele**. Nu este clar de ce SIS ar avea nevoie de toate măsurile speciale de investigații, dacă nu documentează cauze penale, iar probele obținute de SIS nu vor putea fi folosite ca probe în dosarele penale. **Această copiere a tuturor măsurilor speciale pare să aibă un singur scop – oferirea competențelor pentru SIS de a face orice, însă fără o cauză penală și un mecanism eficient de supraveghere.**

Mai mult, SIS nu este un organ de urmărire penală, însă la art. 16 din proiect se propune ca măsurile contrainformative să fie dispuse pentru investigarea acțiunilor de schimbare prin violență a orânduirii constituționale, subminare sau lichidare a suveranității, independenței sau integrității teritoriale, sustragerea de armament, muniții, tehnică de luptă, substanțe explozive, radioactive, contrabanda cu acestea, terorism sau finanțarea terorismului etc. **Toate aceste acțiuni defapt sunt infracțiuni, iar investigarea lor trebuie efectuată conform CPP.** La fel, durata totală propusă pentru efectuarea măsurii speciale de investigații (art.17 alin.5 din proiect), dispusă pe o faptă concretă, nu poate depăși cumulativ 2 ani. **Termenul dat este mai mare decât cel prevăzut de CPP și creează spațiu larg pentru abuz.**

Pe de altă parte, proiectul prevede și instituirea mandatului judecătoresc, care reprezintă autorizarea, de către instanța de judecată de a efectua măsuri contrainformative. Mandatul judecătoresc urmează să fie eliberat, la demersul argumentat al conducerii SIS, **de către un judecător special împuternicit în acest sens.** În condițiile legii cu privire la secretul de stat (a se vedea art.5 alin.(5) lit e din legea 245/2008), doar SIS este autoritatea abilitată să întreprindă măsurile de control în privința cetățenilor cărora urmează să li se perfecteze dreptul de acces la secretul de stat. Proiectul la rândul său prevede că informațiile despre efectuarea măsurilor contrainformative, precum și rezultatele acestor măsuri constituie informații ce vor fi atribuite la secretul de stat și vor putea fi examinate doar de judecătorii care vor fi autorizați de SIS. **Practic, SIS va decide asupra judecătorului care urmează să examineze demersul privind eliberarea mandatului privind aplicarea măsurii contrainformative, dar și asupra judecătorilor care urmează să examineze contestațiile asupra încheierilor judecătorului de instrucție.** Acest fapt poate leza din independența funcțională a judecătorului sau cel puțin crea suspiciuni din partea societății despre o eventuală influență a SIS asupra acestora. La fel, în condițiile art.15 alin. 6 din proiect, examinarea demersului privind

totală pentru efectuarea măsurii contrainformative dispusă pe o faptă concretă.

Cât privește obiecția referitor la faptul că „*practic, SIS va decide asupra judecătorului care urmează să examineze demersul privind eliberarea mandatului privind aplicarea măsurii contrainformative, dar și asupra judecătorilor care urmează să examineze contestațiile asupra încheierilor judecătorului de instrucție*”, notăm că, art. 5 alin. (5) lit. e) Legea nr. 245/2008 cu privire la secretul de stat, prevede atribuțiile SIS în domeniul protecției secretului de stat și anume: „*întreprinde măsuri de control în privința cetățenilor cărora urmează să li se perfecteze dreptul de acces la secretul de stat*”.

Totodată, examinarea informațiilor despre efectuarea măsurilor contrainformative, precum și rezultatele acestor măsuri în vederea eliberării mandatului judecătoresc se realizează de către un judecător din cadrul Curții de Apel Chișinău special împuternicit în acest sens (art. 15 alin. (2) a fost revăzut), iar demersul privind eliberarea mandatului pentru aplicarea măsurii contrainformative urmează a fi repartizat judecătorului care are perfectat dreptul de acces la secret de stat. Concomitent, proiectul a fost completat, la clauzele tranzitorii cu norma care va asigura independența sistemului judecătoresc și anume - *președinții Curții de Apel Chișinău și Curții Supreme de Justiție vor stabili numărul concret de judecători ce vor fi abilitați cu competența*

<p>eliberarea mandatului judecătoresc va fi în ședință închisă, cu participarea ofiterului de informații, care poate prezenta materialele ce confirmă necesitatea efectuării măsurii, fără ca acestea să fie anexate la demers. Prin urmare, acest exercițiu se rezumă la formalitate, or, în practică, ofițerul SIS va putea refuza prezentarea oricăror materiale, iar judecătorul nu va putea verifica justificarea demersului.</p> <p>Un alt exemplu de prevederi cu potențiale riscuri de aplicare abuzivă ar putea servi și art. 23 din proiect, și anume că persoana în privința căreia s-au aplicat măsuri cu autorizarea directorului SIS practic nu va fi informată referitor la aceasta. Aceste prevederi restrâng dreptul de a avea acces la justiție și dreptul la apărare. Doar persoanele, în privința cărora s-au aplicat măsuri autorizate prin eliberarea mandatului judecătoresc, pot fi informate despre măsurile înfăptuite în privința lor. Însă, potrivit proiectului (alin.3 art. 23) informarea nu se va face, <b>chiar dacă procedura a fost finalizată sau dosarul clasat</b>, dacă există motive întemeiate de a considera că acest fapt ar putea constitui un risc sporit pentru viața sau sănătatea oamenilor, ar periclita o altă investigație desfășurată, ar dăuna securității statului sau ar aduce prejudicii scopului pentru care au fost efectuate măsurile contrainformative. Dacă dosarul e clasat, înseamnă că asemenea riscuri nu există. <b>De fapt, această prevedere instituie „o scuză” pentru a nu informa pe nimeni niciodată.</b> Conform CEDO, în cazul în care un stat instituie o măsură de supraveghere secretă, a cărei existență nu este cunoscută de persoanele care fac obiectul controlului, având drept consecință faptul că respectiva supraveghere nu poate fi contestată, persoanele sunt private de drepturile pe care le au în temeiul art. 8 CEDO2.</p> <p>Mai mult, <b>conchidem că proiectul nu prevede termenul în care urmează a fi clasat dosarul special</b>, fapt ce presupune că autorul nu a luat în calcul posibilitatea reală de informare a persoanei supuse măsurilor autorizate de conducerea SIS.</p> <p>Mai mult, proiectul nu stabilește clar răspunderea conducerii SIS sau ofițerului de investigații SIS urmare a unor acțiuni procesuale declarate ilegale. Considerăm că aceștia trebuie să răspundă disciplinar, contravențional sau penal dacă faptele lor în timpul autorizării sau efectuării măsurilor speciale de investigații erau ilegale.</p>	<p>de a elibera mandate judiciare și de examinare a recursurilor, vor desemna judecătorii respectivi și vor organiza procesul de repartizare aleatorii a demersurilor/recursurilor Serviciului</p> <p>Cu referire la obiecția privind includerea unor prevederi în proiect cu potențiale riscuri de aplicare abuzivă și anume că persoana în privința căreia s-au aplicat măsuri cu autorizarea directorului SIS practic nu va fi informată referitor la aceasta, reiterăm faptul că, spectrul de măsuri contrainformative care pot fi efectuate cu autorizarea directorului Serviciului sau directorului adjunct special împuternicit (pct. 1) alin. (1) art. 12 din proiect) au fost revizuite și limitate, ca urmare a dezbaterilor publice.</p> <p>Consecvent, la art. 23 alin. (3) vsunt enumerate expres motivele când persoana nu va fi informată despre măsurile contrainformative înfăptuite în privința sa. Respectiv, motivele privind neinformarea persoanei vor fi examinate de către judecătorul care a eliberat mandatul judecătoresc, fiind supuse controlului judecătoresc. De asemenea, în cazul în care au dispărut temeiurile care au stat la baza neinformării persoanei supuse măsurii contrainformative, persoana urmează a fi informată despre măsurile contrainformative realizate în privința sa.</p>	<p><b>Se acceptă.</b> Textul a fost revăzut. Normele de la art.1 alin. (2) și art. 13 alin. (1) lit. c) și art. 17 alin. (1) a fost excluse.</p>
<p><b>Centrul de Resurse Juridice din Moldova (CRJM)</b></p>	<p><b>2. DEFINIȚII ȘI TERMENI AMBIGUE UTILIZATE ÎN PROIECT</b></p> <p>Pe parcursul textului proiectului se operează cu multe sintagme ambigue. Expresiile utilizate într-un cadru legal contează în mod semnificativ, deoarece definițiile vagi sau excesiv de extinse pot lăsa posibilitatea unor restricții</p>	

<p>Nr. 21/23 din 1 Mai 2023</p>	<p>nejustificate sau încălcări ale drepturilor fundamentale. De exemplu, proiectul operează cu noțiunile de „securitate națională” și „securitatea statului”, fără a face o distincție între aceste două concepte. Art.1 din Legea nr. 618/1995 prevede că <b>securitatea statului este parte integrantă a securității naționale</b>. Securitatea națională fiind un termen mult mai larg care înglobează mai multe componente. În situațiile de criză, care afectează securitatea națională, clarificarea acestor definiții devine crucial pentru a trasa liniile de activitate ale SIS.</p> <p>Sintagmele „<i>cu o probabilitate sporită</i>” și „<i>cu o probabilitate înaltă</i>” trebuie clarificate sau revizuite pentru a nu acorda posibilitatea unei interpretări abuzive din partea SIS. Ambiguă este și formularea la art. 1 alin.(2) – „<i>protejării procesului de decizie politico-statal</i>”. O asemenea sintagmă nu se regăsește nicăieri în cadrul legal național.</p> <p>Temeiurile pentru efectuarea măsurilor contransformative la fel sunt reglementate prea larg. De exemplu, lit c) al art. 13 prevede ca temei „<i>informațiile devenite cunoscute, privind potențialele riscuri și amenințări la adresa securității statului</i>”. <b>Considerăm necesar ca autorii să menționeze în proiect o listă exhaustivă a naturii și definirii tipurilor de riscuri și amenințări.</b></p> <p>La fel, sintagma utilizată în art. 17 din „<i>perioade succesive, precum și pe perioade care nu se succed</i>” crează confuzie și posibilitate de interpretare diferită. De exemplu, conform proiectului, măsurile contransformative se autorizează, pentru o perioadă de până la 90 de zile, cu posibilitatea de prelungire pe perioade succesive, precum și pe perioade care nu se succed, de până la 90 de zile. Prin urmare, redacția actuală permite realizarea măsurilor care <b>nu se succed pe un termen care cumulativ, cu certitudine va depăși termenul prevăzut în proiect ca legal</b>. Prevederea trebuie modificată că să stabilească un termen clar care nu ar crea ingerințe nejustificate asupra drepturilor persoanelor.</p> <p>Adițional, deși a fost enunțat și în cadrul unei consultări publice preliminare a proiectului, reiterăm problematica ce ține de <b>posibilitatea interceptării convorbirilor dintre avocat și client, jurnalist și sursa sa de informare</b>, or prevederile art. 4 și art. 6 sunt prea largi și nu enunță concret subiecții care cad sub incidența legii și cum va fi asigurat secretul profesional al avocaților și jurnaliștilor.</p>	<p>Totodată, cu referire la realizarea măsurilor contransformative în privința avocaților și jurnaliștilor, art. 15 din proiect a fost completat cu un alineat nou, care reglementează interdicția autorizării măsurilor contransformative în privința acestora.</p>
<p><b>3. MECANISME DE CONTROL - FORMALE</b></p> <p>În pofida faptului că proiectul propune patru mecanisme de control (Parlament, procuratura, control intern al SIS și judecător de instrucție), în realitate nu se propun mecanisme, care ar fi, cu adevărat eficiente.</p>	<p><b>Se acceptă parțial.</b></p> <p>În cadrul ședințelor grupului de lucru creat pe lângă Comisia securitate națională, apărare și ordine publică</p>	

**Rolul oferit Parlamentului în acest sens în mod clar este insuficient.** Supravegherea parlamentară va fi efectuată anual, când conducerea SIS va prezenta un raport în cadrul unei ședințe închise a subcomisiei specializate unde vor fi prezentate informații statistice despre operațiunile finalizate de SIS, dacă divulgarea lor nu va prejudicia securitatea statului. Informații despre operațiunile în derulare nu se vor prezenta. Lipsa transparenței în ceea ce privește raportarea și audierea conducerii SIS de către Parlament prin urmare nu este justificată. **Date statistice și alte date care ar putea vorbi despre problemele sistemice din SIS trebuie să fie publice.** Comisia de la Veneția (pct. 34) recomandă ca SIS-ul să fie obligat să furnizeze toate datele cu privire la numărul și tipurile de măsuri desfășurate pe parcursul anului precedent și ca Subcomisia parlamentară să publice un raport cu aceste date statistice. Subcomisia ar trebui să poată emite un raport special pentru a atrage atenția publicului și Parlamentului asupra activităților care necesită un răspuns urgent. Ar trebui luată în calcul, și posibilitatea de a demara anchete parlamentare, care ar putea conduce la anchete judiciare, atunci când sunt bănuite neregularități grave, sub rezerva cerințelor securității statului. Proiectul la rândul său, prevede ca raportul prezentat Subcomisiei parlamentare **poate fi făcut public** (adică rămâne la discreția autorului sau guvernării) excluzându-se informațiile atribuite la secret de stat. **Cu alte cuvinte, proiectul nu aduce alte garanții noi pentru un control parlamentar eficient, dar păstrează practicile existente.** Cu regret, supravegherea parlamentară asupra activității SIS s-a dovedit insuficientă și netransparentă în trecut.

De asemenea, cum menționam mai sus, rolul judecătorului la autorizarea măsurilor va fi unul pur formal, deoarece el nu va avea în față materialele care justifică măsura. Mecanismul de informare a persoanei despre măsuri de asemenea este foarte volatil, permițând de facto ca persoana să nu fie informată niciodată despre faptul că a fost supus supravegherii de către SIS. Mai mult, informarea în cazul SIS nu presupune și accesul la dosar. **În general, proiectul permite distrugerea acestora în condiții neclare, ceea ce ar face orice control ulterior inexistent.**

Controlul intern asupra activității informative/contrainformative se realizează de către directorul SIS, directorul adjunct special imputernicit, inclusiv prin intermediul subunităților interne de control și conducătorii subunităților specializate. **De fapt se crează un non-sens atunci când persoana care inițial autorizează acțiunea ulterior va face și controlul acesteia.** Proiectul nu prevede un mecanism de supraveghere și verificare a abaterilor concrete a conducerii SIS și/sau ofițerilor SIS. În mod surprinzător, proiectul

problemele respective au fost discutate în detaliu și s-a ajuns la formularea în redacția modificată.

Respectiv, articolul 57 a fost completat cu alin. (7) și (8) care vin să implementeze ideile propuse, astfel încât problemele semnalate au fost înlăturate. Complementar alin. (2) al art. 57 din proiect a fost ajustat, astfel încât s-a prevăzut expres informațiile care se conțin în raportul general cu privire la activitatea

informativă/contrainformativă, pe care Directorul Serciciului urmează să-l prezinte anual Subcomisiei parlamentare.

De asemenea, odată ce Subcomisia parlamentară stabilește anumiți indici de suspiciune că au fost săvârșite încălcări grave în activitatea Serciciului, aceasta poate sesiza Procurorul General, care la rândul său va întreprinde acțiuni ce se impun.

Articolul 15 alin. (6) din proiect a fost revăzut, respectiv, pe parcursul examinării demersului privind eliberarea mandatului judecătoresc, judecătorului, la solicitarea acestuia sau din inițiativa Serciciului, îi vor fi prezentate materialele care justifică necesitatea efectuării acestor măsuri.

Cât privește informarea persoanei despre măsurile contrainformative înfăptuite în privința sa remarcăm că, articolul 23 prevede expres procedura de informare sau neinformare a persoanelor în privința cărora au fost efectuate măsuri contrainformative.

Respectiv, doar în cazul existenței unor

<p>reglementează doar drepturile subiecților care efectuează activitatea informativă/contrainformativă, dar nu nici într-un mod nu prevede care sunt obligațiile acestora.</p>	<p>temeiuri obiective în acest sens persoana nu va fi informată, iar în momentul în care temeiurile de neinformare decad, persoana imediat îi va fi adusă la cunoștință faptul efectuării măsurilor contrainformative în privința acesteia.</p> <p>Dispozițiile privind distrugerea materialelor care s-au dovedit a fi irelevante pentru cazul investigat, prevăzute la art. 10 și art. 56 alin. (2) din proiect au fost excluse.</p> <p>Cât privește obiecția precum că „proiectul reglementează doar drepturile subiecților care efectuează activitatea informativă/contrainformativă, dar nu nici într-un mod nu prevede care sunt obligațiile acestora”, notăm că articolul 5 din proiect a fost revizuit, reglementând și obligațiile subiecților..</p>
<p><b>Comisia SNAOP sesizată în fond</b></p>	<p><b>Concluzie:</b> Proiectul este insuficient de fundamentat și suscită probleme iremediabile din perspectiva drepturilor omului. Din toate considerentele enunțate mai sus, CRJM cheamă Parlamentul Republicii Moldova ca proiectul să fie consultat suplimentar cu părțile interesate, iar prevederile periculoase să fie modificate radical pentru a răspunde tuturor recomandărilor Comisiei de la Veneția.</p> <p>Ca urmare al finalizării procesului de examinare al amendamentelor, obiecțiilor și propunerilor parvenite din partea părților interesate asupra prezentului proiect de lege atât în formă scrisă, cât și în cadrul ședințelor de dezbateri publice, textul prezentului proiect de lege a fost definitivat și se propune a fi expus în următoarea redacție finală:</p> <p style="text-align: right;">„Proiect redactat (nr. 422/2022)</p>
<p><b>Comisia SNAOP</b></p>	<p><b>Se acceptă. Proiectul a fost dezbătut pe lar în cadrul grupului de lucru creat pe lângă Comisia parlamentară securitate națională, apărare și ordinie publică, fiind modificat conceptual.</b></p> <p style="text-align: center;"><b>L E G E</b></p> <p style="text-align: center;"><b>privind activitatea contrainformativă și activitatea informativă externă</b></p> <hr/> <p style="text-align: center;">Parlamentul adoptă prezenta lege organică</p> <p style="text-align: center;"><b>Capitolul I</b> <b>DISPOZIȚII GENERALE</b></p>

**Articolul 1.** Noțiuni, scop și domeniu de reglementare

(1) Prezentă lege stabilește cadrul normativ al activității conținutive și activității informative externe (în continuare – *activitate informativă/conținutivă*), realizate de către Serviciul de Informații și Securitate al Republicii Moldova (în continuare – *Serviciu*) sau, după caz, de Ministerul Apărării, modalitatea și condițiile dispunerii și realizării măsurilor conținutive și măsurilor informative externe, precum și ale efectuării controlului asupra legalității acestora, garanțiile minime de protecție a persoanelor supuse măsurilor conținutive.

(2) Activitatea conținutivă constă din ansamblul măsurilor, acțiunilor, operațiunilor și procedurilor desfășurate de către Serviciu în scopul identificării, prevenirii și contracarării vulnerabilităților, factorilor de risc și amenințărilor, conform competenței stabilite în Legea nr. 136/2023 privind Serviciul de Informații și Securitate al Republicii Moldova.

(3) Activitatea informativă externă constă din ansamblul măsurilor, acțiunilor și operațiunilor desfășurate în scopul planificării, culegerii, verificării, evaluării, prelucrării analitice, stocării, păstrării și valorificării datelor și informațiilor despre posibilitățile reale sau potențiale, despre acțiunile, planurile sau intențiile statelor ori ale organizațiilor străine, ale unor entități anticonstituționale sau ale unor persoane, care constituie sau ar putea constitui factori de risc sau amenințări la adresa securității Republicii Moldova, precum și în scopul obținerii informațiilor relevante pentru asigurarea securității naționale sau pentru crearea condițiilor favorabile asigurării și promovării intereselor strategice și realizării cu succes a politicii de securitate ale Republicii Moldova.

(4) Desfășurarea activității informative/conținutive în alte scopuri decât cele indicate în prezenta lege nu se admite.

**Articolul 2.** Principiile desfășurării activității informative/conținutive

Activitatea informativă/conținutivă se desfășoară conform următoarelor principii:

- a) legalitate;
- b) egalitatea tuturor în fața legii;
- c) respectarea drepturilor și libertăților fundamentale și reglementarea exclusiv prin lege a restrângerii exercițiului acestora;
- d) neutralitate politică și imparțialitate;
- e) îmbinarea metodelor și mijloacelor de activitate publică și secretă;
- f) oportunitate;
- g) proporționalitate;
- h) caracterul activ al măsurilor realizate;
- i) confidențialitate;
- j) eficiență și eficacitate.

**Articolul 3.** Subiecții care desfășoară activitate informativă/conținutivă

(1) Activitatea informativă/conținutivă este desfășurată de către Serviciu prin intermediul ofițerilor de informații și securitate (în continuare – *ofițeri de informații*) din cadrul subunităților specializate ale acestuia.

(2) Activitatea informativă externă în domeniul militar este desfășurată de către Ministerul Apărării prin intermediul militarilor prin contract din cadrul organelor și structurilor specializate ale acestuia.

(3) Alte entități sau persoane decât cele prevăzute de prezentul articol nu sunt în drept să desfășoare activitate informativă/contrainformativă.

**Articolul 4.** Drepturile, împuternicirile și obligațiile subiecților care desfășoară activitate informativă/contrainformativă

(1) În cadrul desfășurării activității informative/contrainformative, Serviciul și ofițerii de informații dispun de drepturile, împuternicirile și au obligațiile stabilite în Legea nr. 136/2023 privind Serviciul de Informații și Securitate al Republicii Moldova și în Legea nr. 170/2007 privind statutul ofițerului de informații și securitate.

(2) În cadrul desfășurării activității informative externe în domeniul militar, Ministerul Apărării și militarii prin contract dispun de drepturile, împuternicirile și au obligațiile stabilite în Legea nr. 162/2005 privind statutul militarului și în alte acte normative în domeniul apărării.

**Articolul 5.** Utilizarea mijloacelor tehnice la desfășurarea activității informative/contrainformative

În procesul desfășurării activității informative/contrainformative este permisă utilizarea sistemelor informaționale, a mijloacelor tehnice speciale destinate pentru obținerea ascunsă a informației, a aparatelor de înregistrare video/audio și a altor mijloace tehnice.

**Articolul 6.** Dosarul special

(1) În scopul acumulării și sistematizării informațiilor, al verificării și evaluării rezultatelor activității informative/contrainformative, precum și al adoptării în baza acestora a deciziilor corespunzătoare, sunt deschise dosare speciale la care se anexează toate informațiile și materialele colectate. Deschiderea dosarului special este supusă înregistrării obligatorii.

(2) Dosarul special este deschis:

a) în baza raportului ofițerului de informații din cadrul subunității specializate, aprobat de către directorul Serviciului sau directorul adjunct împuternicit în acest sens;

b) în baza raportului militarului prin contract din cadrul organelor și structurilor specializate ale Ministerului Apărării, aprobat de către conducătorul organului sau structurii respective.

Dosarul special se consideră deschis din data înregistrării acestuia.

(3) Măsurile contrainformative și măsurile informative externe nu pot fi desfășurate în afara unui dosar special.

(4) Fiecare dosar special prevede un mecanism de evidență a persoanelor care au luat cunoștință de informațiile și materialele dosarului, care să includă cel puțin:

a) numele, prenumele și funcția persoanei respective;

b) data și ora începerii studierii informațiilor și materialelor dosarului și data și ora finalizării acesteia;

c) mențiuni vizând accesul la dosarul special integral, la anumite documente, sau compartimente ale acestuia;

d) semnătura persoanei respective.

(5) Serviciul și Ministerul Apărării asigură măsurile necesare pentru a proteja informațiile și materialele păstrate în

dosarele speciale împotriva dezvoltării, modificării sau distrugerii neautorizate.

#### **Articolul 7.** Gestionarea dosarului special clasat

(1) După clasare, dosarul special se păstrează în depozitul special al Serviciului sau, după caz, cel al Ministerului Apărării. Termenul de păstrare al dosarului special clasat este echivalent termenului de secretizare.

(2) După expirarea termenului de păstrare al dosarului special clasat se decide asupra prelungirii termenului de secretizare, conform Legii nr. 245/2008 cu privire la secretul de stat, sau asupra distrugerii acestuia, iar dacă informațiile și materialele dosarului au valoare istorică sau științifică, acestea se desecretizează și se transmit spre păstrare în Arhiva Națională a Republicii Moldova.

#### **Articolul 8.** Reglementarea departamentală a activității informative/contrainformative

Organizarea, metodele desfășurării măsurilor contrainformative și celor informative externe; procedurile interne de autorizare, regulile de întocmire a proceselor-verbale cu privire la gestionarea, păstrarea și distrugerea informațiilor și materialelor obținute, măsurile de asigurare a integrității și confidențialității acestora și a activităților informative/contrainformative; regulile de desfășurare a operațiunilor sub acoperire și cu privire la conducerea și gestionarea activității realizate sub acoperire; modul de înregistrare a dosarelor speciale, categoria acestora, deschiderea, gestionarea, clasarea, termenele de păstrare și procedura de distrugere a acestora; utilizarea resurselor financiare alocate pentru realizarea măsurilor contrainformative și celor informative externe; modalitatea de conlucrare cu persoanele care colaborează confidențial cu Serviciul sau, după caz, cu Ministerul Apărării, inclusiv modul de documentare a informațiilor prezentate de către aceștia, categoriile acestor persoane; organizarea, personalul și resursele, sursele, planurile, procedura, tactica, metodele și mijloacele desfășurării activității informative/contrainformative, precum și valorificarea rezultatelor acesteia constituie informații atribuite la secretul de stat și sunt reglementate prin actele interne ale Serviciului sau, după caz, ale Ministerului Apărării.

## **Capitolul II MĂSURILE CONTRAINFORMATIVE Secțiunea 1 Autorizarea măsurilor contrainformative**

#### **Articolul 9.** Măsurile contrainformative

(1) În cadrul desfășurării activității contrainformative pot fi realizate următoarele măsuri contrainformative:

- 1) cu autorizarea directorului Serviciului sau a directorului adjunct împuternicit – identificarea abonatului sau a utilizatorului unei rețele de comunicații electronice ori a unui serviciu al societății informaționale;
- 2) cu mandat judecătoresc:
  - a) cercetarea domiciliului și/sau, după caz, instalarea în acesta a aparatelor care asigură supravegherea video/audio, fotografierea sau constatarea unor circumstanțe de fapt;
  - b) supravegherea domiciliului prin utilizarea mijloacelor tehnice;
  - c) interceptarea comunicărilor;
  - d) obținerea accesului la informația care se află sau se procesează într-un sistem informatic, pe dispozitive sau

echipamente de comunicații și/sau monitorizarea acesteia;

- e) colectarea informației de la furnizorii de servicii de comunicații electronice;
  - f) reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimerilor poștale;
  - g) înregistrarea video/audio a conținutului comunicărilor;
  - h) blocarea accesului la rețelele de comunicații electronice pentru un sistem informatic, un dispozitiv sau un echipament ori pentru o societate informațională, blocarea unor servicii de comunicații electronice;
  - i) ridicarea operativă;
  - j) obținerea accesului la informația financiară sau monitorizarea tranzacțiilor financiare;
  - k) urmărirea vizuală și/sau documentarea cu ajutorul metodelor și mijloacelor tehnice, precum și localizarea ori urmărirea prin sistemul de poziționare globală sau prin alte mijloace tehnice.
- (2) Lista măsurilor indicate la alin. (1) este exhaustivă și poate fi modificată sau completată doar prin lege.

#### **Articolul 10.** Temeiurile desfășurării măsurilor contrainformative

Drept temeiuri pentru desfășurarea măsurilor contrainformative pot servi:

- 1) informațiile privind:
  - a) pericolele indicate la art. 4 alin. (2) din Legea securității statului nr. 618/1995 și faptele indicate la art. 3 pct. 2) lit. b) și c) din Legea nr. 136/2023 privind Serviciul de Informații și Securitate al Republicii Moldova;
  - b) circumstanțele care pun în pericol securitatea investigatorului sub acoperire, a ofițerului de informații, a persoanelor care colaborează confidențial cu Serviciul sau a membrilor familiilor lor;
  - 2) interpelările organizațiilor internaționale sau ale autorităților altor state, în conformitate cu tratatele internaționale la care Republica Moldova este parte sau în baza acordurilor de colaborare între Serviciu și autoritățile de profil din alte state;
  - 3) necesitatea de a obține informații în interesul asigurării securității Republicii Moldova, al menținerii și dezvoltării potențialului ei tehnico-științific, economic sau de apărare, al creării condițiilor pentru promovarea politicii externe și interne;
  - 4) asigurarea protecției secretului de stat;
  - 5) colectarea informațiilor necesare cu privire la persoanele supuse verificării pentru:
    - a) acordarea accesului la informații ce constituie secret de stat;
    - b) admiterea la muncă la obiectivele infrastructurii critice;
    - c) stabilirea sau întreținerea relațiilor de colaborare cu acestea la organizarea și desfășurarea măsurilor contrainformative și/sau informație externe;
  - 6) verificarea candidaților sau titularilor funcțiilor publice;
  - 7) asigurarea securității interne;
  - 8) colectarea informațiilor necesare cu privire la persoanele care colaborează confidențial cu Serviciul, precum și cu privire la persoanele supuse verificării pentru admiterea acestora la organizarea și desfășurarea unor măsuri contrainformative și/sau informație externe ori pentru acordarea accesului la informațiile și materialele acumulate pe parcursul realizării acestor măsuri.

#### **Articolul 11.** Procedura autorizării măsurilor contrainformative de către

directorul Serviciului sau directorul adjunct împuternicit

(1) Realizarea măsurii contrainformative prevăzute la art. 9 alin. (1) pct. 1) se autorizează, prin ordonanță, de către directorul Serviciului sau directorul adjunct împuternicit în acest sens, în baza demersului conducătorului subunității care desfășoară activitatea contrainformativă în cadrul unui dosar special deschis și înregistrat.

(2) Demersul indicat la alin. (1) cuprinde: circumstanțele de fapt care servesc drept temei pentru realizarea măsurii contrainformative; argumentarea necesității măsurii respective; numărul dosarului special în cadrul căruia urmează a fi realizată măsura contrainformativă.

(3) Pentru emiterea ordonanței indicate la alin. (1), directorul Serviciului sau directorul adjunct împuternicit, pe lângă temeinicia demersului, examinează suplimentar dacă:

a) măsura solicitată urmărește un scop legitim;  
b) măsura este proporțională cu restrângerea exercițiului drepturilor sau libertăților persoanei, garantate de lege, și cu necesitatea realizării acesteia.

(4) Ordonanța directorului Serviciului sau a directorului adjunct împuternicit cuprinde:

a) data emiterii;  
b) numărul dosarului special în cadrul căruia este autorizată măsura contrainformativă;  
c) măsura contrainformativă autorizată.  
(5) Directorul Serviciului, directorul adjunct împuternicit refuză autorizarea măsurii contrainformative dacă constată că demersul prezentat este neîntemeiat, nu urmărește un scop legitim sau măsura solicitată este disproporțională în raport cu restrângerea exercițiului drepturilor sau libertăților persoanei.

#### **Articolul 12.** Procedura autorizării măsurilor contrainformative

prin emiterea mandatului judecătoresc

(1) În sensul prezentei legi, mandatul judecătoresc reprezintă autorizarea de a realiza, în cadrul unui dosar special deschis și înregistrat, măsurile contrainformative prevăzute la art. 9 alin. (1) pct. 2).

(2) Mandatul judecătoresc este emis, în baza demersului în formă scrisă al directorului Serviciului sau al directorului adjunct împuternicit, de către un judecător din cadrul Curții de Apel Chișinău desemnat în acest sens.

(3) Demersul pentru emiterea mandatului judecătoresc conține următoarele informații:

a) numele, prenumele și funcția persoanei care solicită emiterea mandatului judecătoresc;

b) datele de identitate ale persoanei supuse măsurii contrainformative, dacă acestea sunt cunoscute;

c) deținerea statutului de avocat sau de jurnalist de către persoana supusă măsurii contrainformative și circumstanțele de fapt care exclud incidența interdicției stabilite la alin. (6);

d) măsura contrainformativă pentru care se solicită autorizarea;

e) circumstanțele de fapt care servesc drept temei pentru realizarea măsurii contrainformative și, după caz, consecințele posibile ale acesteia;

f) argumentarea proporționalității măsurii contrainformative, pentru care se solicită autorizarea, cu restrângerea exercițiului drepturilor sau libertăților persoanei;

g) în cazul solicitării prelungirii termenului de realizare a măsurii contrainformative, temeiurile și motivele care justifică prelungirea;

h) rezultatele care se preconizează a fi obținute în urma realizării măsurii contrainformative;

- i) termenul de realizare a măsurii respective;
- j) locul desfășurării măsurii contrainformative;
- k) alte informații care au importanță pentru justificarea măsurii contrainformative și care ar susține legalitatea și temeinicia autorizării acesteia.
- (4) Examinarea demersului pentru emiterea mandatului judecătoresc are loc în decurs de 24 de ore. La solicitarea judecătorului, la examinarea demersului participă și ofițerul de informații, care dă explicațiile de rigoare. Pe parcursul examinării demersului, judecătorului, la solicitarea acestuia sau din inițiativa Serviciului, i se prezintă informațiile și materialele care justifică necesitatea realizării măsurii respective, fără a dezvălui datele de identificare ale persoanelor care colaborează confidențial cu Serviciul.
- (5) Pentru emiterea mandatului judecătoresc, judecătorul verifică suplimentar dacă:
- a) măsura solicitată urmărește un scop legitim;
- b) este imposibilă realizarea scopului prevăzut de prezenta lege pe altă cale;
- c) măsura solicitată este proporțională cu restrângerea exercițiului drepturilor și libertăților fundamentale.
- (6) Este interzisă autorizarea realizării măsurilor contrainformative:
- a) în privința raporturilor legale de asistență juridică dintre avocat și clientul său;
- b) în privința jurnaliștilor, cu scopul stabilirii surselor de informații ale acestora.
- (7) Informațiile care cad sub incidența alin. (6) și care au fost colectate accidental nu pot fi folosite de către Serviciu și se distrug, cu autorizarea judecătorului.
- (8) După verificarea legalității și a temeiniciei demersului indicat la alin. (2), judecătorul, prin încheiere, autorizează realizarea măsurii contrainformative sau respinge demersul. În temeiul încheierii privind autorizarea, judecătorul emite un mandat judecătoresc care este obligatoriu pentru executare.
- (9) Mandatul judecătoresc se transmite nu mai târziu de 24 de ore de la depunerea demersului pentru emiterea acestuia. Încheierea motivată este redactată și emisă în cel mult 48 de ore.
- (10) Încheierea indicată la alin. (8) conține următoarele informații: data și locul întocmirii încheierii; numele și prenumele judecătorului; numele, prenumele și funcția persoanei care solicită emiterea mandatului judecătoresc; organul care va realiza măsurile contrainformative; datele de identitate ale persoanei supuse măsurilor contrainformative, dacă acestea sunt cunoscute; temeiurile și motivele care justifică necesitatea realizării și, respectiv, autorizării măsurilor contrainformative; măsurile contrainformative autorizate; termenul de realizare a măsurilor contrainformative; locul desfășurării măsurilor contrainformative; alte informații care au importanță pentru justificarea autorizării măsurilor contrainformative.
- (11) Măsurile contrainformative care pot fi realizate doar cu mandat judecătoresc pot fi desfășurate, ca excepție, fără mandat judecătoresc, în baza ordonanței motivate a directorului Serviciului sau a directorului adjunct împuternicit, în cazul în care există circumstanțe excepționale care nu permit amânarea acesteia, iar mandatul judecătoresc nu poate fi obținut fără expunerea la un risc esențial de întârziere care să poată duce la pierderea informațiilor relevante sau să pună într-un pericol iminent securitatea statului sau a persoanelor. În acest caz, judecătorul este informat în termen de 24 de ore de la dispunerea măsurii contrainformative despre desfășurarea acesteia, prezentându-i-se toate informațiile și materialele în care este argumentată necesitatea realizării măsurii respective și circumstanțele excepționale care nu au permis amânarea acesteia. Dacă există temeiuri și motive suficiente, judecătorul confirmă, prin încheiere motivată, legalitatea realizării măsurii contrainformative. În caz contrar, judecătorul declară ilegalitatea desfășurării măsurii respective.

(12) Măsurile contrainformative inițiate în temeiul alin. (11) se desfășoară până la emiterea încheierii motivate a judecătorului, ulterior procedându-se conform încheierii respective.

(13) Concomitent cu confirmarea legalității realizării măsurilor contrainformative, judecătorul, la solicitarea directorului Serviciului sau a directorului adjunct împuternicit, emite mandat judecătoresc privind autorizarea continuării desfășurării acestora.

(14) La declararea ilegalității desfășurării măsurii contrainformative, realizarea măsurii respective se sistează.

(15) Încheierea motivată a judecătorului privind respingerea demersului pentru emiterea mandatului judecătoresc, precum și încheierea motivată privind declararea ilegalității desfășurării măsurii contrainformative pot fi contestate de către Serviciu cu recurs la Curtea Supremă de Justiție.

(16) Recursul indicat la alin. (15) se examinează de un complet de 3 judecători, în condițiile alin. (4).

(17) Recursul indicat la alin. (15) se depune în termen de 3 zile lucrătoare de la data emiterii încheierii motivate și conține temeiurile de fapt și de drept privind netemeinicia și/sau ilegalitatea încheierii contestate.

(18) După examinarea recursului indicat la alin. (15), completul Curții Supreme de Justiție, prin decizie:

a) admite recursul, casează încheierea și, după caz, emite mandat judecătoresc sau confirmă legalitatea realizării măsurilor contrainformative;

b) respinge recursul și menține încheierea.

(19) Redactarea și emiterea deciziei indicate la alin. (18) se efectuează în conformitate cu prevederile alin. (9).

**Articolul 13.** Condițiile speciale de realizare a măsurilor contrainformative autorizate prin mandat judecătoresc

(1) Realizarea măsurilor contrainformative se autorizează în temeiurile prevăzute la art. 10.

(2) În temeiurile indicate la art. 10 pct. 4)–6) poate fi autorizată realizarea doar a măsurilor contrainformative prevăzute la art. 9 alin. (1) pct. 1) și pct. 2) lit. e) și j).

(3) Cu acordul expres sau la cererea prealabilă, în formă scrisă, a persoanelor care contribuie la desfășurarea activității informative/contrainformative, pot fi realizate măsurile contrainformative prevăzute de prezenta lege, atât în privința acestora, cât și a rudelor și a membrilor familiilor lor, dacă există un pericol iminent la adresa vieții, sănătății sau a altor drepturi fundamentale ale acestora ori dacă realizarea măsurilor respective este necesară pentru prevenirea unei infracțiuni sau a unor consecințe nefavorabile care vizează persoanele menționate.

**Articolul 14.** Termenul pentru care se autorizează realizarea măsurilor contrainformative

(1) Măsurile contrainformative prevăzute la art. 9 alin. (1) pct. 2) care nu reprezintă măsuri de realizare unică, cu excepția celor prevăzute la art. 9 alin. (1) pct. 2) lit. a), se autorizează pentru un termen de până la 90 de zile, cu posibilitatea prelungirii acestuia cu perioade succesive, precum și cu perioade care nu se succed, de până la 90 de zile.

(2) Măsura contrainformativă prevăzută la art. 9 alin (1) pct. 2) lit. a) se autorizează pentru un termen de până la 30 de zile, cu posibilitatea prelungirii acestuia cu perioade succesive, precum și cu perioade care nu se succed, de până la 30 de zile.

(3) Durata totală a desfășurării unei măsuri contrainformative în privința unei persoane, dispusă cu privire la o faptă concretă, nu poate depăși, cumulativ, 24 de luni, iar finalizarea acesteia nu poate avea loc peste mai mult de 4 ani de

la inițierea măsurii. La fiecare solicitare privind prelungirea termenului de realizare a măsurii contrainformative, judecătorul are obligația de a examina temeiurile și motivele care justifică prelungirea acestuia, iar în cazul în care consideră că solicitarea respectivă nu este motivată, respinge prelungirea termenului.

(4) Desfășurarea măsurilor contrainformative trebuie să înceapă la data indicată în actul prin care s-a dispus realizarea acesteia sau, cel târziu, la data expirării termenului pentru care măsura respectivă a fost autorizată.

#### **Articolul 15.** Încetarea desfășurării măsurii contrainformative înainte de termen

Directorul Serviciului sau directorul adjunct împuternicit dispune, prin ordonanță, încetarea măsurii contrainformative înainte de expirarea termenului pentru care a fost emis mandat judecătoresc imediat ce au dispărut temeiurile și motivele care au justificat autorizarea măsurii. Despre încetarea înainte de termen a măsurii contrainformative și temeiurile încetării este informat judecătorul care a eliberat mandatul judecătoresc.

#### **Articolul 16.** Consemnarea măsurilor contrainformative

(1) După finalizarea desfășurării măsurii contrainformative și constatarea lipsei necesității continuării acesteia sau după încetarea acesteia înainte de termen, ofițerul de informații care a realizat măsura respectivă întocmește câte un proces-verbal pentru fiecare măsură contrainformativă autorizată, în care consemnează:

a) denumirea măsurii contrainformative realizate, locul și data desfășurării acesteia, după caz, ora începerii și finalizării acesteia, date cu privire la autorizarea măsurii sau cu privire la mandatul judecătoresc;

b) funcția, numele și prenumele ofițerului de informații care întocmește procesul-verbal. Dacă măsura contrainformativă a fost realizată nemijlocit de către ofițerii de informații din cadrul subunităților de asigurare a activității informative/contrainformative care fac parte din personalul criptic al Serviciului, în procesul-verbal se indică funcția, numele și prenumele conducătorului subunității respective, care verifică corectitudinea informațiilor indicate în procesul-verbal și îl semnează. În cadrul subunităților menționate se ține evidența strictă a ofițerilor de informații care au realizat măsuri contrainformative și au întocmit procese-verbale;

c) numele, prenumele și statutul persoanelor care au participat la realizarea măsurii. Datele respective nu se consemnează în procesul-verbal în cazul ofițerilor de informații din cadrul subunităților de asigurare a activității informative/contrainformative care fac parte din personalul criptic al Serviciului, precum și nici în cazul persoanelor care colaborează confidențial cu Serviciul;

d) faptele constatate, precum și acțiunile întreprinse în cadrul realizării măsurii contrainformative;

e) informațiile privind utilizarea mijloacelor tehnice, condițiile și modalitățile de aplicare a acestora, obiectele față de care au fost aplicate mijloacele respective, rezultatele obținute; mențiunea privind înregistrarea informațiilor acumulate.

(2) În cazul înregistrării rezultatelor măsurii contrainformative, la procesul-verbal se anexează suportul material al informațiilor.

(3) Procesul-verbal și suportul material al informațiilor se anexează la dosarul special.

#### **Articolul 17.** Verificarea legalității realizării măsurilor contrainformative de către judecător

(1) După finalizarea desfășurării măsurii contrainformative și constatarea lipsei necesității continuării acesteia sau

după încetarea acesteia înainte de termen, pentru verificarea respectării legalității măsurii, ofițerul de informații transmite, în termen de 10 zile lucrătoare, judecătorului care a autorizat măsura respectivă procesul-verbal privind măsura contrainformativă, la care anexează toate informațiile și materialele acumulate ca urmare a realizării acesteia.

(2) În procesul de verificare a respectării legalității, judecătorul stabilește dacă măsura contrainformativă a fost realizată: în privința persoanelor și pentru investigarea faptelor, indicate în demersul pentru emiterea mandatului judecătoresc; conform mandatului judecătoresc emis; cu respectarea termenelor de realizare.

(3) Dacă măsura a fost realizată în conformitate cu legislația, judecătorul, prin încheiere, confirmă legalitatea realizării măsurii contrainformative.

(4) În cazul în care judecătorul constată că măsura contrainformativă s-a desfășurat cu încălcarea vădită a drepturilor și libertăților persoanei ori au fost depășite prevederile mandatului judecătoresc, acesta, prin încheiere, declară drept nule rezultatele măsurii contrainformative și informează Procuratura Generală pentru investigarea încălcărilor admise.

(5) Încheierea privind declararea drept nule a rezultatelor măsurii contrainformative poate fi contestată cu recurs conform prevederilor art. 12.

(6) Originalul suportului material al informațiilor care conține înregistrările datelor obținute, după verificarea legalității conform prezentului articol, este sigilat de către judecător și se păstrează în cadrul Serviciului într-un mod care să asigure nonrepudierea informației și să excludă accesul ofițerului de informații care a desfășurat cercetarea cazului. La dosarul special se anexează o copie a suportului respectiv. Originalul suportului material se prezintă în cadrul controlului sau poate fi utilizat în alte scopuri, cu autorizarea judecătorului, la solicitarea motivată a directorului Serviciului sau directorului adjunct împuternicit.

**Articolul 18.** Utilizarea rezultatelor măsurilor contrainformative

(1) Rezultatele realizării măsurilor contrainformative sunt utilizate:

a) la realizarea atribuțiilor Serviciului;

b) la desfășurarea altor măsuri contrainformative.

(2) În cazul în care în urma desfășurării măsurilor contrainformative se constată că există bănueli rezonabile cu privire la săvârșirea unei infracțiuni sau pregătirea săvârșirii acesteia, printr-un raport este informat neîntârziat procurorul desemnat în acest sens din cadrul Procuraturii Generale.

(3) Rezultatele măsurilor contrainformative din cadrul unui dosar special pot fi utilizate în cadrul altui dosar special doar cu autorizarea judecătorului care a emis mandatul judecătoresc.

(4) Rezultatele realizării măsurilor contrainformative nu sunt admise ca probe în procesul penal.

**Articolul 19.** Confidențialitatea informației cu privire la

măsurile contrainformative și cele informative externe

(1) Informația cu privire la desfășurarea măsurilor contrainformative și celor informative externe, cu privire la personalul, sursele, sursele, mijloacele, metodele, planurile și rezultatele activității informative/contrainformative, precum și cu privire la organizarea, procedurile și tactica desfășurării măsurilor contrainformative și celor informative externe constituie secret de stat și poate fi desecretizată numai în conformitate cu legislația.

(2) Persoanele care au luat cunoștință, în virtutea funcției, statutului, circumstanțelor sau întâmplător, de desfășurarea măsurilor contrainformative sau celor informative externe ori de rezultatele acestora sunt obligate să păstreze confidențialitatea informațiilor respective.

(3) Orice divulgare neautorizată a informațiilor indicate la alin. (1) atrage răspunderea prevăzută de legislație.

#### **Articolul 20.** Informarea persoanei despre măsurile contrainformative realizate în privința sa

(1) După finalizarea cercetării cauzei și clasării dosarului special, dacă în cadrul acestuia au fost realizate măsurile contrainformative prevăzute la art. 9 alin. (1) pct. 2), Serviciul, în termen de 5 zile lucrătoare de la data clasării dosarului respectiv, informează persoanele în privința cărora au fost realizate măsurile respective. Materialele ce atestă informarea persoanelor se anexează la dosarul special.

(2) În fiecare caz în care este informată o persoană conform alin. (1), Serviciul notifică despre aceasta judecătorul care a emis mandatul judecătoresc.

(3) Informarea persoanei nu are loc dacă există motive întemeiate de a considera că aceasta ar putea expune unui risc esențial viața sau sănătatea persoanelor, ar periclita altă investigație în desfășurare, ar dăuna securității statului sau ar aduce prejudicii scopului pentru care au fost realizate măsurile contrainformative.

(4) Cu privire la existența motivelor menționate la alin. (3) ofițerul de informații care a efectuat cercetarea cauzei întocmește un raport în formă scrisă, în care specifică detaliat motivele respective și îl prezintă spre aprobare directorului Serviciului. Dacă raportul este aprobat, directorul Serviciului solicită judecătorului care a emis mandatul judecătoresc autorizarea neinformării persoanei.

(5) În urma examinării demersului directorului Serviciului indicat la alin. (4), judecătorul constată existența sau lipsa temeiurilor pentru neinformarea persoanei, stabilește dacă temeiurile respective au caracter permanent sau provizoriu și, după caz, admite autorizarea persoanei sau respinge demersul. În funcție de caracterul permanent sau provizoriu al temeiurilor constatate, judecătorul poate autoriza neinformarea permanentă sau neinformarea pentru o perioadă determinată, dar nu mai mare de 1 an. La expirarea perioadei respective, Serviciul este obligat să reevalueze temeiurile care au stat la baza neinformării persoanei și să întreprindă acțiunile necesare, în conformitate cu prevederile prezentului articol, inclusiv, după caz, să solicite autorizarea neinformării persoanei pentru o nouă perioadă. Respingerea demersului pentru autorizarea neinformării persoanei poate fi contestată de către Serviciu cu recurs, aplicându-se, corespunzător, prevederile art. 12.

(6) În cazul în care temeiurile care au stat la baza neinformării persoanei supuse măsurii contrainformative au dispărut înainte de expirarea perioadei stabilite, ofițerul de informații întocmește un raport în acest sens și îl prezintă spre aprobare directorului Serviciului, prin care solicită informarea neîntârziată a persoanei în privința căreia a fost realizată măsura respectivă. În cazul aprobării raportului, persoana este informată în condițiile alin. (1).

(7) Încheierea judecătorului privind autorizarea neinformării persoanei, precum și rapoartele aprobate de către directorul Serviciului se anexează la dosarul special.

### **Secțiunea a 2-a** **Măsurile contrainformative**

#### **Articolul 21.** Identificarea abonatului sau utilizatorului

unei rețele de comunicații electronice ori al unui serviciu al societății informaționale

(1) Identificarea abonatului sau utilizatorului unei rețele de comunicații electronice ori al unui serviciu al societății informaționale constă în stabilirea datelor de identificare ale abonatului sau ale utilizatorului unei rețele de comunicații electronice (identificatorul internațional al abonatului mobil (IMSI), numărul de telefon, numărul de serie al modului de identificare a abonatului (al cartelei SIM), adresa de internet protocol (IP), adresele fizice de prestare a serviciului fix) ori al unui serviciu al societății informaționale, precum și a datelor de identificare ale abonaților (numele, prenumele, IDNP, adresa), ori în stabilirea faptului dacă un serviciu de comunicații electronice este activ sau a fost activ la o anumită dată, ori în stabilirea, fără suportul furnizorului de servicii electronice, prezenței mijloacelor de comunicații electronice într-un moment dat la o persoană.

(2) În cazul în care măsura contrainformativă se realizează cu suportul unui furnizor de servicii electronice, acestuia i se prezintă extrasul din ordonanța corespunzătoare a directorului Serviciului sau a directorului adjunct împuternicit privind autorizarea măsurii, în care este indicat doar tipul informației care urmează a fi prezentată. După recepționarea extrasului din ordonanță, furnizorul de servicii electronice prezintă informațiile solicitate în cel mai restrâns termen, fără păstrarea copiei (inclusiv în format electronic) a răspunsului și datelor remise.

**Articolul 22.** Cercetarea domiciliului și/sau, după caz, instalarea în acesta a aparatelor care asigură supravegherea video/audio, fotografierea sau constatarea unor circumstanțe de fapt

(1) Cercetarea domiciliului și/sau, după caz, instalarea în acesta a aparatelor ce asigură supravegherea video/audio, fotografierea sau constatarea unor circumstanțe de fapt presupune accesul secret sau legendat în interiorul domiciliului, fără înștiințarea proprietarului, a posesorului sau a persoanei care locuiește sau se află în domiciliul respectiv, în scopul instalării aparatelor care să asigure supravegherea, precum și al studierii acestuia pentru descoperirea urmelor activității, persoanelor care prezintă interes, pentru obținerea altor informații necesare constatării circumstanțelor de fapt, observării și înregistrării evenimentelor care se desfășoară în domiciliu. Aparatele care asigură supravegherea efectuează interceptarea și înregistrarea de la distanță a informației sau înregistrarea informației nemijlocit în domiciliu, cu ridicarea ulterioară a acestora.

(2) În cadrul cercetării domiciliului este permisă prelevarea mostrelor pentru cercetarea comparativă, dacă aceasta nu va duce la deconspirarea măsurii contrainformative realizate.

(3) După expirarea termenului de realizare a măsurii sau în cazul încetării măsurii înainte de termen, este permis accesul secret sau legendat în domiciliu, cu autorizarea prealabilă a directorului Serviciului sau directorului adjunct împuternicit, pentru demontarea aparatelor respective. În acest caz, domiciliul nu se cercetează și nu se întreprind alte acțiuni decât cele de demontare a aparatelor. Cu privire la pătrunderea în domiciliu și demontarea aparatelor se întocmește un proces-verbal, în care se indică data și persoanele care au pătruns în domiciliu. Procesul-verbal se remite pentru informare judecătorului care a autorizat măsura respectivă.

(4) Demontarea aparatelor are loc într-un termen cât mai restrâns, după expirarea termenului de realizare a măsurii sau după încetarea măsurii. Se interzice utilizarea în orice mod a informației înregistrate după expirarea termenului de realizare a măsurii sau după încetarea măsurii, inclusiv vizualizarea sau audierea acesteia, informația respectivă fiind distrusă neîntârziat.

**Articolul 23.** Supravegherea domiciliului prin utilizarea mijloacelor tehnice

Supravegherea domiciliului prin utilizarea mijloacelor tehnice presupune supravegherea domiciliului din exterior, fără acordul proprietarului, al posesorului sau al persoanei care locuiește sau se află în domiciliul respectiv, prin utilizarea mijloacelor tehnice, în scopul stabilirii evenimentelor ce se desfășoară în interiorul domiciliului, a convorbirilor, a altor sunete sau circumstanțe de fapt, cu înregistrarea celor stabilite.

**Articolul 24.** Interceptarea comunicărilor

(1) Interceptarea comunicărilor reprezintă accesul și monitorizarea în regim de timp real a conținutului comunicărilor efectuate prin intermediul rețelelor de comunicații electronice sau al altor mijloace tehnice de comunicare, cu înregistrarea comunicărilor respective, precum și colectarea, înregistrarea în regim de timp real a tipului comunicării, a datelor de trafic (transfer) și a datelor de localizare asociate comunicărilor respective.

(2) Mandatul judecătoresc pentru autorizarea efectuării interceptării comunicărilor trebuie să conțină, suplimentar, identificatorii tehnici sau datele de identificare ale abonatului sau ale echipamentului prin intermediul căruia se realizează comunicările care urmează a fi interceptate.

**Articolul 25.** Efectuarea și certificarea interceptării comunicărilor

(1) Asigurarea tehnică a interceptării comunicărilor se realizează de către subunitatea specializată a Serviciului, cu utilizarea produselor de program sau a mijloacelor tehnice speciale conectate, în caz de necesitate, la echipamentul furnizorilor de rețele/de servicii de comunicații electronice și/sau la dispozitivele persoanei interceptate. Ofițerii de informații ai subunității care asigură tehnic interceptarea comunicărilor, angajații care efectuează nemijlocit ascultarea înregistrărilor, vizualizarea informațiilor comunicate, traducerea acestora, întocmirea stenogramei sunt obligați să păstreze secretul informațiilor obținute și poartă răspundere pentru încălcarea acestei obligații.

(2) Informația obținută în procesul interceptării comunicărilor poate fi ascultată și vizualizată de către ofițerul de informații în regim de timp real.

(3) Stenograma constituie reproducerea în formă scrisă a comunicărilor interceptate care au importanță pentru dosarul special. În stenograma comunicărilor se indică data, ora și durata comunicării, numele persoanelor ale căror comunicări sunt stenografiate, dacă sunt cunoscute, precum și alte date relevante. Stenograma se întocmește de către angajații subunității care asigură activitatea informativă/contrainformativă, iar în caz de necesitate sau la solicitarea ofițerului de informații care realizează măsura contrainformativă – personal de către acesta.

(4) Comunicările interceptate se stenografiază, de regulă, în limba în care a avut loc comunicarea. În cazul în care comunicarea a avut loc în altă limbă decât limba română, comunicarea se traduce în limba română de către un traducător.

(5) În cadrul subunității de asigurare a activității informative/contrainformative se ține evidența strictă a ofițerilor de informații care au avut acces la comunicarea interceptată, a angajaților care au întocmit stenograma sau au tradus comunicarea.

(6) Comunicările interceptate se păstrează integral pe suportul material oferit de către subunitatea specializată ofițerului de informații. Acest suport se păstrează în dosarul special. Accesul la suportul respectiv este supus evidenței, fiind înregistrate:

- a) numele, prenumele și funcția persoanei care a avut acces;
- b) data și ora inițierii accesului și data și ora finalizării accesului;
- c) mențiuni despre faptul dacă s-a ascultat/vizualizat informația înregistrată pe suportul material;
- d) temeiul/motivul ascultării/vizualizării informației;
- e) semnătura persoanei care a avut acces.

**Articolul 26.** Accesul la informația care se află sau se procesează într-un sistem informatic, pe dispozitive sau echipamente de comunicații și/sau monitorizarea acestora

(1) Accesul la informația care se află într-un sistem informatic, pe dispozitive sau echipamente de comunicații presupune întreprinderea unor acțiuni care să permită obținerea informației care se află într-un sistem informatic, pe dispozitive sau echipamente de comunicații sau înregistrarea informației necesare pe un suport material.

(2) Monitorizarea informației care se află sau se procesează într-un sistem informatic, pe dispozitive sau echipamente de comunicații presupune întreprinderea unor măsuri care să permită monitoringul, în regim de timp real, al acțiunilor care se întreprind într-un sistem informatic, în dispozitiv sau echipament, să permită obținerea informației care se prelucrează, precum și a datelor informatice asociate acțiunilor respective.

(3) Accesul la informația care se află sau se procesează într-un sistem informatic, pe dispozitive sau echipamente de comunicații și/sau monitorizarea acestora poate fi efectuată:

- a) prin stabilirea unui canal permanent sau temporar de conexiune fizică dintre subunitatea specializată a Serviciului și echipamentul persoanei fizice/juridice care deține sistemul informatic, dispozitivele sau echipamentele de comunicații ori suportul tehnic respectiv;
- b) prin intermediul unor produse de program;
- c) prin prezentarea nemijlocită către deținătorul sistemului informatic, al dispozitivelor sau echipamentelor de comunicații ori al suportului tehnic a extrasului din mandatul judecătoresc corespunzător, eliberat de către judecător concomitent cu mandatul judecătoresc, în care este indicată tipul de informații care urmează a fi prezentate.
- (4) Accesul la informația care se află sau se procesează într-un sistem informatic sau monitorizarea acesteia nu poate fi realizat conform prevederilor prezentului articol dacă prezenta lege prevede o altă modalitate de obținere a informației respective.

**Articolul 27.** 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 suportul furnizorilor de servicii de comunicații electronice, 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, pentru identificarea destinației, tipului, datei, orei și duratei comunicației electronice, pentru identificarea echipamentului de comunicații electronice al utilizatorului sau a altui dispozitiv utilizat pentru comunicație, pentru identificarea coordonatelor echipamentului terminal de comunicații mobile, informație, în special, despre:

- a) numerele de telefon înregistrate pe numele unei persoane;
- b) serviciile de comunicații electronice prestate utilizatorului;

- c) sursa de comunicații electronice (numărul de telefon sau adresa de internet protocol (IP) ale apelantului);
  - d) destinația comunicației electronice (numărul de telefon sau adresa de internet protocol (IP) ale apelatului; numărul de telefon spre care este redirecționat apelul);
  - e) 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 avut loc un răspuns sau a avut loc o intervenție legată de gestionarea rețelei;
  - f) echipamentul de comunicații electronice al utilizatorului sau un alt dispozitiv utilizat pentru comunicație (identificatorul internațional al echipamentului mobil (IMEI) al apelantului și cel al apelatului; adresa media acces control (adresa MAC) a echipamentului de acces la serviciile fixe amplasat în locația clientului (CPE); în cazul serviciilor preplătite anonime – data și ora la care a fost inițial activat serviciul și denumirea locației (Cell ID) din care a fost activat serviciul);
  - g) locația echipamentului de comunicații mobile (denumirea locației (Cell ID) de la începutul comunicației; locația geografică a celei prin referință la denumirea locației, în perioada în care datele sunt reținute).
- (2) Colectarea informației de la furnizorii de servicii de comunicații electronice se realizează prin prezentarea nemijlocită către furnizorii de servicii de comunicații electronice a extrasului din mandatul judecătoresc corespunzător, eliberat de către judecător concomitent cu mandatul judecătoresc, în care se indică doar tipul de informații care urmează a fi prezentate.

**Articolul 28.** Reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimerilor poștale

- (1) Reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimerilor poștale constă în următoarele acțiuni, întreprinse fără înștiințarea expeditorului și destinatarului trimerilor poștale:
- a) oprirea livrării trimerii poștale pentru o perioadă strict determinată sau relativ determinată ori livrarea trimerii poștale la o anumită dată sau într-un anumit interval de timp;
  - b) accesarea și verificarea trimerii poștale, vizualizarea și înregistrarea informației existente, identificarea obiectelor sau substanțelor ce se află în trimerii poștală.
- (2) În cadrul realizării măsurilor tehnico-științifice care să permită identificarea obiectelor sau a substanțelor din trimerii poștală ori a altor circumstanțe de fapt;
- a) efectuarea constatărilor tehnico-științifice care să permită identificarea obiectelor sau a substanțelor din trimerii poștală ori a altor circumstanțe de fapt;
  - b) copierea, înregistrarea pe suport material, cu ajutorul mijloacelor tehnice, a informațiilor care se conțin în trimerii poștală;
  - c) prelevarea mostrelor.
- (3) Mandatul judecătoresc pentru reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimerilor poștale trebuie să conțină denumirea instituției poștale asupra căreia se pune obligația de a reține trimerii poștale, numele și prenumele persoanei sau persoanelor ale căror trimerii poștale trebuie să fie reținute, adresele exacte ale persoanelor respective, dacă sunt cunoscute, sau alte elemente caracteristice, în baza cărora se vor putea identifica trimerii poștale, genul de trimerii poștale față de care este orientată măsura contrainformativă.
- (4) Concomitent cu mandatul judecătoresc, judecătorul eliberează și un extras din acesta care se transmite conducătorului instituției poștale sau furnizorului de trimerii poștale, pentru care executarea măsurii indicate în extrasul respectiv este obligatorie.

(5) Conducătorul instituției poștale sau furnizorul de trimiteri poștale informează neîntârziat ofițerul de informații despre reținerea trimiterilor poștale indicate în extrasul din mandatul judecătoresc, fiind obligat să asigure și să păstreze confidențialitatea măsurii contrainformative realizate.

**Articolul 29.** Înregistrarea video/audio a conținutului comunicărilor

Înregistrarea video/audio a conținutului comunicărilor presupune înregistrarea secretă video/audio a comunicărilor transmise de persoane în spații deschise, în locuri publice sau în încăperi care nu constituie domiciliu, precum și a comunicărilor transmise către sau în prezența unui offer de informații sau a unei persoane care colaborează confidențial cu Serviciul, fără a cunoaște statutul acestora.

**Articolul 30.** Blocarea accesului la rețelele de comunicații electronice pentru un sistem informatic, un dispozitiv sau un echipament ori pentru o societate informațională, blocarea unor servicii de comunicații electronice

(1) Blocarea accesului la rețelele de comunicații electronice pentru un sistem informatic, un dispozitiv sau un echipament ori pentru o societate informațională, blocarea unor servicii de comunicații electronice presupun:

- a) blocarea posibilității accesării unor rețele de comunicații electronice de un sistem informatic, un dispozitiv sau un echipament ori de o societate informațională;
- b) suspendarea unui serviciu de comunicații electronice sau a unui serviciu al societății informaționale pentru un număr de telefon, pentru o adresă statică de internet protocol (IP), pentru o persoană sau o adresă fizică.

(2) Acțiunile prevăzute la alin. (1) lit. a) se efectuează de către Serviciu cu utilizarea produselor de program sau a mijloacelor tehnice speciale, iar cele prevăzute la alin. (1) lit. b) – de către furnizorii de servicii de comunicații electronice, la prezentarea extrasului din mandatul judecătoresc corespunzător.

**Articolul 31.** Ridicarea operativă

Ridicarea operativă reprezintă ridicarea secretă, cu ulterioara returnare secretă, a bunurilor, documentelor, suporturilor materiale de informații cu scopul examinării și analizării acestora, al efectuării constatării tehnico-științifice, al colectării informațiilor necesare, precum și pentru prelevarea și examinarea mostrelor.

**Articolul 32.** Accesul la informația financiară sau monitorizarea tranzacțiilor financiare

(1) Accesul la informația financiară reprezintă obținerea de la bănci, de la alte persoane/organizații care intermediază tranzacțiile financiare sau de la alte instituții competente a înscrisurilor sau informațiilor, aflate în posesia acestora, referitoare la depuneri, la conturi sau la circulația unor anumite mijloace bănești.

(2) Monitorizarea tranzacțiilor financiare reprezintă operațiunile prin care se asigură cunoașterea, inclusiv în regim de timp real, a conținutului tranzacțiilor financiare efectuate prin intermediul băncilor, al altor persoane/organizații care intermediază tranzacțiile financiare sau al altor instituții competente, referitoare la depuneri, la conturi sau la tranzacțiile unei persoane ori la circulația unor anumite mijloace bănești.

(3) Băncilor, altor persoane/organizații care intermediază tranzacțiile financiare și altor instituții competente li se prezintă extrasul din mandatul judecătoresc corespunzător, în care se indică doar tipul de informații care urmează a fi prezentate și, după caz, termenul de efectuare a monitorizării.

**Articolul 33.** Urmărirea vizuală și/sau documentarea cu ajutorul metodelor și mijloacelor tehnice, precum și localizarea sau urmărirea prin sistemul de poziționare globală ori prin alte mijloace tehnice

(1) Urmărirea vizuală și/sau documentarea cu ajutorul metodelor și mijloacelor tehnice reprezintă observarea, și cu fixarea observațiilor, a unor imobile, spații, mijloace de transport, bunuri, a acțiunilor/inacțiunilor persoanei, a altor circumstanțe de fapt care se desfășoară, cu sau fără utilizarea mijloacelor tehnice de înregistrare.

(2) Localizarea sau urmărirea prin sistemul de poziționare globală sau prin alte mijloace tehnice constă în folosirea mijloacelor tehnice pentru determinarea locului unde se află sau s-a aflat persoana sau obiectul, precum și în monitorizarea deplasării sau aflării acestora, cu înregistrarea informației obținute.

### **Capitolul III**

## **ACTIVITATEA INFORMATIVĂ EXTERNĂ**

**Articolul 34.** Sarcinile activității informative externe

Activitatea informativă externă are sarcina de identificare, prevenire și contracarare a factorilor de risc și a amenințărilor externe sau de proveniență externă la adresa securității naționale, a consecințelor în cazul materializării acestora, precum și de protecție și promovare a intereselor strategice ale Republicii Moldova și ale partenerilor săi.

**Articolul 35.** Măsurile informative externe

Serviciul și Ministerul Apărării sunt în drept să creeze, să achiziționeze, să dețină și să utilizeze tactici, metode, mijloace și surse specifice pentru planificarea, culegerea, verificarea, evaluarea, prelucrarea analitică, stocarea, păstrarea și valorificarea informațiilor necesare realizării activității informative externe.

**Articolul 36.** Condițiile și modul de desfășurare a activității informative externe

(1) Desfășurarea măsurilor informative externe se admite doar în scopul realizării sarcinilor prevăzute de prezenta lege.

(2) Realizarea măsurilor informative externe și aplicarea tacticilor, metodelor și mijloacelor specifice de desfășurare a activității informative externe se efectuează în conformitate cu actele interne ale Serviciului sau, după caz, ale Ministerului Apărării.

### **Capitolul IV**

## **ASIGURAREA FINANCIARĂ, TEHNICO-MATERIALĂ ȘI ȘTIINȚIFICĂ A ACTIVITĂȚII INFORMATIVE/CONTRAINFORMATIVE**

**Articolul 37.** Asigurarea financiară și tehnico-materială a activității informative/contrainformative

- (1) Asigurarea financiară și tehnico-materială a activității informative/contrainformative se efectuează din contul mijloacelor financiare alocate Serviciului sau, după caz, Ministerului Apărării din bugetul de stat, conform legislației.
- (2) Proiectele de acte cu privire la asigurarea financiară și tehnico-materială a activității informative/contrainformative se examinează și se aprobă de către autoritățile competente în ședințe închise, constituie secret de stat și nu pot fi făcute publice.

**Articolul 38.** Asigurarea științifică a activității informative/contrainformative

- (1) În cadrul desfășurării activității informative/contrainformative pot fi efectuate constatări tehnico-științifice sau expertize extrajudiciare.
- (2) Constatarea tehnico-științifică efectuată în cadrul activității informative/contrainformative reprezintă activitatea desfășurată de un specialist în scopul explicării unor fapte sau circumstanțe, al constatării unor situații, care necesită deținerea unor competențe și cunoștințe speciale.
- (3) În cadrul efectuării constatării tehnico-științifice, specialistul nu soluționează chestiuni cu caracter juridic.
- (4) Constatările tehnico-științifice se dispun și se efectuează în conformitate cu prevederile prezentei legi.
- (5) Expertizele extrajudiciare se dispun și se efectuează în conformitate cu legislația în vigoare.

**Articolul 39.** Temeiurile pentru dispunerea și efectuarea constatării tehnico-științifice

- (1) Constatarea tehnico-științifică se efectuează în temeiul dispoziției scrise a ofițerului de informații sau, după caz, a militarului prin contract, care desfășoară activitate informativă/contrainformativă, aprobată de către conducătorul subunității specializate.
- (2) În dispoziția cu privire la efectuarea constatării tehnico-științifice se menționează, în mod obligatoriu, circumstanțele de fapt și chestiunile la care urmează să dea răspuns specialistul și se anexează materialele care urmează a fi cercetate.

**Articolul 40.** Subiecții abilitați cu dreptul de efectuare a constatărilor tehnico-științifice

- (1) Constatarea tehnico-științifică este efectuată de către specialiștii din cadrul Serviciului sau, după caz, al Ministerului Apărării.
- (2) În cazul în care în cadrul Serviciului sau al Ministerului Apărării nu activează specialiști care să dețină competențe și cunoștințe speciale într-un anumit domeniu de activitate sau dacă complexitatea cauzei impune, efectuarea constatării tehnico-științifice poate fi solicitată specialiștilor din afara Serviciului sau Ministerului Apărării.
- (3) Constatarea tehnico-științifică poate fi solicitată specialiștilor din afara Serviciului sau Ministerului Apărării doar cu consimțământul acestora, în baza unui acord sau contract.

#### **Articolul 41.** Organizarea și efectuarea constatării tehnico-științifice

(1) La recepționarea dispoziției cu privire la efectuarea constatării tehnico-științifice, conducătorul subunității de constatare tehnico-științifică desemnează un specialist care deține competențele și cunoștințele necesare pentru efectuarea acesteia.

(2) Specialistul desemnat conform alin. (1) înregistrează dispoziția respectivă și, în termen de 3 zile, își expune opinia dacă deține competențele și cunoștințele necesare pentru a efectua constatarea.

(3) În caz de necesitate, specialistul poate solicita informații și materiale suplimentare de la ofițerul de informații sau militarul prin contract care a dispus efectuarea constatării.

(4) După examinarea materialelor și întreprinderea acțiunilor care se impun, specialistul întocmește un raport de constatare tehnico-științifică în care își expune opinia asupra chestiunilor prezentate spre examinare, explică faptele, circumstanțele neclare, constată situațiile de fapt.

(5) Raportul de constatare tehnico-științifică conține următoarele informații:

- a) datele de identificare ale specialistului;
- b) datele cu privire la studiile sau calificările deținute de specialist pentru efectuarea cercetărilor, precum și la experiența în domeniu;
- c) datele cu privire la ofițerul de informații sau militarul prin contract care a dispus efectuarea constatării;
- d) chestiunile prezentate spre examinare;
- e) circumstanțele de fapt;
- f) cercetările efectuate, cu descrierea metodelor de cercetare aplicate;
- g) concluziile.

#### **Capitolul V**

### **CONTROLUL ACTIVITĂȚII INFORMATIVE/CONTRAINFORMATIVE**

#### **Articolul 42.** Controlul parlamentar

(1) Controlul parlamentar asupra activității informative/contrainformative este efectuat de către subcomisia parlamentară pentru exercitarea controlului parlamentar asupra activității Serviciului (în continuare – *subcomisie parlamentară*), în conformitate cu prevederile Regulamentului Parlamentului, adoptat prin Legea nr. 797/1996, și ale regulamentului de activitate al subcomisiei respective, aprobat prin hotărârea Parlamentului.

(2) Subcomisia parlamentară informează sistematic despre activitatea sa comisia parlamentară pentru securitatea națională, apărare și ordinea publică.

(3) Până la prezentarea în ședința în plin a Parlamentului a raportului anual privind activitatea Serviciului, directorul Serviciului prezintă subcomisiei parlamentare, în ședință închisă, un raport cu privire la activitatea informativă/contrainformativă, care să cuprindă, în mod obligatoriu, informații despre:

- a) numărul total al măsurilor contrainformative dispuse, realizate și respinse, pe fiecare măsură în parte;
  - b) numărul dosarelor speciale deschise și al celor clasate;
  - c) numărul persoanelor informate despre realizarea în privința acestora a măsurilor contrainformative;
  - d) date privind eventualele încălcări admise de ofițerii de informații în executarea prevederilor prezentei legi.
- (4) În cadrul ședinței indicate la alin. (3) pot fi prezentate informații despre operațiunile finalizate realizate de către

Serviciu dacă dezvăluirea acestora nu va dauna securității statului. Informații despre operațiunile în derulare nu se prezintă.

(5) După prezentarea informației conform alin. (3), membrii subcomisiei parlamentare pot adresa întrebări cu privire la activitatea informativă/contrainformativă desfășurată de către Serviciu în anul precedent. În baza informației prezentate, subcomisia parlamentară poate formula recomandări privind activitatea informativă/contrainformativă a Serviciului.

(6) După examinarea informației privind activitatea informativă/contrainformativă a Serviciului conform prevederilor prezentului articol, subcomisia parlamentară ia act de informația prezentată și publică pe pagina web oficială a Parlamentului rezultatele controlului activității informative/contrainformative, în care, în mod obligatoriu, sunt specificate numărul măsurilor contrainformative realizate de către Serviciu, pe fiecare măsură în parte, și numărul încheierilor privind respingerea demersului pentru emiterea mandatului judecătoresc, pe fiecare măsură în parte, într-un mod în care să nu fie dezvăluite informațiile atribuite la secret de stat.

(7) În cazul în care subcomisia parlamentară constată că există bănuiele rezonabile privind admiterea încălcărilor grave în activitatea informativă/contrainformativă a Serviciului, aceasta poate solicita efectuarea unei anchete parlamentare sau poate sesiza Procurorul General.

(8) Raportul anual privind activitatea Serviciului conține, în mod obligatoriu, un compartiment cu privire la activitatea informativă/contrainformativă desfășurată de către Serviciu și la măsurile întreprinse de către acesta în urma recomandărilor subcomisiei parlamentare.

#### **Articolul 43.** Controlul exercitat de către procuror

(1) Controlul exercitat de către procuror asupra activității contrainformative se efectuează de către procurorii din cadrul Procuraturii Generale, abilitați în acest sens de către Procurorul General.

(2) Controlul se efectuează fie în baza petițiilor depuse de către persoanele ale căror drepturi și interese legitime se presupune că au fost încălcate, fie, din oficiu, în cazul în care procurorul i-au devenit cunoscute informații despre încălcarea legislației în legătură cu desfășurarea măsurilor contrainformative, dacă faptele respective pot constitui infracțiuni.

(3) În cadrul controlului exercitat de către procuror, informația privind persoanele care au colaborat sau colaborează confidențial cu Serviciul poate fi prezentată doar procurorului din categoria celor menționați la alin. (1), abilitat în acest sens prin ordinul Procurorului General. Informația respectivă se prezintă doar dacă aceasta este în legătură directă cu obiectul controlului efectuat și doar dacă este absolut necesară realizării controlului respectiv.

(4) Înainte de a fi abilitați să exercite controlul asupra activității contrainformative, procurorilor li se perfectează dreptul de acces la secretul de stat, dacă nu dispun de dreptul respectiv.

#### **Articolul 44.** Controlul intern

(1) Controlul intern asupra activității informative/contrainformative se realizează de către directorul Serviciului, directorul adjunct împuternicit în acest sens și, după caz, de ministrul apărării, inclusiv prin intermediul subunităților interne de control și al conducătorilor subunităților specializate.

(2) Persoanele care nu sunt implicate nemijlocit în lucrul cu persoanele care colaborează confidențial cu Serviciul sau cu Ministerul Apărării, inclusiv directorul și directorii adjuncți ai Serviciului, ministrul apărării, nu sunt în drept să

solicite informații despre identitatea reală a persoanelor care colaborează confidențial cu Serviciul sau cu Ministerul Apărării dacă aceasta nu este dictată de o necesitate stringentă de serviciu.

#### **Articolul 45.** Controlul judecătoresc

Controlul judecătoresc se efectuează prin verificarea temeiniciei realizării măsurilor contrainformative la emiterea mandatului judecătoresc sau în cazul în care se evaluează legalitatea acțiunilor efectuate.

#### **Articolul 46.** Controlul extern asupra cheltuirii mijloacelor financiare

Controlul extern asupra cheltuirii mijloacelor financiare alocate pentru asigurarea realizării activității informative/contrainformative se efectuează de către Curtea de Conturi, în ședință închisă, în condițiile Legii nr. 245/2008 cu privire la secretul de stat. Controlul respectiv se efectuează în limite care să nu permită dezvăluirea conținutului, formelor, tacticii, metodelor și mijloacelor activității informative/contrainformative, a datelor de identificare ale persoanelor care colaborează confidențial cu Serviciul sau cu Ministerul Apărării, a operațiunilor în derulare și a operațiunilor care au fost finalizate, dar a căror dezvăluire ar putea dauna securității statului.

#### **Articolul 47.** Controlul asupra prelucrării datelor cu caracter personal în cadrul activității informative/contrainformative

Prelucrarea și controlul asupra prelucrării datelor cu caracter personal în cadrul activității informative/contrainformative se efectuează în condițiile legislației privind protecția datelor cu caracter personal, ținând cont de particularitățile prevăzute de prezenta lege.

### **Capitolul VI**

## **DISPOZIȚII FINALE ȘI TRANZITORII**

#### **Articolul 48**

- (1) Prezenta lege intră în vigoare după 90 de zile de la data publicării acesteia în Monitorul Oficial al Republicii Moldova, cu excepția prezentului articol care intră în vigoare la data publicării.
- (2) În termen de 60 de zile de la data publicării prezentei legi:
  - a) președintele Curții de Apel Chișinău și cel al Curții Supreme de Justiție vor stabili numărul de judecători care vor fi abilitați cu competența de a emite mandate judecătorești și de a examina recursuri, în sensul prezentei legi, vor desemna judecătorii respectivi și vor organiza procesul de repartizare aleatorie a demersurilor/recursurilor Serviciului;
  - b) judecătorii desemnați conform prevederilor lit. a) vor iniția procesul de perfectare a dreptului de acces la secretul de stat, dacă nu dispun de acesta;
  - c) Procurorul General va desemna procurorii abilitați cu dreptul de control asupra activității contrainformative.
- (3) Guvernul, în termen de 6 luni de la data publicării prezentei legi, va prezenta Parlamentului propuneri privind aducerea legislației în vigoare în concordanță cu aceasta.

## **PREȘEDINTELE PARLAMENTULUI**

**Lilian CARP**  
**Președintele Comisiei**