



**CENTRUL NAȚIONAL PENTRU PROTECȚIA DATELOR  
CU CARACTER PERSONAL AL REPUBLICII MOLDOVA**



MD-2004, mun. Chișinău, str. Serghei Lazo, 48, tel: +373-22-820801, fax: +373-22-820807, [www.datepersonale.md](http://www.datepersonale.md)

Nr. 04-06/245

„27” ianuarie 2023

**Comisia securitate națională, apărare și ordine  
publică a Parlamentului Republicii Moldova**  
[csn@parlament.md](mailto:csn@parlament.md)

Prin prezenta, în contextul procesului de consultare publică, Centrul Național pentru Protecția Datelor cu Caracter Personal (CNPDCP), prezintă opinia asupra proiectului de lege privind activitatea contrainformativă și activitatea informativă externă, înaintat cu titlu de inițiativa legislativă nr. 422 la 17 noiembrie 2022.

În context, comunicăm următoarele:

***I. Cu privire la aspectele de constituționalitate a prevederilor proiectelor și a compatibilității cu tratatele internaționale în domeniul drepturilor omului ratificate de Republica Moldova:***

*În partea ce vizează respectarea prevederilor Convenției pentru apărarea drepturilor omului și a libertăților fundamentale (Convenție) și a protocoalelor adiționale, ratificate prin Hotărârea Parlamentului Republicii Moldova nr. 1298/1997, precum și jurisprudența Curții Europene a Drepturilor Omului:*

Conform art. 4 din Constituția Republicii Moldova, dispozițiile constituționale privind drepturile și libertățile fundamentale ale omului se interpretează și se aplică în concordanță cu pactele și tratatele la care Republica Moldova este parte. Subsecvent, legea supremă stabilește că dacă există neconcordanțe între pactele și tratatele privitoare la drepturile fundamentale ale omului la care Republica Moldova este parte și legile ei interne, prioritate au reglementările internaționale.

Astfel, art. 15 - 53 din Constituția Republicii Moldova consacră și garantează drepturi și libertăți unanim recunoscute de tratatele internaționale, inclusiv dreptul la viața intimă, familială și privată, dreptul la inviolabilitatea domiciliului, precum și secretul corespondenței.

Concomitent, art. 54 din Constituția Republicii Moldova prevede că exercițiul drepturilor și libertăților nu poate fi supus altor restrângeri decât celor prevăzute de lege, care corespund normelor unanim recunoscute ale dreptului internațional și sunt necesare într-o societate democratică. În acest sens, legea supremă stabilește că restrângerea unor drepturi și libertăți trebuie să fie proporțională cu situația care a determinat-o și nu poate atinge însuși existența acestora. Însă, în nici un caz nu pot fi restrânse drepturile proclamate la art. 20-24 din Constituție, printre care dreptul de acces liber la justiție.

Prin urmare, reieșind din prevederile constituționale enumerate supra, restrângerea exercițiului dreptului la viața intimă, familială și privată, dreptului la inviolabilitatea domiciliului, precum și a dreptului la secretul corespondenței poate fi efectuată doar în conformitate cu prevederile Convenției pentru apărarea drepturilor omului și a libertăților fundamentale (Convenție) și a protocoalelor adiționale ratificate prin Hotărârea Parlamentului nr. 1298/1997, și nu în ultimul rând, ținând cont de jurisprudența Curții Europene a Drepturilor

Omului (CtEDO, Curtea) care este cu caracter obligatoriu și la care se va face trimitere în continuare.

Art. 8 din Convenție - dreptul la respectarea vieții private și de familie

„1. Orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului său și a corespondenței sale.

2. Nu este admis amestecul unei autorități publice în exercitarea acestui drept decât în măsura în care acest amestec este prevăzut de lege și dacă constituie o măsură care, într-o societate democratică, este necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei, ori protejarea drepturilor și libertăților altora.

**Scopul** principal al art. 8 este protejarea indivizilor împotriva ingerințelor arbitrare în exercitarea dreptului la respectarea vieții private și de familie, a domiciliului și a corespondenței. Condițiile în care poate exista o ingerință, din partea unui stat, în exercitarea unui drept protejat sunt stabilite la art. 8 § 2, și anume: **în interesul securității naționale**, al siguranței publice sau al bunăstării economice a țării, pentru apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei ori protejarea drepturilor și libertăților altora. **Sunt permise limitări în cazul în care acestea sunt „conforme cu legea” sau „prevăzute de lege” și sunt „necesare într-o societate democratică” pentru atingerea unuia dintre obiectivele menționate anterior.**

CtEDO a afirmat în repetate rânduri că orice ingerință a unei autorități publice în exercitarea dreptului unei persoane la respectarea vieții private și a corespondenței trebuie să fie „prevăzută de lege”. Această expresie nu implică doar respectarea legislației interne, ci **se referă, de asemenea, la calitatea acestei legislații, care trebuie să fie compatibilă cu statul de drept** (*Halford împotriva Regatului Unit, pct. 49*).

**Legislația națională trebuie să fie clară, previzibilă și suficient de accesibilă** (*Silver și alții împotriva Regatului Unit, pct. 87*). Acest lucru include un caracter suficient de previzibil pentru a permite persoanelor particulare să acționeze în conformitate cu legea, precum și o delimitare clară a marjei de apreciere a autorităților publice. De exemplu, în contextul măsurilor de supraveghere, Curtea a precizat că legea trebuie să fie redactată în termeni suficient de clari pentru a le furniza cetățenilor indicii adecvate privind circumstanțele și condițiile în care autoritățile au dreptul să recurgă la orice măsuri de supraveghere secretă și de colectare de date (*Shimovolos împotriva Rusiei, pct. 68*).

**Cerința de claritate** se aplică marjei de apreciere exercitate de autoritățile publice. Legislația internă trebuie să indice cu o claritate rezonabilă sfera și modul de exercitare a discreției relevante conferite autorităților publice, astfel încât să li se asigure persoanelor private gradul minim de protecție de care beneficiază în temeiul principiului statului de drept într-o societate democratică (*Piechowicz împotriva Poloniei, pct. 212*).

În ceea ce privește **previzibilitatea**, expresia „prevăzut de lege” implică așadar, în special, faptul că dreptul intern trebuie să fie redactat suficient de previzibil pentru a le furniza persoanelor particulare indicii adecvate privind circumstanțele și condițiile în care autoritățile au dreptul să recurgă la măsuri care le afectează drepturile protejate de Convenție [*Fernández Martínez împotriva Spaniei (MC), pct. 117*].

Art. 8 § 2 din Convenție enumeră **scopurile legitime care pot justifica o ingerință** în exercitarea drepturilor protejate de art. 8: „**este necesară pentru securitatea națională,**

siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei, ori protejarea drepturilor și libertăților altora”. Curtea a stabilit că **este sarcina guvernului pârât să demonstreze că ingerința a avut un scop legitim** [*Mozer împotriva Republicii Moldova și Rusiei (MC)*, pct. 194].

Ulterior, Curtea a afirmat că, pentru a stabili dacă măsurile atacate erau „**necesare într-o societate democratică**”, va analiza, în lumina cauzei respective în ansamblul său, dacă motivele invocate pentru justificarea măsurilor sunt relevante și suficiente și dacă măsurile au fost proporționale cu scopurile legitime urmărite (*Z împotriva Finlandei*, pct. 94). Curtea a oferit clarificări suplimentare privind această cerință, afirmând că noțiunea de „necesitate” în sensul art. 8 implică faptul că **ingerința trebuie să corespundă unei nevoi sociale imperioase și, în special, că trebuie să rămână proporțională cu scopul legitim urmărit**. Pentru a stabili dacă o ingerință a fost „necesară”, Curtea ține seama de marja de apreciere lăsată autorităților statului, însă **este obligația statului pârât să demonstreze existența unei nevoi sociale imperioase, care a stat la baza ingerinței** (*Piechowicz împotriva Poloniei*, pct. 212). „

În ceea ce privește măsurile generale adoptate de guvernul național, din jurisprudența Curții reiese că, pentru a stabili proporționalitatea unei măsuri generale, Curtea trebuie să evalueze în principal opțiunile legislative care stau la baza acesteia. În acest sens, **calitatea controlului parlamentar și judiciar al necesității măsurii este deosebit de importantă**, inclusiv aplicarea marjei de apreciere relevantă. **Garanțiile procedurale de care dispune persoana particulară sunt deosebit de importante pentru a determina dacă statul pârât și-a depășit sau nu marja de apreciere atunci când a stabilit cadrul de reglementare**. Curtea trebuie să examineze, în special, dacă procesul decizional finalizat prin măsuri care constituie o ingerință a fost echitabil și a permis respectarea adecvată a intereselor garantate unei persoane de către art. 8 (*A.-M.V. împotriva Finlandei*, pct. 82-84).

Curtea a hotărât că, **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, fără să știe acest lucru și fără să aibă posibilitatea de a exercita o cale de atac la nivel național sau în fața organelor Convenției** (*Klass și alții împotriva Germaniei*, pct. 36). Un reclamant poate pretinde că este victima unei încălcări ocazionate de simpla existență a unor măsuri de supraveghere secretă sau a unei legislații care permite instituirea unor astfel de măsuri, în cazul în care sunt îndeplinite anumite condiții [*Roman Zakharov împotriva Rusiei (MC)*, pct. 171-172]. În această cauză, Curtea a constatat că abordarea din *cauza Kennedy* este cel mai bine adaptată la **necesitatea de a garanta că natura secretă a măsurilor de supraveghere nu are ca rezultat măsuri imposibil de contestat în mod eficient** și care se află în afara sferei controlului exercitat de autoritățile judiciare naționale și de Curte (*Kennedy împotriva Regatului Unit*, pct. 124).

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 [*Weber și Saravia împotriva Germaniei (dec.)*, pct. 78]. 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 nu beneficiază de o putere discreționară nelimitată de a supune persoanele aflate în jurisdicția lor unor măsuri de supraveghere secretă**. Curtea a afirmat că statele contractante nu pot adopta, în numele luptei împotriva spionajului și a terorismului, orice măsură pe care o consideră adecvată, 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

[*Klass și alții împotriva Germaniei, pct. 42; Szabó și Vissy împotriva Ungariei, pct. 72-73*]. O astfel de ingerință trebuie susținută de motive pertinente și suficiente și trebuie să fie proporțională cu obiectivul sau obiectivele legitime urmărite (*Segerstedt-Wiberg și alții împotriva Suediei, pct. 88*).

Legislația internă ar trebui să ofere garanții suficiente de precise, eficiente și cuprinzătoare cu privire la dispunerea și executarea măsurilor de supraveghere, **precum și la posibilitățile de reparare a consecințelor acestora** (*Szabó și Vissy împotriva Ungariei*).

În prima hotărâre pronunțată în materie de supraveghere secretă, *Klass și alții împotriva Germaniei, pct. 48*, Curtea a precizat, în special următoarele: „În prezent, societățile democratice sunt amenințate de forme extrem de sofisticate de spionaj și de terorism, ceea ce impune ca statul să fie capabil, pentru a combate eficient astfel de amenințări, să asigure supravegherea secretă a elementelor subversive care operează în jurisdicția sa. Prin urmare, Curtea trebuie să admită faptul că existența unei legislații care acordă competențe de supraveghere secretă a corespondenței, a trimiterilor poștale și a telecomunicațiilor este necesară într-o societate democratică, în condiții excepționale, în interesul securității naționale și/sau pentru apărarea ordinii și prevenirea infracțiunilor.”

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 emiterea 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 înregistrărilor [*Roman Zakharov împotriva Rusiei (MC), pct. 231 și 238-301; Amann împotriva Elveției (MC), pct. 56-58*].

**Examinarea și controlul măsurilor de supraveghere secretă** pot interveni în cadrul a **trei etape: în momentul dispunerii măsurii de supraveghere, în cursul punerii sale în aplicare sau ulterior încetării sale**. În ceea ce privește primele două etape, procedurile existente trebuie să prevadă ele însele garanții adecvate și echivalente care să protejeze drepturile persoanei. Având în vedere că abuzurile se pot produce cu ușurință, în principiu, este de dorit **să se încredințeze controlul măsurilor de supraveghere unei instanțe**, întrucât controlul judecătoresc oferă cele mai bune garanții de independență și imparțialitate, precum și o procedură adecvată. În ceea ce privește cea de-a treia etapă – respectiv încetarea supravegherii – **problema notificării a posteriori a măsurilor de supraveghere este strâns legată de cea a eficienței căilor de atac în fața instanțelor și, prin urmare, de existența unor garanții efective împotriva folosirii abuzive a competențelor de supraveghere**. În principiu, **persoana vizată nu poate sesiza instanțele judecătorești, decât în cazul în care aceasta este informată cu privire la măsurile adoptate fără cunoașterea sa și, astfel, poate să conteste retroactiv legalitatea lor sau, în altă ipoteză, suspectând că îi sunt sau i-au fost interceptate comunicările, persoana în cauză poate sesiza instanțele judecătorești, acestea având competență de examinare, chiar dacă persoana care a făcut obiectul interceptării nu a fost informată cu privire la măsura în cauză**.

**Sfera de aplicare a măsurilor de supraveghere secretă:** 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 [*Roman*

*Zakharov împotriva Rusiei (MC), pct. 243 și 247*]. 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 [*Iordachi și alții împotriva Republicii Moldova, pct. 44,*].

**Durata măsurilor de supraveghere:** problema duratei totale a măsurilor de interceptare poate fi lăsată la aprecierea autorităților responsabile pentru emiterea și reînnoirea mandatelor de interceptare, cu condiția să existe garanții adecvate, cum ar fi precizări clare în dreptul intern cu privire la data expirării mandatului de interceptare, condițiile în care poate fi reînnoit un mandat și circumstanțele în care acesta trebuie să fie anulat [*Roman Zakharov împotriva Rusiei (MC), pct. 250; Kennedy împotriva Regatului Unit, pct. 161*]. În cauza Iordachi și alții împotriva Republicii Moldova, legislația națională a fost criticată pentru că nu stabilea un termen suficient de clar în cazul autorizării unei măsuri de supraveghere (*pct. 45*).

**Procedurile de urmat pentru păstrarea, consultarea, examinarea, utilizarea, transmiterea și distrugerea datelor interceptate** [*Roman Zakharov împotriva Rusiei (MC), pct. 253-256*]. Păstrarea automată, timp de 6 luni, a unor date vădit lipsite de interes nu poate fi considerată justificată în temeiul art. 8. *Cauza Liberty și alții împotriva Regatului Unit* privea interceptarea de către Ministerul Apărării, pe baza unui mandat, a comunicărilor externe ale organizațiilor care activează în domeniul (protecției) libertăților civile. Curtea a constatat o încălcare, hotărând în special că publicul nu a avut la dispoziție nicio indicație privind procedura aplicabilă selectării în vederea examinării, partajării, păstrării și distrugerii materialelor interceptate (*pct. 69*).

**Procedurile de autorizare:** pentru a stabili dacă procedurile de autorizare sunt în măsură să garanteze că supravegherea secretă nu este dispusă la întâmplare, contrar legii sau fără o examinare corespunzătoare, Curtea va lua în considerare o serie de factori, incluzând, în special, **autoritatea competentă să autorizeze supravegherea**, domeniul de aplicare a examinării pe care o efectuează și conținutul autorizației de interceptare [*Roman Zakharov împotriva Rusiei (MC), pct. 257-267; a se vedea și Szabó și Vissy împotriva Ungariei, pct. 73 și 75-77, cu privire la măsurile de supraveghere supuse autorizării judiciare prealabile de către ministrul Justiției și chestiunea măsurilor de urgență, pct. 80-81*]. În cazul în care un sistem permite serviciilor secrete să intercepteze direct comunicațiile oricărui cetățean, fără a le impune obligația de a prezenta o autorizație de interceptare furnizorului de servicii de comunicații sau altcuiva, necesitatea unor garanții împotriva arbitrarului și abuzului pare deosebit de mare [*Roman Zakharov împotriva Rusiei (MC), pct. 270*].

**Controlul aplicării măsurilor de supraveghere secretă:** obligația impusă organelor de interceptare, de a păstra arhive despre interceptări, este deosebit de importantă pentru a garanta organului de control un acces efectiv la detaliile operațiunilor de supraveghere întreprinse [*Kennedy împotriva Regatului Unit, pct. 165; Roman Zakharov împotriva Rusiei (MC), pct. 275-285*]. Deși, în principiu, este de dorit să se încredințeze unui judecător sarcina de control a măsurilor de supraveghere, controlul efectuat de către un organism non-judiciar poate fi considerat compatibil cu Convenția, **cu condiția ca organul de control să fie independent de autoritățile care efectuează supravegherea și să fie investit cu suficiente competențe și atribuții pentru a exercita un control eficient și permanent** (*Klass și alții împotriva Germaniei, pct. 56*).

**Notificarea privind interceptarea comunicațiilor și căile de atac disponibile** [Roman Zakharov împotriva Rusiei (MC), pct. 286-301]. Caracterul secret al măsurilor de supraveghere ridică problema notificării persoanei în cauză, astfel încât aceasta din urmă să poată contesta legalitatea respectivelor măsuri. Deși lipsa unei notificări a posteriori adresate persoanelor afectate de măsuri de supraveghere secretă, imediat după ridicarea acestora, nu poate constitui, în sine, o încălcare, **este de dorit informarea persoanei vizate după ridicarea măsurilor, „de îndată ce notificarea poate fi emisă fără a pune în pericol scopul restricției”** [Roman Zakharov împotriva Rusiei (MC), pct. 287-290; Cevat Özel împotriva Turciei, pct. 34-37]. Problema necesității notificării unei persoane cu privire la faptul că este supusă unor măsuri de interceptare este indisolubil legată de cea a caracterului efectiv al căilor de atac [Roman Zakharov împotriva Rusiei (MC), pct. 286].

*În partea ce vizează respectarea prevederilor Convenției pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal (Convenția 108), ratificată prin Hotărârea Parlamentului Republicii Moldova nr. 483/1999:*

Se remarcă că urmare a ratificării Convenției pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal (Convenția 108), prin adoptarea Hotărârii Parlamentului nr. 483/1999, Republica Moldova s-a obligat să asigure corespunderea dreptului intern cu prevederile acesteia. Astfel, prin adoptarea Legii nr. 271/2013 au fost formulate declarații în privința modului de aplicare a Convenției 108, care stabilește excepțiile în care nu se vor aplica prevederile acesteia. Una dintre excepțiile declarate constituie circumstanța ***prelucrărilor de date cu caracter personal atribuite la secret de stat în modul stabilit, cu excepția celor efectuate în cadrul acțiunilor de prevenire și investigare a infracțiunilor, al punerii în executare a sentințelor de condamnare sau al altor acțiuni ce țin de procedura penală ori contravențională, în condițiile legii.***

Astfel, reieșind din prevederile enumerate la art. 1 pct. 1 lit. b) din Legea nr. 271/2013, la art. 2 alin. (2) lit. d) și la art. 2 alin. (4) lit. b) din Legea nr. 133/2011 privind protecția datelor cu caracter personal, prelucrărilor de date cu caracter personal efectuate în cadrul acțiunilor menționate supra se aplică **prevederile Convenției 108 și ale Legii nr. 133/2011, chiar dacă informațiile supuse prelucrării sunt atribuite la secret de stat.**

Suplimentar, evocăm că prin Decretul Președintelui Republicii Moldova nr. 757 din 22 decembrie 2022<sup>1</sup>, s-a aprobat semnarea Protocolului de amendare a Convenției pentru protecția persoanelor referitor la prelucrarea datelor cu caracter personal<sup>2</sup>, care face referire inclusiv la prelucrarea datelor în scopul asigurării securității naționale:

#### **Articolul 14**

Textul Articolului 9 al Convenției<sup>3</sup> (noul Articol 11) se înlocuiește cu următorul text:

1. Nu se permite nici o excepție de la dispozițiile prezentului capitol, cu excepția dispozițiilor Articolului 5 aliniatul 4<sup>4</sup>, Articolul 7 aliniatul 2<sup>5</sup>, Articolul 8 alineatului 1<sup>6</sup> și Articolul 9<sup>7</sup>, atunci

<sup>1</sup> [https://www.legis.md/cautare/getResults?doc\\_id=134721&lang=ro](https://www.legis.md/cautare/getResults?doc_id=134721&lang=ro)

<sup>2</sup> [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=090000168089ff4e](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e)

<sup>3</sup> [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=09000016807c65bf](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf)

<sup>4</sup> Care reglementează principiile de prelucrare a datelor cu caracter personal care trebuie transpuse în legislația internă;

<sup>5</sup> Norma care stabilește obligația notificării autorității de supraveghere competente privind prelucrarea datelor care afectează grav drepturile și libertățile fundamentale ale persoanelor vizate;

<sup>6</sup> Articolul dat stabilește obligația asigurării transparenței prelucrărilor de date prin obligarea operatorului de a informa persoanele vizate despre anumite aspect legate de prelucrările de date;

<sup>7</sup> Care stabilește drepturile subiectului de date.

când o astfel de excepție este prevăzută de lege, respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică pentru:

- a. protecția securității naționale, apărarea, siguranța publică, interesele economice și financiare importante ale statului, imparțialitatea și independența sistemului judiciar sau prevenirea, cercetarea și urmărirea penală a infracțiunilor și executarea sancțiunilor penale și alte obiective esențiale de interes public general;
- b. protecția persoanei vizate sau drepturile și libertățile fundamentale ale altora, în special libertatea de exprimare.

2. Restricțiile privind exercitarea dispozițiilor prevăzute la Articolele 8 (*transparența prelucrării*) și 9 (*drepturile subiectului de date*) pot fi prevăzute de lege în ceea ce privește prelucrarea datelor în scopul arhivării, în interes public, în scopuri științifice sau istorice de cercetare sau în scopuri statistice, atunci când nu există riscuri recunoscute de încălcare a drepturilor și libertăților fundamentale ale persoanelor vizate.

3. Pe lângă excepțiile prevăzute la alineatul 1 din prezentul articol, cu privire la activitățile de prelucrare în scopuri de securitate națională și de apărare, fiecare parte poate prevedea, prin lege și numai în măsura în care constituie o necesitate pentru îndeplinirea acestui scop, excepții de la Articolul 4 alineatul 3<sup>8</sup>, Articolul 14 alineatele 5 și 6<sup>9</sup> și Articolul 15 alineatul 2, literele a, b, c și d<sup>10</sup>.

**Acest aspect se realizează fără a aduce prejudicii cerinței ca activitățile de prelucrare în scopul securității naționale și al apărării să facă obiectul unei revizuri și supravegheri independente și efective în conformitate cu legislația internă a părții respective. "**

Respectiv, se reconfirmă inclusiv din prevederile Protocolului de amendare a Convenției că pot fi admise anumite norme derogatorii pentru prelucrările de date efectuate în legătură cu protecția securității naționale, însă acest lucru nu presupune faptul că acestea nu fac obiectul revizurii și supravegherii de către un organ independent care să asigure un control permanent și efectiv.

Astfel, în ordinea celor menționate supra, excluderea prelucrărilor de date cu caracter personal efectuate în cadrul activităților informative/contrainformative de la legislația privind protecția datelor cu caracter personal nu este corectă și nu corespunde Convenției pentru apărarea drepturilor omului și a libertăților fundamentale și Convenției pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal.

### *Concluzii generale*

Având în vedere cele evocate, prevederile tratatelor internaționale în domeniul drepturilor omului ratificate de Republica Moldova, dar și ținând cont de jurisprudența CtEDO în domeniu, raportate în special la prevederile proiectului de lege nr. 422 din 17 decembrie 2022 privind activitatea contrainformativă și activitatea informativă externă, au fost constatate următoarele concluzii generale:

1. Scopul proiectelor poate fi încadrat în excepțiile prevăzute de art. 54 alin. (2) din Constituția Republicii Moldova și din art. 8 alin. (2) al Convenției pentru apărarea drepturilor omului și a libertăților fundamentale;

<sup>8</sup> Stabilește obligațiile părților contractante a Convenției;

<sup>9</sup> Stabilește drepturile și atribuțiile autorităților de supraveghere competente în raport cu fluxurile transfrontaliere de date cu caracter personal.

<sup>10</sup> Stabilește competențele autorității de supraveghere.

2. Republica Moldova, în calitate de stat parte la Convenția pentru apărarea drepturilor omului și a libertăților fundamentale și la Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, dispune de o anumită marjă de apreciere pentru a stabili cea mai bună politică în domeniul asigurării securității statului;
3. Scopul proiectelor poate fi considerat că urmărește un scop legitim și adoptarea unor asemenea reglementări poate fi considerată ca fiind necesară într-o societate democratică, **doar în cazul în care sunt respectate anumite garanții minime de protecție a persoanelor vizate de măsurile de supraveghere secretă și în condițiile în care este posibilă contestarea acestora în fața unei autorități judiciare independente, recomandabil în instanța de judecată.**

Însă, potrivit redacției actuale a prevederilor proiectului nr. 422, s-a relevat că la elaborarea acestuia nu s-a ținut cont de prevederile tratatelor internaționale în domeniul drepturilor omului ratificate de Republica Moldova și nici de jurisprudența CtEDO în domeniu, la general<sup>11</sup> fiind constatate următoarele:

1. Prevederile proiectului admit nu doar restrângerea exercițiului dreptului la viața privată, la inviolabilitatea domiciliului și a secretului corespondenței - dar afectează însăși existența acestor drepturi (*lipsa garanțiilor minime de protecție, lipsa garanțiilor procedurale de contestare a măsurilor de supraveghere secretă, lipsa mecanismelor de control efectiv și permanent efectuat de către o autoritate judiciară independentă*);

2. Autorii, inclusiv în nota de informare aferentă proiectului, nu au adus argumente care să justifice rezonabil că, la stabilirea cadrului de reglementare în domeniul securității naționale, nu s-a depășit marja de apreciere a unui stat parte la Convențiile internaționale în domeniul drepturilor omului, ratificate de Republica Moldova;

3. Proiectul de lege nu respectă cerințele de claritate, previzibilitate și accesibilitate, în condițiile în care prevederile acestuia nu definește clar și exhaustiv natura infracțiunilor susceptibile să permită inițierea măsurilor de supraveghere și nici categoriile de persoane care pot deveni obiect al acestor măsuri;

4. Prevederile proiectului nu conțin garanții suficiente (cel puțin garanțiile minime de protecție) care să elimine abuzurile și să asigure respectarea drepturilor și libertăților fundamentale ale omului;

5. Nu este reglementată suficient problema notificării persoanelor vizate de măsurile de supraveghere secretă (*cel puțin a posteriori, atunci când scopul urmărit este atins*);

6. Prevederile proiectului nu asigură pentru persoanele vizate de măsurile de supraveghere o cale de contestare efectivă și nici posibilitatea de reparare a consecințelor acestora;

7. Autorii nu au adus argumente suficiente care să justifice proporționalitatea intenției de a mări termenul măsurilor de supraveghere până la 2 ani în raport cu consecințele ingerinței în viața privată a persoanelor supuse acestor măsuri;

8. Este deficientă reglementarea procedurilor de păstrare, consultare, examinare, utilizare, transmitere și distrugere a datelor interceptate;

9. Nu se regăsesc garanții care să excludă abuzurile și riscurile în legătură cu procedura de autorizare a măsurilor de supraveghere de către conducătorii autorității competente să efectueze aceste măsuri;

---

<sup>11</sup> Info detaliată se regăsește infra, separat pe marginea articolelor din proiectele de legi.

10. Proiectul de lege prevede mecanisme de control insuficiente și viciate, în condițiile în care pentru a fi excluse potențialele abuzuri este imperioasă stabilirea unor mecanisme de control efective și permanente, care poate fi realizat în special de către o autoritate judecătorească independentă.

În concluzie, se relevă că în cazul neadaptării proiectului de lege privind activitatea informativă și contrainformativă la cerințele și rigorile evocate mai sus, va fi adusă atingere existenței drepturilor fundamentale garantate de Constituție și vor apărea premisele condamnării Republicii Moldova în calitate de parte contractantă a tratatelor internaționale în domeniul drepturilor omului.

## II. Cu privire la prevederile proiectului de lege nr. 422 privind activitatea contrainformativă și informativă externă:

Conținutul articolelor proiectului de lege nr. 422 din 17 noiembrie 2022	Conținutul obiecției/propunerii/recomandării	Trimiteri la prevederile tratatelor internaționale contractate/la legislația conexă
<p><b>Articolul 1.</b> <b>Noțiuni, scop și domeniu de reglementare</b></p> <p>(1) Prezenta lege stabilește cadrul juridic al activității contrainformative și activității informative externe (<i>în continuare – activitatea informativă/contrainformativă</i>) realizate de către Serviciul de Informații și Securitate al Republicii Moldova (<i>în continuare – Serviciul</i>), modalitatea și condițiile de dispunere și efectuare a măsurilor contrainformative și măsurilor informative externe, precum și de efectuare a controlului asupra legalității acestora.</p> <p>(2) Activitatea contrainformativă constă din ansamblul măsurilor, acțiunilor, operațiunilor și procedeele 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.</p> <p>(3) Activitatea informativă externă constă din ansamblul măsurilor, acțiunilor și operațiunilor 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 sau ar putea constitui riscuri sau amenințări la adresa securității Republicii Moldova, 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.</p>	<p>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>Cerința de claritate</b> se aplică marjei de apreciere exercitate de autoritățile publice. Legislația internă trebuie să indice cu o claritate rezonabilă sfera și modul de exercitare a discreției relevante conferite autorităților publice, astfel încât să li se asigure persoanelor private gradul minim de protecție de care beneficiază în temeiul principiului statului de drept într-o societate democratică (<i>Piechowicz împotriva Poloniei, pct. 212</i>).</p> <p>Art. 8 § 2 din Convenție enumeră <b>scopurile legitime care pot justifica o ingerință</b> în exercitarea drepturilor protejate de art. 8: „<u>este necesară pentru securitatea națională</u>, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei, ori protejarea drepturilor și libertăților altora”. Curtea a stabilit că <b>este sarcina guvernului pârât să demonstreze că ingerința a avut un scop legitim</b> [<i>Mozer împotriva Republicii Moldova și Rusiei (MC), pct. 194</i>].</p> <p><b>Garanțiile procedurale de care dispune persoana particulară sunt deosebit de importante pentru a determina dacă statul pârât și-a depășit sau nu marja de apreciere atunci când a stabilit cadrul de reglementare.</b> Curtea trebuie să examineze, în special, dacă procesul decizional finalizat prin măsuri care constituie o ingerință a fost echitabil și a permis respectarea adecvată a intereselor garantate unei persoane de către art. 8 (<i>A.-M.V. împotriva Finlandei, pct. 82-84</i>).</p>

<p><b>Articolul 2.</b> <b>Principiile activității informative/contrainformative</b></p> <p>Activitatea informativă/contrainformativă se bazează pe principiile:</p> <ol style="list-style-type: none"> <li>legalității;</li> <li>egalității tuturor în fața legii;</li> <li>respectării drepturilor și libertăților omului și reglementarea exclusiv prin lege a restrângerii exercițiului acestora;</li> <li>oportunității;</li> <li>proporționalității;</li> <li>caracterului activ al măsurilor realizate;</li> <li>confidențialității, îmbinării metodelor și mijloacelor de activitate publică și secretă;</li> <li>neutralității politice și imparțialității.</li> </ol>	<p>Se propune, la enumerarea principiilor, de completat suplimentar cu o nouă literă:</p> <p><i>i) contestării efective în fața unei autorități judiciare independente a legalității acțiunilor/inacțiunilor subiecților care efectuează activitatea informativă/contrainformativă;</i></p>	
<p><b>Articolul 3.</b> <b>Asigurarea legalității activității informative/contrainformative</b></p> <ol style="list-style-type: none"> <li>Legalitatea activității informative/contrainformative se asigură prin realizarea controlului asupra acestei activități în conformitate cu prevederile prezentei legi.</li> <li>Desfășurarea activității informative/contrainformative în alte scopuri decât cele menționate de prezenta lege nu se admite.</li> <li>Desfășurarea activității informative/contrainformative cu încălcarea prezentei legi atrage după sine răspunderea prevăzută de legislație.</li> </ol>	<p>Se propune completarea art. 3 cu două alineate noi:</p> <ol style="list-style-type: none"> <li><i>Rezultatele activității informative/contrainformative, inclusiv 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></li> <li><i>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></li> </ol>	<p>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 (Szabó și Vissy împotriva Ungariei).</p>
	<p>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:</p> <p><b>Obligații:</b></p> <ol style="list-style-type: none"> <li>să respecte drepturile și interesele legitime ale persoanei;</li> <li>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;</li> <li>să respecte confidențialitatea datelor cu caracter personal ce au devenit cunoscute în timpul efectuării măsurii speciale de investigații;</li> <li>să respecte proporționalitatea dintre dreptul lezat și necesitatea măsurii ce se efectuează;</li> <li>să asigure documentarea și arhivarea fără excepții a materialelor privind desfășurarea activității informative și contrainformative</li> </ol> <p><b>Restricții:</b></p> <ol style="list-style-type: none"> <li>Subiecților care efectuează activitatea informativă/contrainformativă li se interzice: <ol style="list-style-type: none"> <li>să provoace comiterea de infracțiuni;</li> <li>să antreneze în activitatea informativă/contrainformativă, în calitate de persoane care colaborează confidențial cu Serviciul, deputați, judecători, procurori, ofițeri de urmărire penală și avocați.</li> </ol> </li> </ol>	<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 [Weber și Saravia împotriva Germaniei (dec.), pct. 78]. 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 nu beneficiază de o putere discreționară nelimitată de a supune persoanele aflate în jurisdicția lor unor măsuri de supraveghere secretă. Curtea a afirmat că statele contractante nu pot adopta, în numele luptei împotriva spionajului și a terorismului, orice măsură pe care o consideră adecvată, ci, mai degrabă, indiferent de sistemul de supraveghere adoptat, <b>acestea trebuie să asigure garanții adecvate și eficiente împotriva abuzurilor</b> (ibidem, pct. 106). „Calitatea legii” implică faptul că dreptul intern trebuie să fie nu doar accesibil și previzibil în ceea ce privește aplicarea sa, dar trebuie, în plus, să garanteze că măsurile de supraveghere secretă sunt aplicate numai atunci când sunt „necesare într-o societate democratică”, în special prin furnizarea unor garanții suficiente și efective împotriva abuzurilor [Roman Zakharov împotriva Rusiei (MC), pct. 236].</p>

<p><b>Articolul 7.</b> <b>Asistența acordată la efectuarea activității informative/contrainformative</b></p> <p>(1) Persoanele fizice și juridice, indiferent de forma de proprietate, sînt obligate, în condițiile prezentei legi, să acorde asistența necesară Serviciului, să pună imediat, gratis la dispoziția acestuia informațiile solicitate, precum și, în măsura posibilității, bunuri mobile și imobile, alte obiecte și documente necesare pentru realizarea activității informative/contrainformative.</p> <p>.....</p>	<p>Sintagma „<i>în condițiile prezentei legi</i>” 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: (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>Controlul aplicării măsurilor de supraveghere secretă: obligația impusă organelor de interceptare, de a păstra arhive despre interceptări, este deosebit de importantă pentru a garanta organului de control un acces efectiv la detaliile operațiunilor de supraveghere întreprinse [Kennedy împotriva Regatului Unit, pct. 165; Roman Zakharov împotriva Rusiei (MC), pct. 275-285].</p> <p>O lege privind măsuri de supraveghere secretă trebuie 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 înregistrărilor [Roman Zakharov împotriva Rusiei (MC), pct. 231 și 238-301; Amann împotriva Elveției (MC), pct. 56-58].</p>
<p><b>Articolul 8.</b> <b>Utilizarea mijloacelor tehnice la efectuarea activității informative/contrainformative</b></p> <p>În procesul efectuării activității informative/contrainformative se permite utilizarea sistemelor informaționale, mijloacelor tehnice speciale destinate pentru obținerea ascunsă a informației, aparatelor de înregistrare video, audio sau a altor mijloace tehnice.</p>	<p>Se propune completarea articolului cu un nou alineat cu următorul conținut: <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>În vederea excluderii circumstanțelor care să permită abuzuri potențiale se impune necesitatea interzicerii utilizării mijloacelor și dispozitivelor care nu aparțin Serviciului sau a celor neînregistrate în modul stabilit.</p>
<p><b>Articolul 9.</b> <b>Dosarul special</b></p> <p>(1) În scopul colectării și sistematizării informațiilor, verificării și aprecierii rezultatelor activității informative/contrainformative, precum și adoptării, în baza lor, a deciziilor corespunzătoare, se inițiază dosare speciale în care se anexează toate materialele acumulate. Inițierea dosarului este supusă înregistrării obligatorii.</p> <p>(2) Fiecare dosar special va include un mecanism de evidență a persoanelor care au făcut cunoștință cu materialele dosarului, care va include:</p> <ol style="list-style-type: none"> <li>numele, prenumele și funcția persoanei;</li> <li>data, anul și ora inițierii luării de cunoștință cu materialele dosarului și data, anul și ora finalizării acesteia;</li> <li>mențiuni vizând accesul la dosarul special integral, anumite documente sau compartimente ale acestuia,</li> <li>semnătura persoanei.</li> </ol> <p>(3) Serviciul asigură măsurile necesare pentru a proteja informațiile păstrate în dosarele speciale de dezvăluire, modificare sau distrugere. În cazurile în care informațiile păstrate în dosarele speciale ale Serviciului nu mai sunt necesare îndeplinirii sarcinilor sale sau în cazurile în care există oricare alt temei legal, Serviciul le va distruge sau le va păstra într-o manieră care să permită accesul doar în cazuri exclusiv reglementate prin lege.</p> <p>(4) Inițierea dosarului special nu poate servi drept temei pentru limitarea drepturilor și libertăților omului prevăzute de lege.</p>	<p>Se propune completarea articolului cu noi alineate cu următorul conținut: <i>Activitatea informativă/contrainformativă efectuată în afara urmăririi 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 urmăririi penale și în afara unui dosar special este nulă de drept și atrage răspunderea disciplinară, contravențională și/sau penală prevăzută de legislație.</i></p> <p><i>Conducătorul subdiviziunii specializate este responsabil de legalitatea inițierii dosarului special și a acțiunilor efectuate în cadrul acestuia.</i></p> <p><i>Oșterul de informație nu poate iniția un dosar special fără coordonarea conducătorului subdiviziunii specializate.</i></p>	<p>Obligația impusă organelor de interceptare, de a păstra arhive, este deosebit de importantă pentru a garanta organului de control (instanței judiciare) un acces efectiv la detaliile operațiunilor de supraveghere întreprinse [Kennedy împotriva Regatului Unit, pct. 165; Roman Zakharov împotriva Rusiei (MC), pct. 275-285].</p> <p>Controlul aplicării măsurilor de supraveghere secretă: obligația impusă organelor de interceptare, de a păstra arhive despre interceptări, este deosebit de importantă pentru a garanta organului de control un acces efectiv la detaliile operațiunilor de supraveghere întreprinse [Kennedy împotriva Regatului Unit, pct. 165; Roman Zakharov împotriva Rusiei (MC), pct. 275-285].</p> <p>O lege privind măsuri de supraveghere secretă trebuie să ofere următoarele garanții minime de protecție împotriva abuzurilor de putere: să definească natura infrațiunilor susceptibile să genereze emiterea 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 înregistrărilor [Roman Zakharov împotriva Rusiei (MC), pct. 231 și 238-301; Amann împotriva Elveției (MC), pct. 56-58].</p>

<p><b>Articolul 10.</b> <b>Gestionarea materialelor irelevante pentru activitatea informativă/contrainformativă</b></p> <p>După finalizarea cercetării cauzei, în cadrul activității informative/contrainformative, și clasarea dosarului special, materialele care s-au dovedit a fi irelevante pentru cauza cercetată sunt distruse, cu excepția documentelor ce confirmă autorizarea și realizarea unei măsuri contrainformative sau alte excepții prevăzute de lege, cu întocmirea unui act în acest sens. Restul materialelor se arhivează și urmează regimul de păstrare a dosarului special, cu ulterioara distrugere sau, după caz, desecretizare și transmitere spre păstrare în Arhiva Națională a Republicii Moldova, conform prevederilor legale..</p>	<p>Se propune completarea articolului cu două alineate cu următorul conținut: <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> <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>Problema necesității notificării unei persoane cu privire la faptul că este supusă unor măsuri de interceptare este indisolubil legată de cea a caracterului efectiv al căilor de atac [Roman Zakharov împotriva Rusiei (MC), pct. 286].</p> <p>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 emiterea 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 înregistrărilor [Roman Zakharov împotriva Rusiei (MC), pct. 231 și 238-301; Amann împotriva Elveției (MC), pct. 56-58].</p>
<p><b>Articolul 11.</b> <b>Reglementarea departamentală a activității informative/contrainformative</b></p> <p>Organizarea, metodele efectuării măsurilor contrainformative sau informative externe, procedurile interne de autorizare, regulile de întocmire a proceselor-verbale cu privire la gestionarea, păstrarea și distrugerea materialelor obținute, măsurile de asigurare a integrității și confidențialității acestora și a activităților informative/contrainformative, regulile de înfăptuire a operațiunilor sub acoperire și cu privire la conducerea și gestionarea activității efectuate sub acoperire, 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 acesteia constituie informații atribuite la secretul de stat și sînt reglementate prin acte normative departamentale ale Serviciului.</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><b>Legislația națională trebuie să fie clară, previzibilă și suficient de accesibilă</b> (<i>Silver și alții împotriva Regatului Unit, pct. 87</i>). Acest lucru include un caracter suficient de previzibil pentru a permite persoanelor particulare să acționeze în conformitate cu legea, precum și o delimitare clară a marjei de apreciere a autorităților publice. De exemplu, în contextul măsurilor de supraveghere, Curtea a precizat că legea trebuie să fie redactată în termeni suficient de clari pentru a le furniza cetățenilor indicii adecvate privind circumstanțele și condițiile în care autoritățile au dreptul să recurgă la orice măsuri de supraveghere secretă și de colectare de date (<i>Shimovolos împotriva Rusiei, pct. 68</i>).</p> <p><b>Cerința de claritate se aplică marjei de apreciere exercitate de autoritățile publice.</b> Legislația internă trebuie să indice cu o claritate rezonabilă sfera și modul de exercitare a discreției relevante conferite autorităților publice, astfel încât să li se asigure persoanelor private gradul minim de protecție de care beneficiază în temeiul principiului statului de drept într-o societate democratică (<i>Piechowicz împotriva Poloniei, pct. 212</i>).</p>
<p><b>Articolul 12.</b> <b>Măsurile contrainformative</b></p> <p>(1) În cadrul activității contrainformative pot fi efectuate următoarele măsuri contrainformative:</p> <p>1) cu autorizarea directorului Serviciului sau directorului adjunct special împuternicit:</p> <p>a) accesul la informația financiară sau monitorizarea tranzacțiilor financiare;</p> <p>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;</p> <p>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;</p>	<p>Având în vedere riscurile înalte de abuzuri care reies din acordarea posibilității de a autoriza măsurile contrainformative 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>Procedurile de autorizare: pentru a stabili dacă procedurile de autorizare sunt în măsură să garanteze că supravegherea secretă nu este dispusă la întâmplare, contrar legii sau fără o examinare corespunzătoare, Curtea va lua în considerare o serie de factori, incluzând, în special, autoritatea competentă să autorizeze supravegherea, domeniul de aplicare a examinării pe care o efectuează și conținutul autorizației de interceptare [Roman Zakharov împotriva Rusiei (MC), pct. 257-267; a se vedea și Szabó și Vissy împotriva Ungariei, pct. 73 și 75-77, cu privire la măsurile de supraveghere supuse autorizării judiciare prealabile de către ministrul Justiției și chestiunea măsurilor de urgență, pct. 80-81]. În cazul în care un sistem permite serviciilor secrete și poliției să</p>

<p>d) controlul transmiterii banilor sau altor valori materiale sau nemateriale, precum și prestării serviciilor;</p> <p>e) investigația sub acoperire;</p> <p>f) livrarea supraveghetă;</p> <p>g) colectarea mostrelor pentru cercetarea comparativă;</p> <p>h) cercetarea obiectelor și actelor;</p> <p>i) achiziția de control;</p> <p>j) cercetarea încăperilor, clădirilor, porțiunilor de teren sau a mijloacelor de transport, în cazul în care aceasta nu constituie o violare a domiciliului;</p> <p>k) experimentul operativ;</p> <p>2) cu mandat judecătoresc:</p> <p>a) 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;</p> <p>b) supravegherea domiciliului prin utilizarea mijloacelor tehnice cu sau fără efectuarea înregistrărilor;</p> <p>c) interceptarea comunicărilor cu sau fără înregistrarea acestora;</p> <p>d) accesul la informația ce se află sau se prelucrează într-un sistem informațional și/sau monitorizarea acesteia cu sau fără efectuarea înregistrărilor;</p> <p>e) colectarea informației de la furnizorii de servicii de comunicații electronice;</p> <p>f) reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimiterilor poștale;</p> <p>g) urmărirea vizuală cu înregistrarea audio a conținutului comunicărilor transmise de către persoane în spații deschise, locuri publice sau încăperi ce nu constituie domiciliu;</p> <p>h) blocarea unui punct de acces conectat la un sistem informatic sau la rețele de comunicații electronice;</p> <p>i) sustragerea operativă.</p> <p>(2) Lista măsurilor enumerate la alin. (1) al prezentului articol este exhaustivă și poate fi modificată sau completată numai prin lege.</p>		<p>intercepteze direct comunicațiile oricărui cetățean, fără a le impune obligația de a prezenta o autorizație de interceptare furnizorului de servicii de comunicații sau altcuiva, necesitatea unor garanții împotriva arbitrarului și abuzului pare deosebit de mare [Roman Zakharov împotriva Rusiei (MC), pct. 270].</p> <p>Competențele de supraveghere secretă a cetățenilor, caracteristice statului polițienesc, sunt tolerabile în temeiul Convenției numai în măsura strict necesară pentru protejarea instituțiilor democratice (ibidem, pct. 42; Szabó și Vissy împotriva Ungariei, pct. 72-73). În această ultimă cauză, Curtea a clarificat noțiunea de „strictă necesitate”. Astfel, o măsură de supraveghere secretă trebuie, în general, să fie strict necesară pentru apărarea instituțiilor democratice și, în special, pentru obținerea de informații vitale în cadrul unei anumite operațiuni. În caz contrar, ar exista un „abuz” din partea autorităților (pct. 73).</p>
<p><b>Articolul 13.</b> <b>Temeiurile pentru efectuarea măsurilor contrainformative</b></p> <p>(1) Temeiurile pentru efectuarea măsurilor contrainformative sunt:</p> <p>1) informațiile devenite cunoscute, privind:</p> <p>a) fapta în curs de pregătire, de comitere sau comisă, care periclitează securitatea statului, precum și privind persoanele care o pregătesc, o comit sau au comis-o, complicității acestora;</p> <p>b) circumstanțele ce pun în pericol securitatea investigatorului sub acoperire, a ofițerului de informații, a persoanelor care colaborează confidențial cu Serviciul sau a membrilor familiei lor;</p> <p>c) potențialele riscuri și amenințări la adresa securității statului;</p> <p>2) cercetarea sau contracararea activității serviciilor speciale ale statelor străine sau ale entităților neconstituționale;</p> <p>3) interpelările organizațiilor internaționale sau ale autorităților de drept ale altor state, în conformitate cu tratatele internaționale la care Republica Moldova este parte sau în baza acordurilor de colaborare între Serviciu și autoritățile publice de profil din alte state;</p> <p>4) interpelările autorităților care organizează și efectuează activitatea specială de investigații, urmărirea penală, judecarea</p>	<p>Pentru asigurarea clarității și previzibilității legii, se necesită excluderea temeiurilor legale precum:</p> <p>- informațiile devenite cunoscute.</p> <p>Se propune de reformulat cu <i>informațiile veridice care pot fi probate</i>;</p> <p>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>Primul aspect se referă la faptul că măsura de supraveghere trebuie să aibă un temei legal în dreptul intern și să fie compatibilă cu statul de drept. Prin urmare, legea trebuie să îndeplinească anumite cerințe de calitate: aceasta trebuie să fie accesibilă persoanei în cauză și să fie previzibilă în ceea ce privește efectele sale (Kennedy împotriva Regatului Unit, pct. 151). În materie de interceptare a comunicărilor, „caracterul previzibil” nu poate fi înțeles în același mod ca în multe alte domenii. În contextul special al măsurilor secrete de supraveghere, caracterul previzibil nu poate însemna că o persoană ar trebui să fie în măsură să prevadă situațiile în care este posibil ca autoritățile să le intercepteze comunicările, astfel încât aceasta să își poată adapta comportamentul în consecință (Weber și Saravia împotriva Germaniei, pct. 93). Cu toate acestea, pentru a evita ingerințele arbitrare, este esențial să existe norme clare și detaliate privind interceptarea convorbirilor telefonice. Legea trebuie să fie suficient de clară încât să le ofere cetățenilor indicii privind circumstanțele și condițiile în care autoritățile publice sunt abilitate să recurgă la astfel de măsuri</p>

<p>cauzelor, în cazul faptelor care periclitează securitatea statului;</p> <p>5) necesitatea de a obține date informative în interesul asigurării securității Republicii Moldova, sporirii potențialului ei economic, tehnico-științific sau defensiv, creării condițiilor pentru promovarea politicii ei externe și interne;</p> <p>6) protecția secretului de stat;</p> <p>7) colectarea informațiilor necesare ce caracterizează persoanele supuse verificării, privind:</p> <p>a) accesul la informații ce constituie secret de stat;</p> <p>b) admiterea la muncă la obiectivele infrastructurii critice;</p> <p>c) admiterea la organizarea și desfășurarea unor măsuri contrainformative și/sau informative externe sau accesul la materialele primite pe parcursul efectuării acestor măsuri;</p> <p>d) stabilirea sau întreținerea relațiilor de colaborare la organizarea și desfășurarea măsurilor contrainformative sau informative externe;</p> <p>8) verificarea candidaților sau titularilor la funcții publice;</p> <p>9) asigurarea securității interne.</p>		<p>secrete [Roman Zakharov împotriva Rusiei (MC), pct. 229; Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiev împotriva Bulgariei, pct. 75]. În plus, legea trebuie să precizeze suficient de clar domeniul de aplicare și modalitățile de exercitare ale marjei de apreciere acordate executivului sau unei instanțe, astfel încât să ofere individului o protecție adecvată împotriva ingerințelor arbitrare [Roman Zakharov împotriva Rusiei (MC), pct. 230; Malone împotriva Regatului Unit, pct. 68; Huvig împotriva Franței, pct. 29; Weber și Saravia împotriva Germaniei (dec.), pct. 94].</p> <p>Astfel, există o ingerință în dreptul la respectarea vieții private, astfel cum este protejat de art. 8 § 1 din Convenție, în cazul în care dreptul intern nu menționează suficient de clar domeniul de aplicare și modul de exercitare a puterii discreționare conferite autorităților naționale pentru a colecta și a stoca, într-o bază de date privind persoanele supravegheate, informații referitoare la viața privată a persoanelor fizice, în special atunci când nu furnizează, într-o formă accesibilă publicului, niciun indiciu privind existența unor garanții minime împotriva abuzurilor (Shimovolov împotriva Rusiei, pct. 66, în care numele reclamantului a fost înregistrat în „baza de date privind persoanele supravegheate”, în care au fost colectate informații privind deplasările sale în Rusia, cu trenul sau cu avionul). Legislația internă ar trebui să ofere garanții suficient de precise, eficiente și cuprinzătoare cu privire la disponerea și executarea măsurilor de supraveghere, precum și la posibilitățile de reparare a consecințelor acestora (Szabó și Vissy împotriva Ungariei).</p>
<p><b>Articolul 14.</b>  <b>Procedura autorizării măsurilor contrainformative de către directorul Serviciului sau directorului adjunct special împuternicit</b></p> <p>(1) Măsurile contrainformative prevăzute la art. 12 alin. (1) pct. 1) din prezenta lege se autorizează, prin ordonanță, de către directorul Serviciului sau directorul adjunct special împuternicit, la demersul șefului subunității care efectuează activitatea informativă/contrainformativă în cadrul unui dosar special deschis și înregistrat.</p> <p>(2) Demersul va cuprinde: circumstanțele faptice care servesc ca temelie pentru efectuarea măsurilor contrainformative; după caz, posibilele consecințe ale acestora; argumentarea efectuării anume a acestor măsuri; numărul dosarului special în cadrul căruia urmează a fi efectuate măsurile; rezultatele care se preconizează să fie obținute în urma efectuării acestor măsuri; termenul de efectuare a măsurilor respective; dacă se solicită prelungirea măsurii se indică datele despre autorizările precedente și termenul cumulativ de îndeplinire a măsurii; locul efectuării; datele de identificare a persoanei supuse măsurii, dacă sunt cunoscute; alte date ce au importanță.</p> <p>(3) Ordonanța directorului Serviciului sau directorului adjunct special împuternicit va cuprinde:</p> <p>a) data întocmirii;</p> <p>b) datele dosarului special în cadrul căruia se autorizează măsura;</p> <p>c) măsura concret autorizată;</p>	<p>Având în vedere riscurile înalte de abuzuri care reies din acordarea posibilității a autoriza măsurilor 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).</p> <p>Suplimentar, se propune reformularea alin. (4) pentru ca și în cazul autorizării măsurilor contrainformative de către conducerea Serviciului să fie stabilită obligația verificării în prealabil dacă:</p> <p>a) <i>acțiunea solicitată urmărește un scop legitim;</i></p> <p>c) <i>acțiunea va fi proporțională cu dreptul sau libertatea persoanei garantată de lege și necesitatea apărută.</i></p>	<p>Procedurile de autorizare: pentru a stabili dacă procedurile de autorizare sunt în măsură să garanteze că supravegherea secretă nu este dispusă la întâmplare, contrar legii sau fără o examinare corespunzătoare, Curtea va lua în considerare o serie de factori, incluzând, în special, autoritatea competentă să autorizeze supravegherea, domeniul de aplicare a examinării pe care o efectuează și conținutul autorizației de interceptare [Roman Zakharov împotriva Rusiei (MC), pct. 257-267; a se vedea și Szabó și Vissy împotriva Ungariei, pct. 73 și 75-77, cu privire la măsurile de supraveghere supuse autorizării judiciare prealabile de către ministrul Justiției și chestiunea măsurilor de urgență, pct. 80-81]. În cazul în care un sistem permite serviciilor secrete și poliției să intercepteze direct comunicațiile oricărui cetățean, fără a le impune obligația de a prezenta o autorizație de interceptare furnizorului de servicii de comunicații sau altcuiva, necesitatea unor garanții împotriva arbitrarului și abuzului pare deosebit de mare [Roman Zakharov împotriva Rusiei (MC), pct. 270].</p> <p>Astfel, există o ingerință în dreptul la respectarea vieții private, astfel cum este protejat de art. 8 § 1 din Convenție, în cazul în care dreptul intern nu menționează suficient de clar domeniul de aplicare și modul de exercitare a puterii discreționare conferite</p>

<p>d) perioada pentru care a fost autorizată, dacă este cazul;</p> <p>e) subunitatea Serviciului sau, după caz ofițerii de informații, care o vor desfășura, în cazul în care măsura nu este realizată nemijlocit de către ofițerul de informații care a înaintat demersul;</p> <p>f) alte informații, în cazul în care există prevederi în acest sens în prezenta Lege.</p> <p>(4) Directorul Serviciului, directorul adjunct special împuternicit, vor refuza autorizarea măsurii contrainformative dacă constată că demersul înaintat este neîntemeiat și neargumentat.</p>		<p>autorităților naționale pentru a colecta și a stoca, într-o bază de date privind persoanele supravegheate, informații referitoare la viața privată a persoanelor fizice, în special atunci când nu furnizează, într-o formă accesibilă publicului, niciun indiciu privind existența unor garanții minime împotriva abuzurilor (Shimovolov împotriva Rusiei, pct. 66, în care numele reclamantului a fost înregistrat în „baza de date privind persoanele supravegheate”, în care au fost colectate informații privind deplasările sale în Rusia, cu trenul sau cu avionul). Legislația internă ar trebui să ofere garanții suficient de precise, eficiente și cuprinzătoare cu privire la disponerea și executarea măsurilor de supraveghere, precum și la posibilitățile de reparare a consecințelor acestora (Szabó și Vissy împotriva Ungariei).</p>
<p><b>Articolul 20.</b> <b>Consemnarea măsurilor contrainformative</b></p> <p>(1) Ofițerul de informații care efectuează măsura contrainformativă întocmește un proces-verbal pentru fiecare măsură autorizată, în care consemnează:</p> <p>a) denumirea măsurii contrainformative efectuate, locul și data efectuării acesteia, după caz ora începerii și finalizării acesteia, date despre autorizarea măsurii sau mandatul judecătoresc;</p> <p>b) funcția, numele și prenumele ofițerului de informații care întocmește procesul-verbal. Dacă măsura contrainformativă a fost efectuată 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 date, care verifică corectitudinea celor menționate în procesul-verbal și-l semnează. În cadrul subunităților menționate se ține evidența strictă a ofițerilor de informații care au realizat măsuri contrainformative și au întocmit procese-verbale;</p> <p>c) numele, prenumele și statutul persoanelor care au participat la efectuarea măsurilor, iar dacă este necesar, adresele lor, obiectele și explicațiile acestora. Datele respective nu se consemnează în procesul-verbal în cazul participării la efectuarea măsurilor a ofițerilor de informații din cadrul subunităților de asigurare a activității informative/contrainformative, care fac parte din personalul criptic al Serviciului;</p> <p>d) descrierea faptelor constatate, precum și a acțiunilor întreprinse în cadrul efectuării măsurii contrainformative;</p> <p>e) mențiunea privind utilizarea mijloacelor tehnice, condițiile și modalitățile de aplicare a acestora, obiectele față de care au fost aplicate aceste mijloace, rezultatele obținute, înregistrarea informațiilor acumulate.</p> <p>(2) În cazul înregistrării rezultatelor măsurii contrainformative, la procesul-verbal se anexează purtătorul material de informații.</p> <p>(3) Procesul-verbal și purtătorul material de informații se anexează la dosarul special.</p>	<p>Se propune completarea articolului cu două alineate noi cu următorul conținut:</p> <p>(4) <i>Rezultatele activității informative/contrainformative efectuate cu încălcarea legislației nu pot fi sususe ștergerii/distrugerii fără notificarea persoanei lezate în drepturi.</i></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 contrainformative de către persoanele și entitățile de drept public sau privat enumerate la art. 7 alin. (1) al legii.</i></p>	<p>O lege privind măsuri de supraveghere secretă trebuie 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 înregistrărilor [Roman Zakharov împotriva Rusiei (MC), pct. 231 și 238-301; Amann împotriva Elveției (MC), pct. 56-58].</p> <p>Procedurile de urmat pentru păstrarea, consultarea, examinarea, utilizarea, transmiterea și distrugerea datelor interceptate [Roman Zakharov împotriva Rusiei (MC), pct. 253-256]. Păstrarea automată, timp de 6 luni, a unor date vădit lipsite de interes nu poate fi considerată justificată în temeiul art. 8 (ibidem, pct. 255). Cauza Liberty și alții împotriva Regatului Unit privea interceptarea de către Ministerul Apărării, pe baza unui mandat, a comunicărilor externe ale organizațiilor care activează în domeniul (protecției) libertăților civile. Curtea a constatat o încălcare, hotărând în special că publicul nu a avut la dispoziție nicio indicație privind procedura aplicabilă selectării în vederea examinării, partajării, păstrării și distrugerii materialelor interceptate (pct. 69).</p>

<p><b>Articolul 21.</b> <b>Utilizarea rezultatelor măsurilor contrainformative</b></p> <p>(1) Rezultatele măsurilor contrainformative se utilizează:</p> <ol style="list-style-type: none"> <li>la realizarea atribuțiilor Serviciului;</li> <li>la efectuarea altor măsuri contrainformative;</li> <li>la efectuarea măsurilor speciale de investigații, în scopul depistării, prevenirii, urmării criminalității și asigurării ordinii publice.</li> </ol> <p>(2) Informația despre forțele, mijloacele, sursele, metodele, planurile și rezultatele activității informative/contrainformative, precum și despre organizarea și tactica desfășurării măsurilor contrainformative, constituie secret de stat și poate fi deosebită numai în conformitate cu legislația.</p> <p>(3) În cazul în care, în urma efectuării măsurilor contrainformative, se constată o bănuială rezonabilă cu privire la săvârșirea unei infracțiuni sau pregătirea săvârșirii ei, printr-un raport se informează procurorul special împuternicit din cadrul Procuraturii Generale.</p> <p>(4) Rezultatele măsurilor contrainformative din cadrul unui dosar special pot fi utilizate în cadrul altui dosar special doar cu autorizarea judecătorului sau, după caz, a directorului Serviciului/directorului adjunct special împuternicit, care a eliberat mandat judecătoresc, sau, după caz, ordonanța, pentru efectuarea măsurilor contrainformative respective.</p> <p>(5) Rezultatele măsurilor contrainformative nu pot constitui probe în cadrul unei cauze penale.</p>	<p>Se propune completarea articolului cu un alineat nou cu următorul conținut:</p> <p>(6) <i>Rezultatele măsurilor contrainformative obținute cu încălcarea legii și alte informații cu privire la fapte de încălcare a drepturilor și libertăților fundamentale ale omului se deosebită în modul stabilit de legislația cu privire la secretul de stat, cu notificarea obligatorie a persoanelor vizate de acestea.</i></p>	<p>O lege ce instituie măsuri de supraveghere secretă trebuie să ofere următoarele garanții minime de protecție împotriva abuzurilor de putere: să definească natura infracțiunilor susceptibile să genereze emiterea 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 înregistrărilor [Roman Zakharov împotriva Rusiei (MC), pct. 231 și 238-301; Amann împotriva Elveției (MC), pct. 56-58].</p> <p>Procedurile de urmat pentru păstrarea, consultarea, examinarea, utilizarea, transmiterea și distrugerea datelor interceptate [Roman Zakharov împotriva Rusiei (MC), pct. 253-256]. Păstrarea automată, timp de 6 luni, a unor date vădit lipsite de interes nu poate fi considerată justificată în temeiul art. 8 (ibidem, pct. 255). Cauza Liberty și alții împotriva Regatului Unit privea interceptarea de către Ministerul Apărării, pe baza unui mandat, a comunicărilor externe ale organizațiilor care activează în domeniul (protecției) libertăților civile. Curtea a constatat o încălcare, hotărând în special că publicul nu a avut la dispoziție nicio indicație privind procedura aplicabilă selectării în vederea examinării, partajării, păstrării și distrugerii materialelor interceptate (pct. 69).</p>
<p><b>Articolul 23.</b> <b>Informarea persoanei despre măsurile contrainformative înfăptuite în privința sa</b></p> <p>(1) 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) Serviciul, în termen de 5 zile lucrătoare de la data clasării, va informa persoanele în privința cărora aceste măsuri au fost înfăptuite. Materialele ce confirmă informarea persoanei se anexează la dosarul special.</p> <p>(2) În fiecare caz de informare a persoanelor în privința cărora au fost înfăptuite măsuri contrainformative prevăzute la art. 12 alin. (1) pct. 2), Serviciul va anunța despre aceasta judecătorul care a eliberat mandat judecătoresc.</p> <p>(3) Informarea persoanei nu se va face 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.</p> <p>(4) Despre existența temeiurilor menționate la alin. (3), ofițerul de informații, care a efectuat cercetarea cauzei, întocmește un raport în scris în care detaliază aceste temeiuri și îl prezintă pentru aprobare directorului Serviciului. Dacă raportul este aprobat, directorul Serviciului solicită judecătorului care a eliberat mandat judecătoresc autorizarea neinformării persoanei.</p> <p>(5) Judecătorul, la examinarea demersului directorului Serviciului, constată</p>	<p>În vederea asigurării unei notificări veridice funcționale, se propune completarea articolului cu un alineat nou:</p> <p>(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></p> <p>(9) <i>Neinformarea persoanei contrar prevederilor prezentului articol atrage răspunderea disciplinară, contravențională și/sau penală prevăzută de legislație.</i></p>	<p>Notificarea privind interceptarea comunicațiilor și căile de atac disponibile [Roman Zakharov împotriva Rusiei (MC), pct. 286-301]. Caracterul secret al măsurilor de supraveghere ridică problema notificării persoanei în cauză, astfel încât aceasta din urmă să poată contesta legalitatea respectivelor măsuri. Deși lipsa unei notificări a posteriori adresate persoanelor afectate de măsuri de supraveghere secretă, imediat după ridicarea acestora, nu poate constitui, în sine, o încălcare, este de dorit informarea persoanei vizate după ridicarea măsurilor, „de îndată ce notificarea poate fi emisă fără a pune în pericol scopul restricției” [Roman Zakharov împotriva Rusiei (MC), pct. 287-290; Cevat Özel împotriva Turciei, pct. 34-37]. Problema necesității notificării unei persoane cu privire la faptul că este supusă unor măsuri de interceptare este indisolubil legată de cea a caracterului efectiv al căilor de atac [Roman Zakharov împotriva Rusiei (MC), pct. 286].</p> <p>Examinarea și controlul măsurilor de supraveghere secretă pot interveni în cadrul a trei etape: în momentul dispunerii măsurii de supraveghere, în cursul punerii sale în aplicare sau ulterior încetării sale (ibidem, pct. 233-234 și trimiterile citate). În ceea ce privește primele două etape, procedurile existente trebuie să prevadă ele însele garanții adecvate și echivalente</p>

<p>lipsa sau prezența temeiurilor privind neinformarea persoanei, stabilește dacă aceste temeuri au caracter permanent sau provizoriu, și, după caz admite sau refuză autorizarea neinformării persoanei. În dependență de caracterul permanent sau provizoriu al temeiurilor de neinformare, judecătorul, poate autoriza neinformarea permanentă sau neinformarea pentru o anumită perioadă de timp determinată, dar nu mai mare de 1 an, Serviciul fiind obligat la expirarea perioadei respective să reevalueze temeiurile de neinformare și să întreprindă acțiunile necesare, în conformitate cu prevederile prezentului articol, inclusiv, după caz, să solicite neinformarea persoanei pentru o nouă perioadă de timp. Refuzul de a autoriza neinformarea poate fi contestat de către Serviciu cu recurs, aplicându-se, corespunzător, în acest sens prevederile art. 15 din prezenta Lege.</p> <p>(6) În cazul în care anticipat au dispărut temeiurile care au stat la baza neinformării persoanei supuse măsurii contrainformative, ofițerul de investigații întocmește un raport și îl prezintă spre aprobare directorului Serviciului prin care se solicită informarea imediată a persoanei. În cazul aprobării raportului, persoana se informează în condițiile alin. (1) din prezentul articol.</p> <p>(7) Încheierea judecătorului privind autorizarea neinformării, precum și raportul aprobat se anexează la dosarul special.</p>		<p>care să protejeze drepturile persoanei. Având în vedere că abuzurile se pot produce cu ușurință, în principiu, este de dorit să se încredințeze controlul măsurilor de supraveghere unei instanțe, întrucât controlul judecătoresc oferă cele mai bune garanții de independență și imparțialitate, precum și o procedură adecvată. În ceea ce privește cea de-a treia etapă – respectiv încetarea supravegherii – problema notificării a posteriori a măsurilor de supraveghere este strâns legată de cea a eficienței căilor de atac în fața instanțelor și, prin urmare, de existența unor garanții efective împotriva folosirii abuzive a competențelor de supraveghere. În principiu, persoana vizată nu poate sesiza instanțele judecătorești decât în cazul în care aceasta este informată cu privire la măsurile adoptate fără cunoștința sa și, astfel, poate să conteste retroactiv legalitatea lor sau, în altă ipoteză, suspectând că îi sunt sau i -au fost interceptate comunicările, persoana în cauză poate sesiza instanțele judecătorești, acestea având competență chiar dacă persoana care a făcut obiectul interceptării nu a fost informată cu privire la măsura în cauză (ibidem, pct. 233-234).</p> <p>Curtea a hotărât că, 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, fără să știe acest lucru și fără să aibă posibilitatea de a exercita o cale de atac la nivel național sau în fața organelor Convenției (Klass și alții împotriva Germaniei, pct. 36).</p>
<p><b>Articolul 55.</b></p> <p><b>Controlul asupra prelucrării datelor cu caracter personal în cadrul activității informative/contrainformative</b></p> <p>(1) Controlul asupra prelucrării datelor cu caracter personal în cadrul activității informative/contrainformative se efectuează, în exclusivitate, în conformitate cu prevederile prezentei Legi.</p> <p>(2) Prelucrarea datelor cu caracter personal în cadrul activității informative/contrainformative nu constituie obiectul legislației privind protecția datelor cu caracter personal.</p> <p>(3) Persoanele care au acces sau au luat cunoștință despre datele cu caracter personal ale persoanei care constituie obiectul activității informative/contrainformative, au obligația de a păstra confidențialitatea datelor respective.</p> <p>(4) Mecanismul de evidență și control al prelucrării datelor cu caracter personal în cadrul activității informative/contrainformative se stabilește prin act normativ departamental.</p>	<p>În forma actuală, prevederile acestui articol, în special alin. (2) <b>nu sunt compatibile</b> 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, 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>Se remarcă că urmare a ratificării Convenției pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal (<i>Convenția 108</i>) prin adoptarea Hotărârii Parlamentului nr. 483/1999, Republica Moldova s-a obligat să asigure corespunderea dreptului intern cu prevederile acesteia. Astfel, prin adoptarea Legii nr. 271/2013 au fost formulate declarații în privința modului de aplicare a Convenției 108, care stabilește excepțiile în care nu se vor aplica prevederile acesteia. Una dintre excepțiile declarate constituie circumstanța <b><u>prelucrării de date cu caracter personal atribuite la secret de stat în modul stabilit, cu excepția celor efectuate în cadrul acțiunilor de prevenire și investigare a infracțiunilor, al punerii în executare a sentințelor de condamnare sau al altor acțiuni ce țin de procedura penală ori contravențională, în condițiile legii.</u></b></p> <p>Reieșind din norma legală menționată, se relevă că atunci când sunt prelucrate date cu caracter personal în cadrul activităților enumerate la art. 1 pct. 1 lit. b) din Legea nr. 271/2013, la art. 2 alin. (2) lit. d) și la art. 2 art. (4) lit. b) din Legea nr. 133/2011 privind protecția datelor cu caracter personal, <b>prevederile Convenției 108 și a Legii nr. 133/2011 urmează a fi aplicate chiar dacă</b></p>

		<p><b>informațiile supuse prelucrării sunt atribuite la secret de stat.</b></p> <p>Suplimentar, evocăm că prin Decretul Președintelui Republicii Moldova nr. 757 din 22 decembrie 2022, 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>Articolul 14 din Protocol:</b> Textul Articolului 9 al Convenției (noul Articol 11) se înlocuiește cu următorul text:</p> <p>1. Nu se permite nici o excepție de la dispozițiile prezentului capitol, cu excepția dispozițiilor Articolului 5 alineatul 4, Articolul 7 alineatul 2, Articolul 8 alineatului 1 și Articolul 9, atunci când o astfel de excepție este prevăzută de lege, respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică pentru:</p> <p><i>a.</i> protecția securității naționale, apărarea, siguranța publică, interesele economice și financiare importante ale statului, imparțialitatea și independența sistemului judiciar sau prevenirea, cercetarea și urmărirea penală a infracțiunilor și executarea sancțiunilor penale și alte obiective esențiale de interes public general;</p> <p><i>b.</i> protecția persoanei vizate sau drepturile și libertățile fundamentale ale altora, în special libertatea de exprimare.</p> <p>2. Restricțiile privind exercitarea dispozițiilor prevăzute la Articolele 8 și 9 pot fi prevăzute de lege în ceea ce privește prelucrarea datelor în scopul arhivării, în interes public, în scopuri științifice sau istorice de cercetare sau în scopuri statistice, atunci când nu există riscuri recunoscute de încălcare a drepturilor și libertăților fundamentale ale persoanelor vizate.</p> <p>3. Pe lângă excepțiile prevăzute la alineatul 1 din prezentul articol, cu privire la activitățile de prelucrare în scopuri de securitate națională și de apărare, fiecare parte poate prevedea, prin lege și numai în măsura în care constituie o necesitate pentru îndeplinirea acestui scop, excepții de la Articolul 4 alineatul 3, Articolul 14 alineatele 5 și 6 și Articolul 15 alineatul 2, literele a, b, c și d.</p> <p><b>Acest aspect se realizează fără a aduce prejudicii cerinței ca activitățile de prelucrare în scopul securității naționale și al apărării să facă obiectul unei revizuri și supravegheri independente și efective în conformitate cu legislația internă a părții respective.</b></p> <p>Respectiv, se reconfirmă inclusiv din prevederile Protocolului de amendare a Convenției că pot fi admise anumite norme derogatorii pentru prelucrările de date efectuate în legătură cu protecția securității naționale, însă</p>
--	--	---

		acest lucru nu presupune faptul că acestea nu fac obiectul revizuirii și supravegherii de către un organ independent care să asigure un control permanent și efectiv.
<p><b>Articolul 56.</b></p> <p><b>Protecția datelor cu caracter personal ce nu au legătură cu amenințările la adresa securității naționale</b></p> <p>(1) Serviciul șterge datele cu caracter personal, colectate în cadrul activității informative/contrainformative, de îndată ce se constată că acestea nu au legătură cu amenințări la adresa securității naționale.</p> <p>(2) Informațiile privind datele cu caracter personal, viața privată, onoarea și reputația persoanelor, cunoscute incidental în cadrul obținerii datelor necesare realizării atribuțiilor Serviciului, dacă nu au relevanță pentru asigurarea securității statului, nu pot fi făcute publice, stocate sau arhivate, iar suportul pe care acestea sunt înregistrate va fi distrus sau, după caz, șters.</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 temei 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>Articolul 57.</b></p> <p><b>Controlul parlamentar</b></p> <p>(1) Controlul parlamentar asupra activității informative/contrainformative este exercitat de către Comisia securitate națională, apărare și ordine publică, prin intermediul Subcomisiei pentru exercitarea controlului parlamentar asupra activității Serviciului de Informații și Securitate al Republicii Moldova (în continuare – Subcomisia parlamentară).</p> <p>(2) Directorul Serviciului prezintă anual, în ședință închisă, Subcomisiei parlamentare un raport general cu privire la activitatea informativă/contrainformativă, care va cuprinde, în mod obligatoriu, informații despre numărul total al măsurilor contrainformative efectuate, numărul măsurilor contrainformative, stabilite la art. 12 alin. (1), efectuate, pe fiecare măsură în parte.</p> <p>(3) Subcomisia parlamentară poate solicita de la Președintele Judecătoriei Chișinău și Curții de Apel Chișinău informații privind numărul măsurilor contrainformative pentru care s-a eliberat mandat judecătoresc și numărul celor refuzate de a fi autorizate.</p> <p>(4) După prezentarea raportului, membrii Subcomisiei parlamentare pot înainta întrebări cu privire la activitatea informativă/contrainformativă înfăptuită de către Serviciu în anul precedent. În cadrul ședinței pot fi prezentate informații despre operațiunile finalizate realizate de către Serviciu, dacă divulgarea lor nu va prejudicia securitatea statului. Informații despre operațiunile în derulare nu se prezintă.</p> <p>(5) În baza raportului prezentat, Subcomisia parlamentară poate înainta recomandări privind activitatea Serviciului.</p> <p>(6) Raportul prezentat Subcomisiei parlamentare poate fi făcut public, excluzându-se din acesta informațiile atribuite la secret de stat.</p>	<p>În vederea eficientizării acestui tip de control, se propune:</p> <p>(7) <i>În baza informațiilor din Raportul general privind activitatea informativă /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 drept sau în instanța de judecată pe fapte de încălcare a legislației la efectuarea activității informative/contrainformative.</i></p> <p>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>În ceea ce privește măsurile generale adoptate de guvernul național, din jurisprudența Curții reiese că, pentru a stabili proporționalitatea unei măsuri generale, Curtea trebuie să evalueze în principal opțiunile legislative care stau la baza acesteia. În acest sens, <b>calitatea controlului parlamentar și judiciar al necesității măsurii este deosebit de importantă</b>, inclusiv aplicarea marjei de apreciere relevantă. Garanțiile procedurale de care dispune persoana particulară sunt deosebit de importante pentru a determina dacă statul pârât și-a depășit sau nu marja de apreciere atunci când a stabilit cadrul de reglementare. Curtea trebuie să examineze, în special, dacă procesul decizional finalizat prin măsuri care constituie o ingerință a fost echitabil și a permis respectarea adecvată a intereselor garantate unei persoane de către art. 8 (A.-M.V. împotriva Finlandei, pct. 82-84).</p>

<p><b>Articolul 58.</b> <b>Controlul exercitat de către procuror</b></p> <p>(1) Controlul exercitat de către procuror asupra activității contrainformative se efectuează de către procurori din cadrul Procuraturii Generale, special împuterniciți în acest sens de către Procurorul General.</p> <p>(2) Controlul se efectuează în baza plingerilor depuse de către persoane ale căror drepturi și interese legitime se presupune că au fost încălcate sau din oficiu, în cazul în care procurorului i-au devenit cunoscute informații despre încălcarea legislației la efectuarea măsurilor contrainformative, dacă aceste fapte pot constitui infracțiuni.</p> <p>(3) În timpul controlului, informația privind activitatea persoanele care au colaborat sau colaborează confidențial cu Serviciul poate fi prezentată doar unui procuror din categoria celor menționați la alin. (1), împuternicit special în acest sens prin ordin al Procurorului General. Informația se prezintă doar dacă aceasta este în legătură directă cu obiectul controlului efectuat și doar dacă este absolut necesară realizării controlului.</p> <p>(4) Procurorii, premergător împuternicirii de a exercita controlul asupra activității contrainformative, vor perfecta dreptul de acces la secretul de stat, dacă la moment nu dispun de asemenea drept, și vor fi supuși verificării în conformitate cu prevederile Legii nr. 271/2008 privind verificarea titularilor și a candidaților la funcții publice, indiferent de data ultimei verificări.</p>	<p>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.</p> <p>Suplimentar, se propune completarea cu alineat nou:</p> <p><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><b>Garanțiile procedurale de care dispune persoana particulară sunt deosebit de importante pentru a determina dacă statul pârât și-a depășit sau nu marja de apreciere atunci când a stabilit cadrul de reglementare.</b></p> <p>Curtea trebuie să examineze, în special, dacă procesul decizional finalizat prin măsuri care constituie o ingerință a fost echitabil și a permis respectarea adecvată a intereselor garantate unei persoane de către art. 8 (<i>A.-M.V. împotriva Finlandei, pct. 82-84</i>).</p> <p><b>Examinarea și controlul măsurilor de supraveghere secretă</b> pot interveni în cadrul a <b>trei etape: în momentul dispunerii măsurii de supraveghere, în cursul punerii sale în aplicare sau ulterior încetării</b> sale. În ceea ce privește primele două etape, procedurile existente trebuie să prevadă ele însele garanții adecvate și echivalente care să protejeze drepturile persoanei. Având în vedere că abuzurile se pot produce cu ușurință, în principiu, este de dorit să se <b>încredințeze controlul măsurilor de supraveghere unei instanțe</b>, întrucât controlul judecătoresc oferă cele mai bune garanții de independență și imparțialitate, precum și o procedură adecvată. În ceea ce privește cea de-a treia etapă – respectiv încetarea supravegherii – <b>problema notificării a posteriori a măsurilor de supraveghere este strâns legată de cea a eficienței căilor de atac în fața instanțelor</b> și, prin urmare, de <b>existența unor garanții efective împotriva folosirii abuzive a competențelor de supraveghere</b>. În principiu, persoana vizată nu poate sesiza instanțele judecătorești decât în cazul în care aceasta este informată cu privire la măsurile adoptate fără cunoștința sa și, astfel, poate să conteste retroactiv legalitatea lor sau, în altă ipoteză, suspectând că îi sunt sau i-au fost interceptate comunicările, persoana în cauză poate sesiza instanțele judecătorești, acestea având competență chiar dacă persoana care a făcut obiectul interceptării nu a fost informată cu privire la măsura în cauză.</p>
<p><b>Articolul 60.</b> <b>Controlul exercitat de către magistrați</b></p> <p>Controlul exercitat de către magistrați 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>Se propune completarea articolului cu un alineat nou:</p> <p><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>Un reclamant poate pretinde că este victima unei încălcări ocazionale de simplă existență a unor măsuri de supraveghere secretă sau a unei legislații care permite instituirea unor astfel de măsuri, în cazul în care sunt îndeplinite anumite condiții [<i>Roman Zakharov împotriva Rusiei (MC), pct. 171-172</i>]. În această cauză, Curtea a constatat că abordarea din <i>cauza Kennedy</i> este cel mai bine adaptată la <b>necesitatea de a garanta că natura secretă a măsurilor de supraveghere nu are ca rezultat măsuri imposibil de contestat în mod eficient</b> și care se află în afara sferei controlului exercitat de autoritățile judiciare naționale și de Curte (<i>Kennedy împotriva Regatului Unit, pct. 124</i>).</p> <p>Legislația internă ar trebui să ofere garanții suficient de precise, eficiente și cuprinzătoare cu privire la dispunerea și executarea măsurilor de supraveghere, <b>precum și la posibilitățile</b></p>

		<p><b>de reparare a consecințelor acestora</b> (<i>Szabó și Vissy împotriva Ungariei</i>).</p> <p>Având în vedere că abuzurile se pot produce cu ușurință, în principiu, este de dorit să se <b>încredințeze controlul măsurilor de supraveghere unei instanțe</b>, întrucât controlul judecătoresc oferă cele mai bune garanții de independență și imparțialitate, precum și o procedură adecvată. În ceea ce privește cea de-a treia etapă – respectiv încetarea supravegherii – <b>problema notificării a posteriori a măsurilor de supraveghere este strâns legată de cea a eficienței căilor de atac în fața instanțelor și, prin urmare, de existența unor garanții efective împotriva folosirii abuzive a competențelor de supraveghere</b>. În principiu, persoana vizată nu poate sesiza instanțele judecătorești decât în cazul în care aceasta este informată cu privire la măsurile adoptate fără cunoștința sa și, astfel, poate să conteste retroactiv legalitatea lor sau, în altă ipoteză, suspectând că îi sunt sau i-au fost interceptate comunicările, persoana în cauză poate sesiza instanțele judecătorești, acestea având competență chiar dacă persoana care a făcut obiectul interceptării nu a fost informată cu privire la măsura în cauză.</p>
--	--	--

### **III. Cu referire la prevederile Notei informative a proiectului de lege nr. 422 privind activitatea contrainformativă și informativă externă:**

Examinând conținutul Notei informative, s-a relevat că autorii nu au adus argumente care să justifice rezonabil că, la stabilirea cadrului de reglementare în domeniul securității naționale, nu s-a depășit marja de apreciere a unui stat contractant al Convențiilor internaționale în domeniul drepturilor omului, ratificate de Republica Moldova.

În acest sens, atragem atenția asupra următoarelor cazuri din jurisprudența CtEDO:

Art. 8 § 2 din Convenție enumeră **scopurile legitime care pot justifica o ingerință** în exercitarea drepturilor protejate de art. 8: „este necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei, ori protejarea drepturilor și libertăților altora”. Curtea a stabilit că **este sarcina guvernului pârât să demonstreze că ingerința a avut un scop legitim** [*Mozer împotriva Republicii Moldova și Rusiei (MC)*, pct. 194].

Ulterior, Curtea a afirmat că, pentru a stabili dacă măsurile atacate erau „**necesare într-o societate democratică**”, va analiza, în lumina cauzei respective în ansamblul său, dacă motivele invocate pentru justificarea măsurilor sunt relevante și suficiente și dacă măsurile au fost proporționale cu scopurile legitime urmărite (*Z împotriva Finlandei*, pct. 94). Curtea a oferit clarificări suplimentare privind această cerință, afirmând că noțiunea de „necesitate” în sensul art. 8 implică faptul că **ingerința trebuie să corespundă unei nevoi sociale imperioase și, în special, că trebuie să rămână proporțională cu scopul legitim urmărit**. Pentru a stabili dacă o ingerință a fost „necesară”, Curtea ține seama de marja de apreciere lăsată autorităților statului, însă **este obligația statului pârât să demonstreze existența unei nevoi sociale imperioase, care a stat la baza ingerinței** (*Piechowicz împotriva Poloniei*, pct. 212). „

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 [*Weber și Saravia împotriva Germaniei (dec.), pct. 78*]. 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 nu beneficiază de o putere discreționară nelimitată de a supune persoanele aflate în jurisdicția lor unor măsuri de supraveghere secretă. Curtea a afirmat că statele contractante nu pot adopta, în numele luptei împotriva spionajului și a terorismului, orice măsură pe care o consideră adecvată, 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 [*Klass și alții împotriva Germaniei, pct. 42; Szabó și Vissy împotriva Ungariei, pct. 72-73*]. O astfel de ingerință trebuie susținută de motive pertinente și suficiente și trebuie să fie proporțională cu obiectivul sau obiectivele legitime urmărite (*Segerstedt-Wiberg și alții împotriva Suediei, pct. 88*).

Adițional, s-a stabilit că în conținutul notei se face trimitere la opinia unor experți internaționali, în condițiile în care aceștia s-au expus pe alte proiecte de legi similare care diferă substanțial de cel actual, din care motiv, considerăm că aceste opinii nu pot fi abordate în contextul actual.

*Cu privire la prevederile proiectelor de lege nr. 420 privind Serviciul de Informații și Securitate, nr. 421 privind statutul ofițerului de informații și securitate, precum și nr. 422 privind activitatea contrainformativă și activitatea informativă externă, CNPDCP se va expune, după caz, inclusiv în procedura de avizare a acestora.*

**Victoria MUNTEAN**  
**Director**