Ministerul Afacerilor Interne
Inspectoratul General al Poliției
Centrul pentru combaterea crimelor informatice

Proiectul de lege nr. 161 (2016) pentru modificarea şi completarea unor acte legislative

Chișinău, 2017

Baza juridică (acte internaționale)

- Convenţia Consiliului Europei privind criminalitatea informatică
- Convenţia Consiliului Europei pentru protecţia copiilor împotriva exploatării sexuale şi a abuzurilor sexuale
- Directiva 2011/92/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile
- Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora
- Pactul internaţional privind drepturile civile şi politice al Naţiunilor Unite (1966)

Procesul de elaborare și promovare

- **PHG expediat spre avizare în instituțiile de stat abilitate**
Decembrie 2012

- **PHG publicat pe pagina web a MAI la compartimentul transparență decizională**
Decembrie 2012

- **Expertiza juridică**
Mai 2013

- **PHG expediat spre avizare în instituțiile de stat abilitate**
Martie 2014

- **PHG publicat pe pagina web a MAI la compartimentul transparență decizională**
Martie 2015

- **Expertiza anticorupție**
Septembrie 2015

- **PHG expediat spre avizare în instituțiile de stat abilitate**
Februarie 2016

- **Aprobat în ședință de Guvern**
Martie 2016

- **Înregistrat în Parlament cu nr. 161**
Aprilie 2016

Evenimente comune cu participarea societății civile

- **Şedinţă de lucru, sediul MAI - 18.10.2013**

Consiliul Naţional pentru Participare de pe lîngă Guvern, ONG „La Strada”, ONG „Credo”, „Publika”, „Unimedia”, „www.privesc.eu”, „Orange Moldova”, „Moldcell”, „Moldtelecom”, „Starnet”, „Sun Communications”, „Arax-Impex”, „DAAC-Hermes”, „Interact Media”, „999.md” ş.a.

- **Şedinţă de lucru, sediul IGP - 09.07.2015**

”Asociația Națională a Companiilor TIC din Moldova”, ”Arax-Impex”, ”Moldcell”, ”Orange Moldova”, ”Centrul pentru Jurnalism Independent”.

- **Dezbateri IPN - 04.04.2016**

”Centrul pentru Jurnalism Independent”, ”StarNet”.

- **Teleradio-Moldova - Emisiunea ”Spațiul Public” – 08.04.2016**

”Centrul pentru Jurnalism Independent”.

- **”Generator Hub”, clădirea Kentford - 19.04.2016**

”Interakt Media”, ”Starnet”, ”Centrul de Resurse Juridice din Moldova”, Consultant în domeniu IT/antreprenor, Blogger, Lector universitar, antreprenor, fondator ”www.privesc.eu” ș.a.

- **Conferința internațională cu privire la Ziua Drepturilor Utilizatorilor de Internet în Republica Moldova, Radisson-Blue - 28.04.2016**

”Centrul pentru Jurnalism Independent”.

- **Şedinţă de lucru, sediul MAI - 23.05.2016**

”Orange Moldova”.

- **Dezbatere publică, Joly Alon - 10.10.2016**

”Centrul de Resurse Juridice din Moldova”.

- **Dezbatere publică, sediul ”PromoLex” – 14.02.2017**

”PromoLex”, ”Centrului Internațional de Drept Necomercial (ICNL)”, ”Centrul de Resurse Juridice din Moldova”, ”Asociația Națională a Companiilor TIC din Moldova”, ”Ziarul de Gardă”, companii TIC ș.a.

Actele legislative propuse pentru modificare/completare

Art. I. Legea nr. 753/1999 privind Serviciul de Informaţii şi Securitate

Art. II. Codul penal

Art. III. Codul de procedură penală

Art. IV. Legea nr. 264/2005 cu privire la exercitarea profesiunii de medic

Art. V. Legea nr. 20/2007 comunicaţiilor electronice

Art. VI. Codul contravenţional

Art. VII. Legea nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice

Art. VIII. Legea nr. 59/2012 privind activitatea specială de investigaţii

Art. I. Legea nr. 753/1999
privind Serviciul de Informaţii şi Securitate

Articolul 7. Atribuţiile Serviciului
Serviciului îi revin atribuţiile:
...
e) asigurarea tehnică a interceptării **datelor informatice şi a** comunicărilor efectuate prin intermediul reţelelor de comunicaţii electronice, cu utilizarea unor mijloace tehnice speciale, conectate, în caz de necesitate, la echipamentul furnizorilor de reţele şi/sau servicii de comunicaţii electronice;

Codul de procedură penală

Articolul 132/9. Efectuarea şi certificarea interceptării şi înregistrării comunicărilor

(1) Interceptarea şi înregistrarea comunicărilor se efectuează de către organul de urmărire penală sau de către ofiţerul de investigaţii. Asigurarea tehnică a interceptării comunicărilor se realizează de către autoritatea abilitată prin lege cu asemenea atribuţii, utilizîndu-se mijloace tehnice speciale. Colaboratorii subdiviziunii din cadrul instituţiei autorizate prin lege, care asigură tehnic interceptarea şi înregistrarea comunicărilor, precum şi persoanele care efectuează nemijlocit ascultarea înregistrărilor, ofiţerii de urmărire penală şi procurorul sînt obligaţi să păstreze secretul comunicărilor şi poartă răspundere pentru încălcarea acestei obligaţii.

(4) Subdiviziunea tehnică a organului abilitat prin lege să efectueze interceptarea şi înregistrarea comunicărilor transmite organului de urmărire penală semnalul comunicărilor interceptate şi alte informaţii indicate în extrasul din încheierea judecătorului de instrucţie în regim de timp real, fără a efectua înregistrarea acestora.

(6) Informaţia obţinută în procesul interceptării şi înregistrării comunicărilor se transmite, de către subdiviziunea tehnică care a efectuat interceptarea comunicărilor, ofiţerului de urmărire penală sau procurorului pe purtător material de informaţii împachetat, sigilat cu ştampila subdiviziunii tehnice şi cu indicarea numărului de ordine al purtătorului material.

(7) În termen de 24 de ore după expirarea termenului de autorizare a interceptării, organul de urmărire penală sau, după caz, procurorul întocmeşte la finele fiecărei perioade de autorizare, un proces-verbal privind interceptarea şi înregistrarea comunicărilor.

(13) Comunicările interceptate şi înregistrate se vor păstra integral pe suportul iniţial prezentat organului de urmărire penală de către subdiviziunea tehnică. Acest suport se va păstra la judecătorul de instrucţie care a autorizat măsura specială de investigaţii.

(15) În termen de 48 de ore de la finisarea perioadei de autorizare a interceptării şi înregistrării, procurorul prezintă judecătorului de instrucţie procesul-verbal şi suportul în original pe care au fost înregistrate comunicările. Judecătorul de instrucţie se expune printr-o încheiere asupra respectării cerinţelor legale la interceptarea şi înregistrarea comunicărilor de către organul de urmărire penală şi decide care din comunicările înregistrate urmează a fi nimicite, desemnînd persoanele responsabile de nimicire. Nimicirea informaţiilor în baza încheierii judecătorului de instrucţie este consemnată de către persoana responsabilă într-un proces-verbal, care se anexează la cauza penală.

HG Nr. 1123 din 14-12-2010
privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal

- Securitatea mediului fizic şi a tehnologiilor informaţionale folosite în procesul prelucrării datelor cu caracter personal
- Identificarea şi autentificarea utilizatorului sistemului informaţional de date cu caracter personal
- Administrarea accesului utilizatorilor
- Protecţia sistemelor informaţionale şi comunicaţiilor în care sînt prelucrate date cu caracter personal
- Auditul securităţii în sistemele informaţionale de date cu caracter personal
- Etc.

Art. II. Codul penal

1. În tot cuprinsul codului, cuvîntul „telecomunicaţii”, la orice caz gramatical, se substituie cu cuvintele „comunicaţii electronice”, la cazul gramatical corespunzător.

2. **Articolul 178. Violarea dreptului la secretul corespondenţei**

(1) Violarea dreptului la secretul scrisorilor, telegramelor, coletelor şi altor trimiteri poştale, al convorbirilor telefonice şi ~~înştiinţărilor telegrafice~~ comunicărilor electronice, cu încălcarea legislaţiei

[…]

Art. II. Codul penal

3. **Articolul 208/1. Pornografia infantilă**
Producerea, distribuirea, difuzarea, importarea, exportarea, oferirea, vinderea, procurarea, schimbarea, folosirea, obținerea cu bună știință, prin intermediul tehnologiilor informaționale sau comunicațiilor electronice, a accesului sau deținerea de imagini sau alte reprezentări ale unui sau mai mulți copii implicați în activități sexuale explicite, reale sau simulate, ori de imagini sau alte reprezentări ale organelor sexuale ale unui copil, reprezentate de manieră lascivă sau obscenă, inclusiv în formă electronică,
se pedepsește cu închisoare ~~de la 1 la 3 ani~~ de la 3 la 7 ani, cu amendă, aplicată persoanei juridice, de la 3000 la 5000 de unități convenționale cu privarea de dreptul de a exercita o anumită activitate.

Convenția Lanzarote
Art. 20 Para. 1 lit. f.

Art. II. Codul penal

4. **Articolul 259. Accesul ilegal la informaţia computerizată**
(1) Accesul ilegal la informaţia computerizată, adică la informaţia din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică, al unei persoane care nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic, dacă este însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice ~~şi dacă a cauzat daune în proporţii mari~~,
[...]
(2) Aceeaşi acţiune săvîrşită:
h) ~~în proporţii deosebit de mari~~ cu cauzarea de daune în proporţii mari.

5. **Articolul 260. Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a mijloacelor tehnice sau produselor program**
[...]
se pedepseşte cu amendă în mărime ~~de la 500 la 1000 unităţi convenţionale~~ de la 200 la 500 unităţi convenţionale sau cu închisoare ~~de la 2 la 5 ani~~ de pînă la 3 ani, cu amendă, aplicată persoanei juridice, în mărime de la 4000 la 7000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea întreprinderii.

Art. II. Codul penal

6. **Articolul 260[1]. Interceptarea ilegală a unei transmisii de date informatice**
[...]
se pedepseşte cu amendă în mărime de la 850 la 1350 unităţi convenţionale sau cu închisoare ~~de la 2 la 5 ani~~ de pînă la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 4000 la 7000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea întreprinderii.

7. **Articolul 260[2]. Alterarea integrităţii datelor informatice ţinute într-un sistem informatic**
Modificarea, ştergerea sau deteriorarea intenţionată şi fără drept a datelor informatice ţinute într-un sistem informatic ori restricţionarea ilegală a accesului la aceste date, transferul neautorizat de date informatice dintr-un sistem informatic, dintr-un mijloc de stocare, dobîndirea, comercializarea sau punerea la dispoziţie, sub orice formă, a datelor informatice cu acces limitat~~, dacă aceste acţiuni au cauzat daune în proporţii mari~~,
se pedepsesc cu amendă în mărime de la 850 la 1350 unităţi convenţionale sau cu închisoare ~~de la 2 la 5 ani~~ de pînă la 5 ani.

Art. II. Codul penal

8. **Articolul 260³. Perturbarea funcţionării sistemului informatic**

(1) Perturbarea funcţionării unui sistem informatic prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea intenţionată şi fără drept adatelor informatice sau prin restricţionarea accesului la aceste date~~, dacă aceste acţiuni au cauzat daune în proporţii mari~~,

se pedepseşte cu amendă în mărime de la 1050 la 1350 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare ~~de la 2 la 5 ani~~ de pînă la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 4000 la 7000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea întreprinderii.

(2) Aceeaşi acţiune:

[...]

~~d) care a cauzat daune în proporţii deosebit de mari~~

d) care a cauzat daune în proporţii mari

9. **Articolul 260⁴. Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a parolelor, codurilor de acces sau a datelor similare**

(1) Producerea, importul, comercializarea sau punerea la dispoziţie, sub orice altă formă, în mod ilegal, a unei parole, a unui cod de acces sau a unor date similare care permit accesul total sau parţial la un sistem informatic în scopul săvîrşirii uneia dintre infracţiunile prevăzute la art.237, 259, 260¹–260³, 260⁵ şi 260⁶~~, dacă aceste acţiuni au cauzat daune în proporţii mari~~,

se pedepsesc cu amendă în mărime de la 850 la 1350 unităţi convenţionale sau cu închisoare ~~de la 2 la 5 ani~~ de pînă la 3 ani, cu amendă, aplicată persoanei juridice, în mărime de la 2000 la 4000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(2) Aceleaşi acţiuni:

[...]

~~d) care au cauzat daune în proporţii deosebit de mari~~

d) care au cauzat daune în proporţii mari

Art. II. Codul penal

10. **Articolul 260^5. Falsul informatic**

[...]

se pedepsesc cu amendă în mărime de la 1350 la 1850 unităţi convenţionale sau cu închisoare ~~de la 2 la 5 ani~~ de pînă la 5 ani.

11. **Articolul 260^6 . Frauda informatică**

(1) Introducerea, modificarea sau ştergerea intenţionată şi fără drept a datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul~~, dacă aceste acţiuni au cauzat daune în proporţii mari~~,

se pedepsesc cu amendă în mărime de la 1350 la 1850 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare ~~de la 2 la 5 ani~~ de pînă la 5 ani.

(2) Aceleaşi acţiuni:

[...]

~~b) care au cauzat daune în proporţii deosebit de mari~~

b) care au cauzat daune în proporţii mari

se pedepsesc cu închisoare ~~de la 4 la 9 ani~~ de la 4 la 10 ani.

(3) Acţiunile prevăzute la alin. (1) sau (2) din prezentul articol, care au cauzat daune în proporţii deosebit de mari,

se pedepsesc cu închisoare de la 8 la 15 ani.

Art. II. Codul penal

12. **Articolul 261[1]. Accesul neautorizat la reţelele şi serviciile de telecomunicaţii**
(1) Accesul neautorizat la reţelele şi/sau serviciile de telecomunicaţii cu utilizarea reţelelor şi/sau serviciilor de telecomunicaţii ale altor operatori~~, dacă acesta a cauzat daune în proporţii mari~~,
se pedepseşte cu amendă în mărime de la 850 la 1350 unităţi convenţionale sau cu închisoare ~~de pînă la 1 an~~ de pînă la 2 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 2000 la 4000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.
(2) Aceeaşi acţiune:
[...]
~~e) care a cauzat daune în proporţii deosebit de mari~~
e) care a cauzat daune în proporţii mari
[...]

Codul de procedură penală

Articolul 15. Inviolabilitatea vieţii private.

(1) Orice persoană are dreptul la inviolabilitatea vieţii private, la confidenţialitatea vieţii intime, familiale, la protejarea onoarei şi demnităţii personale. În cursul procesului penal, nimeni nu este în drept să se implice în mod arbitrar şi nelegitim în viaţa intimă a persoanei.

(2) La efectuarea acţiunilor procesuale nu poate fi acumulată fără necesitate informaţie despre viaţa privată şi intimă a persoanei. La cererea organului de urmărire penală şi a instanţei de judecată, participanţii la acţiunile procesuale sînt obligaţi să nu divulge asemenea informaţii şi despre aceasta se ia un angajament în scris. Prelucrarea datelor cu caracter personal în cadrul procesului penal se efectuează în conformitate cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecţia datelor cu caracter personal.

(3) Persoanele de la care organul de urmărire penală cere informaţie despre viaţa privată şi intimă sînt în drept să se convingă că această informaţie se administrează într-o cauză penală concretă. Persoana nu este în drept să refuze de a prezenta informaţii despre viaţa privată şi intimă a sa sau a altor persoane sub pretextul inviolabilităţii vieţii private, însă ea este în drept să ceară de la organul de urmărire penală explicaţii asupra necesităţii obţinerii unei asemenea informaţii, cu includerea explicaţiilor în procesul-verbal al acţiunii procesuale respective.

(4) Probele care confirmă informaţia despre viaţa privată şi intimă a persoanei, la cererea acesteia, se examinează în şedinţă de judecată închisă.

(5) Prejudiciul cauzat persoanei în cursul procesului penal prin violarea vieţii private şi intime a acesteia se repară în modul stabilit de legislaţia în vigoare.

Codul de procedură penală

Articolul 128. Procedura efectuării percheziţiei sau ridicării de obiecte şi documente.

(1) Este interzis de a efectua ridicări de obiecte şi documente sau de a face percheziţii în timpul nopţii, cu excepţia cazurilor de delict flagrant.

(3) Pînă la începerea percheziţiei sau ridicării de obiecte şi documente, reprezentantul organului de urmărire penală este obligat să înmîneze, sub semnătură, persoanei la care se face percheziţia sau ridicarea copia de pe ordonanţa respectivă. Ordonanţa trebuie să conţină, pe lîngă datele prevăzute la art. 255, date cu privire la obiectele sau documentele căutate.

(5) În cadrul efectuării percheziţiei, după prezentarea ordonanţei, reprezentantul organului de urmărire penală cere să i se predea obiectele şi documentele menţionate în ordonanţă. Instituţiile financiare nu pot invoca secretul bancar drept motiv pentru a refuza prezentarea documentelor solicitate. Dacă obiectele şi documentele căutate se predau benevol, persoana care efectuează urmărirea penală se limitează la ridicarea acestora, fără a mai efectua alte măsuri de investigaţii.

(8) La efectuarea percheziţiei pot fi utilizate mijloace tehnice, fapt ce va fi menţionat în procesul-verbal.

(9) Organul de urmărire penală este obligat să ia măsuri pentru a nu se da publicităţii circumstanţele privitor la viaţa intimă a persoanei, constatate în legătură cu efectuarea percheziţiei sau ridicării.

Codul de procedură penală

Articolul 164. Înregistrările audio sau video, fotografiile şi alte forme de purtători de informaţie

Înregistrările audio sau video, fotografiile, mijloacele de control tehnic, electronic, magnetic, optic şi alţi purtători de informaţie tehnico-electronică, dobîndite în condiţiile prezentului cod, constituie mijloace de probă dacă ele conţin date sau indici temeinici privind pregătirea sau săvîrşirea unei infracţiuni şi dacă conţinutul lor contribuie la aflarea adevărului în cauza respectivă.

Articolul 159. Păstrarea corpurilor delicte şi a altor obiecte

(1) Corpurile delicte se anexează la dosar şi se păstrează în dosar sau se păstrează în alt mod prevăzut de lege. Corpurile delicte care, din cauza volumului sau din alte motive, nu pot fi păstrate împreună cu dosarul trebuie fotografiate şi fotografiile se anexează la procesul-verbal respectiv. [...]

(6) Corpurile delicte şi alte obiecte ridicate se păstrează pînă ce soarta lor nu va fi soluţionată prin hotărîre definitivă a organului de urmărire penală sau a instanţei. În cazurile prevăzute de prezentul cod, chestiunile privind corpurile delicte pot fi soluţionate pînă la terminarea procesului penal.

Articolul 160. Asigurarea păstrării corpurilor delicte şi a altor obiecte în cadrul desfăşurării procesului penal

(1) La păstrarea corpurilor delicte şi a altor obiecte, la transmiterea lor pentru efectuarea expertizei sau a constatării tehnico-ştiinţifice sau medico-legale, precum şi la transmiterea cauzei altui organ de urmărire penală sau altei instanţe judecătoreşti trebuie să fie luate măsuri pentru a preveni pierderea, deteriorarea, alterarea, atingerea între ele sau amestecul corpurilor delicte ori al altor obiecte.

(2) În cazul transmiterii cauzei, în documentul de însoţire, în anexele la el şi în informaţia anexată la rechizitoriu se indică toate corpurile delicte şi alte obiecte care au fost anexate la dosar şi pe care îl însoţesc, precum şi locul lor de păstrare dacă ele nu sînt anexate la dosar.

(3) La transmiterea cauzei în care figurează corpuri delicte, organul care primeşte cauza verifică prezenţa obiectelor anexate la dosar în conformitate cu datele menţionate în documentul de însoţire a cauzei. Despre rezultatele acestei verificări se face menţiune în documentul de însoţire.

Codul de procedură penală

Articolul 162. Hotărîrea cu privire la corpurile delicte adoptată la soluţionarea cauzei penale

(1) În cazul în care procurorul dispune încetarea urmăririi penale sau în cazul soluţionării cauzei în fond, se hotărăşte chestiunea cu privire la corpurile delicte. În acest caz:

1) uneltele care au servit la săvîrşirea infracţiunii vor fi confiscate şi predate instituţiilor respective sau nimicite;

2) obiectele a căror circulaţie este interzisă vor fi predate instituţiilor respective sau nimicite;

3) lucrurile care nu prezintă nici o valoare şi care nu pot fi utilizate vor fi distruse, iar în cazurile în care sînt cerute de persoane ori instituţii interesate, ele pot fi remise acestora;

4) [...] Celelalte obiecte se predau proprietarilor legali [...]. În caz de conflict referitor la apartenenţa acestor obiecte, litigiul se soluţionează în ordinea procedurii civile;

5) documentele care constituie corpuri delicte rămîn în dosar pe tot termenul de păstrare a lui sau, la solicitare, se remit persoanelor interesate;

6) obiectele ridicate de organul de urmărire penală, dar care nu au fost recunoscute corpuri delicte, se remit persoanelor de la care au fost ridicate.

(2) Valoarea obiectelor alterate, deteriorate sau pierdute în urma efectuării expertizei şi a altor acţiuni legale se atribuie la cheltuielile judiciare. Dacă aceste obiecte au aparţinut învinuitului, inculpatului sau persoanei civilmente responsabile, contravaloarea acestora nu se restituie. Dacă aceste obiecte au aparţinut altor persoane, contravaloarea lor se restituie din bugetul de stat şi poate fi încasată de la condamnat sau de la partea civilmente responsabilă.

(3) În caz de achitare a persoanei, precum şi în caz de scoatere de sub urmărire penală pe temei de reabilitare, contravaloarea obiectelor alterate sau pierdute în cadrul efectuării expertizei sau a altor acţiuni legale se restituie proprietarului sau posesorului legal, indiferent de calitatea lui procesuală, din bugetul de stat.

(4) În cazul în care corpurile delicte au fost transmise conform destinaţiei potrivit prevederilor art.161 alin.(3), proprietarului sau, după caz, posesorului legal i se restituie obiecte de acelaşi gen şi calitate sau i se plăteşte contravaloarea lor pornind de la preţurile libere în vigoare la momentul compensării.

Codul de procedură penală

Articolul 298. Plîngerile împotriva acţiunilor organului de urmărire penală şi ale organului care exercită activitate operativă de investigaţii

(1) Împotriva acţiunilor, inacţiunilor şi actelor organului de urmărire penală şi ale organului care exercită activitate specială de investigaţii pot înainta plîngere bănuitul, învinuitul, reprezentantul lor legal, apărătorul, partea vătămată, partea civilă, partea civilmente responsabilă şi reprezentanţii acestora, precum şi alte persoane ale căror drepturi şi interese legitime au fost lezate de aceste organe.

(2) Plîngerea se adresează procurorului care conduce urmărirea penală şi se depune fie direct la acesta, fie la organul de urmărire penală. În cazurile în care plîngerea a fost depusă la organul de urmărire penală, acesta este obligat să o înainteze, în termen de 48 de ore de la primirea ei, procurorului împreună cu explicaţiile sale sau ale organului care exercită activitate specială de investigaţii, atunci cînd acestea sînt necesare.

(3) Plîngerea depusă în condiţiile prezentului articol nu suspendă executarea acţiunii sau actelor atacate dacă procurorul care conduce urmărirea penală nu consideră aceasta necesar.

Articolul 306. Încheierile judecătoreşti privind efectuarea acţiunilor de urmărire penală, măsurilor speciale de investigaţii sau privind aplicarea măsurilor procesuale de constrîngere

În încheierea judecătorească privind efectuarea acţiunilor de urmărire penală, măsurilor speciale de investigaţii sau privind aplicarea măsurilor procesuale de constrîngere se va indica: data şi locul întocmirii ei, numele şi prenumele judecătorului de instrucţie, persoana cu funcţie de răspundere şi organul care a înaintat demersul, organul care efectuează acţiuni de urmărire penală, măsurilor speciale de investigaţii sau aplică măsurile procesuale de constrîngere, cu indicarea scopului efectuării acestor acţiuni sau măsuri şi a persoanei la care se referă ele, precum şi menţiunea despre autorizarea acţiunii sau respingerea ei în caz de existenţă a obiecţiilor apărătorului, reprezentantului legal, bănuitului, învinuitului, inculpatului, motivîndu-se admiterea sau neadmiterea lor la aplicarea măsurii de constrîngere, termenul pentru care este autorizată acţiunea, persoana cu funcţie de răspundere sau organul abilitat de a executa încheierea, semnătura judecătorului de instrucţie certificată cu ştampila instanţei judecătoreşti.

Codul de procedură penală

Articolul 132/1. Dispoziţiile generale privind activitatea specială de investigaţii

[...]

(2) Măsurile speciale de investigaţii se dispun şi se efectuează dacă sînt îndeplinite cumulativ următoarele condiţii:

1) pe altă cale este imposibilă realizarea scopului procesului penal şi/sau poate fi prejudiciată considerabil activitatea de administrare a probelor;

2) există o bănuială rezonabilă cu privire la pregătirea sau săvîrşirea unei infracţiuni grave, deosebit de grave sau excepţional de grave, cu excepţiile stabilite de lege;

3) acţiunea este necesară şi proporţională cu restrîngerea drepturilor şi libertăţilor fundamentale ale omului.

Art. III. Codul de procedură penală

1. Articolul 130[1]. Percheziţia informatică şi ridicarea obiectelor care conţin date informatice

(1) Prin percheziţie informatică se înţelege procesul de căutare, cercetare, descoperire, identificare şi acumulare a datelor informatice existente într-un sistem informatic sau suport de stocare a datelor informatice, care au importanță pentru cauza penală, realizat prin intermediul unor metode şi mijloace tehnice ce asigură integritatea şi autenticitatea informaţiilor conţinute în acestea.

(2) Percheziţia informatică se efectuează în baza ordonanţei motivate a organului de urmărire penală şi numai cu autorizaţia judecătorului de instrucţie.

(3) La efectuarea percheziţiei informatice și/sau ridicarea obiectelor care conţin date informatice trebuie să fie asigurată prezenţa persoanei la care se face percheziția şi/sau ridicarea ori a unor membri adulţi ai familiei acesteia, ori a celor care reprezintă interesele persoanei în cauză. Dacă prezenţa acestor persoane este imposibilă, se invită reprezentantul autorităţii executive a administraţiei publice locale.

(4) Percheziția informatică și ridicarea obiectelor care conţin date informatice în încăperile instituţiilor, întreprinderilor, organizaţiilor şi unităţilor militare se efectuează în prezenţa reprezentantului respectiv.

(5) În cazul în care, în cadrul efectuării percheziţiei unui sistem informatic sau a unui suport de stocare a datelor informatice, se constată că datele informatice căutate sînt cuprinse parţial sau integral într-un alt sistem informatic ori suport de stocare a datelor informatice şi sînt în mod legal accesibile de la sistemul sau suportul iniţial perchiziţionat ori sunt disponibile pentru sistemul sau suportul iniţial percheziționat,percheziţia informatică a celuilalt sistem informatic ori suport de stocare a datelor informatice se poate efectua în baza ordonanţei motivate a procurorului, fără autorizaţia judecătorului de instrucţie, urmînd ca acestuia să i se prezinte imediat, dar nu mai tîrziu de 24 de ore de la terminarea percheziţiei informatice, datele informatice obţinute în urma acesteia, indicîndu-se motivele efectuării ei. Judecătorul de instrucţie verifică legalitatea acestei acţiuni procesuale.

(6) În cazul constatării faptului că percheziţia informatică efectuată în condițiile alin. (5) al prezentului articol a fost efectuată legal, judecătorul de instrucţie confirmă rezultatele acesteia printr-o încheiere motivată. În caz contrar, prin încheiere motivată, recunoaşte percheziţia informatică a celuilalt sistem informatic ori suport de stocare a datelor informatice ca fiind ilegală. *Convenția Budapesta art. 19*

Art. III. Codul de procedură penală
Dezbateri publice suplimentare

1. Articolul 130[1]. Percheziţia informatică şi ridicarea obiectelor care conţin date informatice

(continuare)

(7) În cazul în care ridicarea obiectelor care conţin date informatice poate afecta grav furnizarea autorizată a reţelelor sau serviciilor publice de comunicaţii electronice, organul de urmărire penală dispune, prin ordonanţă motivată, efectuarea de copii ale acestor date informatice. În alte cazuri, în care obiectele respective nu sînt utilizate pentru furnizarea autorizată a reţelelor sau serviciilor publice de comunicaţii electronice, însă ridicarea acestora poate afecta grav desfăşurarea activităţii persoanei care le deţine sau le are sub control, organul de urmărire penală poate dispune, prin ordonanţă motivată, efectuarea de copii ale acestor date informatice. Copiile respective servesc ca mijloace de probă și se realizează prin utilizarea metodelor şi mijloacelor tehnice ce asigură integritatea şi autenticitatea datelor informatice.

(8) În cazul în care pentru efectuarea percheziţiei informatice se cere un timp îndelungat, persoana care efectuează urmărirea penală ridică obiectele care conţin datele informatice pentru a le examina la sediul organului de urmărire penală. Pentru aceasta, obiectele care conţin datele informatice se împachetează şi se sigilează, iar pachetul se semnează, făcîndu-se menţiunea respectivă în procesul-verbal.

(9) Suplimentar celor prevăzute la art. 260, procesul-verbal cu privire la percheziţia informatică trebuie să cuprindă date cu privire la:

a) descrierea și enumerarea sistemelor informatice ori suporturilor de stocare a datelor informatice față de care s-a dispus percheziția informatică;

b) descrierea și enumerarea activităților desfășurate;

c) descrierea și enumerarea datelor informatice descoperite în cadrul percheziției informatice;

(10) În cazul în care procurorul dispune încetarea urmăririi penale sau în cazul soluţionării cauzei în fond, copiile datelor informatice ce nu prezintă nici o valoare vor fi distruse.

(11) Percheziţia informatică şi ridicarea obiectelor care conţin date informatice se efectuează conform prevederilor prezentului cod.

Art. III. Codul de procedură penală

Articolul 132^6. Cercetarea domiciliului şi/sau instalarea în el a aparatelor ce asigură supravegherea şi înregistrarea audio şi video, a celor de fotografiat şi de filmat
Articolul 132^7. Supravegherea domiciliului prin utilizarea mijloacelor tehnice ce asigură înregistrarea
Articolul 133. Reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale
Articolul 134^3. Documentarea cu ajutorul metodelor şi mijloacelor tehnice, localizarea sau urmărirea prin sistemul de poziţionare globală (GPS) ori prin alte mijloace tehnice
Articolul 134^4. Colectarea informaţiei de la furnizorii de servicii de comunicaţii electronice
Articolul 134^5. Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicaţii electronice ori al unui punct de acces la un sistem informatic
Articolul 134^6. Urmărirea vizuală
Articolul 136. Investigaţia sub acoperire
Articolul 138^1. Supravegherea transfrontalieră
Articolul 138^2. Livrarea controlată
Articolul 138^3. Achiziţia de control

2,3.
( ) Măsura specială de investigaţii prevăzută de prezentul articol poate fi dispusă în cazul infracţiunilor prevăzute la articolul 132^1 alineatul (2) punctul 2) din prezentul cod sau al unei infracţiuni prevăzute la art. 174-175^1, 185^1-185^2, 208^1, 208^2, 237 şi 260-260^2, 260^4, 260^6 şi 261^1 din Codul penal.

Art. III. Codul de procedură penală

4. **Articolul 132/2. Măsurile speciale de investigaţii**

(1) În vederea descoperirii şi cercetării infracţiunilor se efectuează următoarele măsuri speciale de investigaţii:

1) cu autorizarea judecătorului de instrucţie:

[...]

c[1]) interceptarea și înregistrarea datelor informatice;

d) reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale şi a comunicărilor electronice;

[...]

5. **Articolul 132/8. Interceptarea şi înregistrarea comunicărilor**

(2) Prevederile alin. (1) se aplică în exclusivitate la cauzele penale care au ca obiect urmărirea penală sau judecarea persoanelor asupra cărora există date sau probe cu privire la săvîrşirea infracţiunilor prevăzute în următoarele articole din Codul penal: [...] art. 174, [...]. Lista componentelor de infracţiuni este exhaustivă şi poate fi modificată doar prin lege.

Art. III. Codul de procedură penală

6. Articolul 132[11]. Interceptarea şi înregistrarea datelor informatice

(1) Interceptarea şi înregistrarea datelor informatice constă în folosirea unor metode și/sau mijloace tehnice prin intermediul cărora are loc colectarea în timp real a datelor referitoare la traficul informatic şi/sau a datelor referitoare la conţinut, asociate comunicaţiilor respective, altele decît cele prevăzute în art. 132[8], transmise prin intermediul unui sistem informatic, şi stocarea informaţiilor obţinute în urma interceptării pe un suport tehnic.

(2) Interceptarea şi înregistrarea datelor informatice se dispune și se efectuează în condițiile prevăzute la art. 132[9], care se aplică în mod corespunzător.

(3) Măsura specială de investigaţii prevăzută de prezentul articol poate fi dispusă în cazul infracţiunilor prevăzute la art. 132[1] alin. (2) pct. 2) din prezentul cod sau al unei infracţiuni prevăzute la art. 175-175[1], 185[1]-185[3], 208[1], 208[2], 237 şi 259-261[1] din Codul penal.

7. Articolul 132[12]. Verificarea înregistrării interceptărilor

Mijloacele de probă obținute în condițiile art.132[8]–132[11] pot fi verificate prin expertiză tehnică, dispusă de către instanţa de judecată la cererea părţilor sau din oficiu.

Convenția Budapesta
Art. 20, 21

Art. III. Codul de procedură penală

8. Articolul 133. Reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale şi a comunicărilor electronice

(1) Dacă există temeiuri rezonabile de a presupune că trimiterile poştale şi/sau comunicările electronice primite sau expediate de către bănuit, învinuit pot conţine informaţii ce ar avea importanţă probatorie în cauza penală pe una sau mai multe infracţiuni grave, deosebit de grave sau excepţional de grave şi dacă prin alte procedee probatorii nu pot fi obţinute probe, organul de urmărire penală este în drept să reţină, să cerceteze, să predea, să percheziţioneze sau să ridice trimiterile poştale ale persoanelor indicate.

[...]

9. **Articolul 134. Examinarea şi ridicarea trimiterilor poştale**

(4) Dispoziţiile alin. (1)-(3) din prezentul articol se aplică în mod corespunzător şi în cazul informaţiilor ce ţin de comunicările electronice."

Art. III. Codul de procedură penală

10. Articolul 134/2. Monitorizarea sau controlul tranzacţiilor financiare şi accesul la informaţia financiară

(2) Monitorizarea sau controlul tranzacţiilor financiare şi accesul la informaţia financiară se dispun în cazul urmăririi penale pornite pe infracţiunile prevăzute la art. [...] 175[1], 185[1]-185[2], 208-208[2] [...], 259-261[1] din Codul penal.

11. Articolul 134/5. Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicaţii electronice ori al unui punct de acces la un sistem informatic

(1) Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicaţii electronice ori al unui punct de acces la un sistem informatic constă în solicitarea de la un furnizor de servicii electronice de a identifica abonatul, proprietarul sau utilizatorul unui sistem de telecomunicaţii, al unui mijloc de ~~telecomunicaţii~~ comunicaţii electronice ori al unui punct de acces la un sistem informatic sau de a comunica dacă un anumit mijloc de comunicaţii sau punct de acces la un sistem informatic este folosit sau este activ ori a fost folosit sau a fost activ la o anumită dată.

Art. III. Codul de procedură penală

12. Articolul 305. Modul de examinare a demersurilor referitoare la efectuarea acţiunilor de urmărire penală, măsurilor speciale de investigaţii sau la aplicarea măsurilor procesuale de constrîngere

(3) Demersul referitor la cercetarea domiciliului şi/sau instalarea în el a aparatelor ce asigură supravegherea şi înregistrarea audio şi video, a celor de fotografiat şi de filmat, referitor la supravegherea domiciliului prin utilizarea mijloacelor tehnice, la interceptarea şi înregistrarea comunicărilor, la interceptarea şi înregistrarea datelor informatice, la monitorizarea conexiunilor comunicaţiilor telegrafice şi electronice şi referitor la monitorizarea sau controlul tranzacţiilor financiare şi accesul la informaţia financiară se examinează de judecătorul de instrucţie imediat, dar nu mai tîrziu de 4 ore de la primirea demersului.

Art. III. Codul de procedură penală
Dezbateri publice suplimentare

Articolul 126. Temeiurile pentru ridicarea de obiecte sau documente

[...]

(2) Ridicarea de documente ce conţin informaţii care constituie secret de stat, comercial, bancar, precum şi ridicarea informaţiei privind convorbirile telefonice, alte comunicări electronice și traficul informatic se fac numai cu autorizaţia judecătorului de instrucţie.

Art. IV. Legea nr. 264/2005
cu privire la exercitarea profesiunii de medic

Articolul 17. Obligaţiile profesionale ale medicului

(1) Medicul este obligat:

[...]

e[1]) să transmită în adresa organelor de drept orice informaţii, care i-au devenit cunoscute în timpul exercitării atribuţiilor de serviciu, cu privire la cazurile de abuz, violenţă, inclusiv sexuală, faţă de copil;

Art. V. Legea comunicaţiilor electronice nr. 241/2007

Articolul 20

(3) Furnizorii de reţele şi/sau servicii de comunicaţii electronice, indiferent de tipul de proprietate, sînt obligaţi:

a) să prezinte, în condiţiile legii, organelor împuternicite care exercită activitatea ~~operativă~~ specială de investigaţii informaţii despre utilizatori şi despre serviciile publice de comunicaţii electronice furnizate acestora;

b) să permită, din punct de vedere tehnic, organelor împuternicite să efectueze, în condiţiile legii, măsurile ~~operative~~ speciale de investigaţii pe reţelele de comunicaţii electronice şi să prezinte în acest scop datele tehnice necesare;

Art. VI. Codul contravenţional

1. Articolul 90. Producerea, comercializarea, difuzarea sau păstrarea produselor pornografice

Producerea, comercializarea, difuzarea sau păstrarea produselor pornografice pentru a fi comercializate ori difuzate, sau accesarea acestora cu bună ştiinţă în locuri publice

se sancţionează cu amendă de la 24 la 30 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei juridice.

Art. VI. Codul contravenţional

2. Articolul 247/1. Încălcarea legislaţiei cu privire la prevenirea şi combaterea criminalităţii informatice

Încălcarea legislaţiei cu privire la prevenirea şi combaterea criminalităţii informatice de către furnizorii de servicii de comunicaţii electronice, indiferent de tipul de proprietate şi forma juridică de organizare, manifestată prin:

a) neîndeplinirea obligaţiei de ţinere a evidenţei utilizatorilor de servicii;

b) necomunicarea către autorităţile competente despre accesul ilegal la informaţia din sistemul informatic, despre tentativele de introducere a unor programe ilegale, despre încălcarea de către persoane responsabile a regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei ori a regulilor de protecţie a sistemului informatic prevăzute în conformitate cu statutul informaţiei sau cu gradul ei de protecţie, dacă acestea au contribuit la însuşirea, la denaturarea sau la distrugerea informaţiei ori au provocat alte urmări grave, perturbarea funcţionării sistemelor informatice, alte incidente de securitate informatică cu impact semnificativ;

c) neexecutarea, în condiţii de confidenţialitate, a solicitării autorităţii competente privind conservarea rapidă a datelor informatice ori a datelor referitoare la traficul informatic, indicate în solicitarea respectivă, faţă de care există pericolul distrugerii ori alterării, în condiţiile stabilite de lege;

d) neprezentarea către autorităţile competente, în temeiul unei solicitări efectuate în condiţiile legislației procesuale, a datelor referitoare la traficul informatic sau utilizatori;

...

Art. VI. Codul contravenţional
Dezbateri publice suplimentare

2. Articolul 247/1. Încălcarea legislaţiei cu privire la prevenirea şi combaterea criminalităţii informatice

(continuare)

e) neîndeplinirea măsurilor de securitate prin utilizarea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora să fie restricţionat sau interzis accesul la propriul sistem informatic al utilizatorilor fără asemenea drept;

f) neasigurarea păstrării datelor referitoare la trafic, în condiţiile stabilite de lege, pentru identificarea furnizorilor de servicii, utilizatorilor de servicii şi a canalului prin al cărui intermediu comunicaţia a fost transmisă;

g) neîndeplinirea obligaţiei de sistare, folosind metodele şi mijloacele tehnice din posesie, în condiţiile stabilite de lege, a accesului ~~la toate adresele IP pe care sînt amplasate pagini web~~ din propriul sistem informatic la paginile web, inclusiv cele găzduite de furnizorul respectiv, ce conţin pornografie infantilă, promovează abuzul sexual sau exploatarea sexuală a copiilor, conţin informaţii ce fac propaganda războiului sau terorismului, îndeamnă la ură sau discriminare naţională, rasială ori religioasă, la ostilitate sau violenţă, ~~conțin sau difuzează instrucțiuni privind modul de comitere a infracțiunilor~~,

se sancţionează cu amendă de la 100 la 150 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 400 la 500 de unităţi convenţionale aplicată persoanei juridice.

Art. VI. Codul contravenţional

3. Articolul 252 se exclude

Articolul 252. Conectarea neautorizată sau admiterea conectării neautorizate la reţelele de comunicaţii electronice

Conectarea neautorizată sau admiterea conectării neautorizate a echipamentelor terminale sau a altor mijloace de comunicaţii electronice la reţelele de comunicaţii electronice, inclusiv la liniile de abonat,

[...]

4. Articolul 400. Ministerul Afacerilor Interne

(1) Contravenţiile prevăzute la art. [...] , 247^1 [...] se examinează de poliţie.

Art. VII. Legea nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice

1. Articolul 2 se completează cu următoarele noţiuni:

infrastructură critică – un element sau un sistem, aflat pe teritoriul statului, care este esenţial pentru menţinerea funcţiilor de asigurare a sănătăţii, securităţii, bunăstării sociale, economice sau de altă natură a populaţiei şi a cărui perturbare sau distrugere poate avea un impact negativ, ca urmare a incapacităţii de a menţine respectivele funcţii;

proprietar/operator/administrator de infrastructură critică – orice entitate stabilită de Guvern ca fiind deţinător al un element sau al unui sistem care face parte din infrastructura critică ori este investit cu funcţii de operare/administrare a acestuia;

conservarea datelor – păstrarea şi protejarea integrităţii datelor existente într-un sistem informatic, aflate în posesia sau sub controlul persoanei;

securitatea informatică – starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri prin care se asigură confidenţialitatea, integritatea, disponibilitatea şi autenticitatea datelor informatice, a resurselor şi serviciilor publice sau private, inclusiv prin prevenirea şi combaterea criminalităţii informatice;

incident de securitate informatică – o perturbare a securităţii informatice care are sau poate avea un impact negativ asupra menţinerii confidenţialităţii, integrităţii, disponibilităţii şi autenticităţii informaţiilor în format electronic, a resurselor ori serviciilor publice sau private;

criminalitatea informatică – fenomen social negativ caracterizat printr-un ansamblu de activităţi infracţionale în care datele informatice şi/sau sistemele informatice constituie instrument de comitere a infracţiunilor sau obiect al infracţiunilor.”

Art. VII. Legea nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice

2. Articolul 4 va avea următorul cuprins:

Articolul 4. Atribuţiile organelor de drept în domeniul prevenirii şi combaterii criminalităţii informatice

(1) În cadrul Procuraturii Generale, Inspectoratului General al Poliției al Ministerului Afacerilor Interne și Serviciului de Informații și Securitate activează subdiviziuni specializate, ale căror atribuții includ prevenirea și combaterea criminalităţii informatice şi care colaborează în vederea realizării atribuțiilor date.

(2) Inspectoratul General al Poliției desfăşoară activitatea de prevenire şi combatere a criminalităţii informatice, în conformitate cu legislaţia în vigoare, inclusiv prin efectuarea activităţii speciale de investigaţii şi desfăşurarea urmăririi penale pe cauzele privind criminalitatea informatică, dispunerea conservării rapide a datelor informatice ori a datelor referitoare la traficul informatic, desemnarea punctului de contact responsabil să asigure cooperarea internaţională în domeniul combaterii criminalităţii informatice, prin realizarea cooperării internaţionale, analiza tendinţelor criminalităţii informatice, identificarea şi protecţia victimelor criminalităţii informatice.

(3) Inspectoratul General al Poliției şi Serviciul de Informaţii şi Securitate, cu participarea altor autorităţi publice şi instituţii private, elaborează, administrează şi actualizează, prin intermediul unui sistem informaţional automatizat, baze de date privind fenomenul criminalităţii informatice.

(4) Inspectoratul General al Poliției, în comun cu Procuratura Generală, efectuează studii în vederea depistării şi înlăturării cauzelor şi condiţiilor ce favorizează criminalitatea informatică, iar rezultatele acestora le publică prin intermediul mijloacelor de informare în masă.

...

Art. VII. Legea nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice

2. Articolul 4 va avea următorul cuprins:

Articolul 4. Atribuţiile organelor de drept în domeniul prevenirii şi combaterii criminalităţii informatice

(continuare)

(5) Procuratura Generală:

a) desfăşoară, în limitele competenţei, activităţi de prevenire şi combatere a crimelor informatice, în conformitate cu legislaţia în vigoare;

b) coordonează, conduce şi exercită urmărirea penală pe cauzele privind criminalitatea informatică;

c) reprezintă în instanţa de judecată învinuirea în numele statului;

d) primeşte şi transmite cererile de asistenţă juridică internaţională, de extrădare sau de arestare provizorie, formulate în faza de urmărire penală;

e) dispune, în cadrul desfăşurării urmăririi penale, la solicitarea organului de urmărire penală sau din oficiu, conservarea rapidă a datelor informatice ori a datelor referitoare la traficul informatic, faţă de care există pericolul distrugerii ori alterării, în condiţiile legislaţiei de procedură penală;

f) întreprinde alte măsuri orientate spre prevenirea şi combaterea criminalităţii informatice.

(6) Serviciul de Informaţii şi Securitate desfăşoară activităţi de prevenire şi combatere a criminalităţii informatice ce prezintă ameninţări la adresa securităţii naţionale, inclusiv prin efectuarea activităţii speciale de investigaţii, relevarea activităţii grupurilor şi organizaţiilor criminale internaţionale, alte activităţi în limitele competenţei sale.

(7) Institutul Naţional al Justiţiei realizează perfecţionarea profesională a personalului antrenat în înfăptuirea justiţiei în domeniul combaterii criminalităţii informatice.”

Art. VII. Legea nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice

3. Articolul 4/1. Planul naţional de prevenire şi combatere a criminalităţii informatice

(1) În scopul prevenirii şi combaterii criminalităţii informatice, precum şi asigurării protecţiei victimelor acesteia, Guvernul aprobă Planul naţional de prevenire şi combatere a criminalităţii informatice (în continuare – Plan naţional), elaborat cu avizul Procuraturii Generale.

(2) Planul naţional se aprobă periodic pentru un termen de 3 ani şi prevede implementarea unor acţiuni complexe, realizarea de iniţiative social-economice, orientate spre prevenirea şi combaterea criminalităţii informatice, precum şi spre protecţia victimelor acesteia, inclusiv prin cooperare cu organizaţii internaţionale, organizaţii neguvernamentale, alte instituţii şi reprezentanţi ai societăţii civile.

(3) Autorităţile administraţiei publice centrale cu atribuţii în domeniul prevenirii şi combaterii crimelor informatice adoptă planuri de acţiuni proprii pentru realizarea Planului naţional în domeniile lor de activitate.

4. Articolul 5 se completează cu alineatul (2) cu următorul cuprins:

(2) Furnizorii de servicii, organizaţiile neguvernamentale, reprezentanţii societăţii civile şi orice altă persoană sînt încurajaţi să transmită în adresa Inspectoratului General al Poliţiei şi Procuraturii Generale orice informaţii, ce le devin cunoscute, cu privire la persoane fizice şi/sau juridice care distribuie, difuzează, importă sau exportă imagini sau alte reprezentări ale unui sau mai mulţi copii implicaţi în activităţi sexuale, precum şi cu privire la abuzuri sexuale comise faţă de un copil prin utilizarea comunicaţiilor electronice.

Art. VII. Legea nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice

Dezbateri publice suplimentare

5. Articolul 6[1]. Obligaţiile proprietarilor şi operatorilor de infrastructuri critice informatice

(1) Pentru prevenirea criminalităţii informatice, proprietarii şi operatorii de infrastructuri critice informatice sînt obligaţi:

a) să implementeze cerinţele minime, stabilite de autoritatea de stat responsabilă, privind asigurarea securităţii infrastructurii critice informatice deţinute sau operate;

b) să creeze punctul de contact pentru realizarea interacţiunii cu autorităţile publice şi instituţiile statului, abilitate cu asigurarea securităţii infrastructurilor critice informatice;

c) să coopereze cu autorităţile competente în procesul de asigurare a securităţii infrastructurii critice informatice deţinute sau operate;

d) să comunice autorităţilor competente imediat, dar nu mai tîrziu de ~~24~~ 72 de ore de la momentul depistării, informaţiile despre accesul ilegal la datele din propriul sistem informatic, despre tentativele de introducere a unor programe ilegale, despre încălcarea de către persoane responsabile a regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei ori a regulilor de protecţie a sistemului informatic prevăzute în conformitate cu statutul informaţiei sau cu gradul ei de protecţie, dacă acestea au contribuit la însuşirea, denaturarea sau distrugerea informaţiei ori au provocat alte urmări grave, perturbarea funcţionării sistemelor informatice, alte incidente de securitate informatică cu impact semnificativ.

(2) Autorităţile competente, responsabile de recepţionarea şi prelucrarea informaţiilor, comunicate de proprietarii şi operatorii de infrastructuri critice informatice, sunt stabilite prin hotărîre de Guvern.

Art. VII. Legea nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice

6. Articolul 7. Obligaţiile furnizorilor de servicii

(1) Furnizorii de servicii sînt obligaţi:

a) să ţină evidenţa utilizatorilor de servicii, iar în cazul serviciilor anonime preplătite – data și ora primei activări a serviciului;

b) să comunice autorităţilor competente ~~datele despre traficul informatic, inclusiv~~, prevăzute la art. 4 alin. (1), datele despre accesul ilegal la informaţia din sistemul informatic, despre tentativele de introducere a unor programe ilegale, despre încălcarea de către persoane responsabile a regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei ori a regulilor de protecţie a sistemului informatic prevăzute în conformitate cu statutul informaţiei sau cu gradul ei de protecţie, dacă acestea au contribuit la însuşirea, la denaturarea sau la distrugerea informaţiei ori au provocat alte urmări grave, perturbarea funcţionării sistemelor informatice, alte ~~delicte informatice~~ incidente de securitate informatică cu impact semnificativ;

c) să execute, în condiţii de confidenţialitate, solicitarea autorităţii competente privind conservarea ~~imediată~~ rapidă a datelor informatice ori a datelor referitoare la traficul informatic, indicate în solicitarea respectivă, faţă de care există pericolul distrugerii ori alterării, pe un termen de pînă la ~~120 de zile calendaristice~~ 180 de zile calendaristice, în condiţiile legislaţiei naţionale;

d) să prezinte autorităţilor competente, în temeiul unei solicitări efectuate în condiţiile ~~legii~~ legislației procesuale, date referitoare la traficul informatic și la utilizatori, inclusiv la tipul de comunicaţie şi la serviciul de care a beneficiat utilizatorul, la modalitatea de plată a serviciului;

e) să întreprindă măsuri de securitate prin utilizarea unor proceduri, dispozitive sau programe informatice specializate cu al căror ajutor accesul la ~~un~~ propriul sistem informatic să fie restricţionat sau interzis utilizatorilor ~~neautorizaţi~~ fără asemenea drept;

f) să asigure ~~monitorizarea, supravegherea şi~~ păstrarea datelor referitoare la trafic~~, pe o perioadă de 180 de zile calendaristice~~ în rețeaua de telefonie fixă și de telefonie mobilă pe o perioadă de un an, iar a celor referitoare la trafic în Internet și telefonie prin Internet – pe o perioadă de 6 luni, pentru identificarea furnizorilor de servicii, utilizatorilor de servicii şi a canalului prin al cărui intermediu comunicaţia a fost transmisă; ...

Art. VII. Legea nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice

Dezbateri publice suplimentare

6. Articolul 7. Obligaţiile furnizorilor de servicii

(1) Furnizorii de servicii sînt obligaţi:

(continuare)

g) să asigure descifrarea datelor informatice care se conţin în pachetele protocoalelor de reţea, cu excepția datelor referitoare la conținut, în baza solicitării autorităţii competente prevăzute la art. 4 alin. (1), în limita capacităţilor sale tehnice, cu conservarea acestor date pe o perioadă de 90 de zile calendaristice.

h) să sisteze, folosind metodele şi mijloacele tehnice din posesie, accesul din propriul sistem informatic ~~la toate adresele IP pe care sînt amplasate pagini web~~ la paginile web, inclusiv cele găzduite de furnizorul respectiv, ce conţin pornografie infantilă, promovează abuzul sexual sau exploatarea sexuală a copiilor, conţin informaţii ce fac propaganda războiului sau terorismului, îndeamnă la ură sau discriminare naţională, rasială ori religioasă, la ostilitate sau violenţă~~, conţin sau difuzează instrucţiuni privind modul de comitere a infracţiunilor~~;

(2) În cazul în care datele referitoare la traficul informatic se află în posesia mai multor furnizori de servicii, furnizorul de servicii solicitat este obligat să pună ~~de îndată~~ în termen rezonabil la dispoziţia autorităţii competente informaţia necesară identificării celorlalţi furnizori de servicii.

Se completează cu alin. (3):

(3) Sistarea accesului la paginile web, prevăzute la alin. (1) lit. h) din prezentul articol, se dispune de instanță în cadrul cauzelor penale, în cazul în care furnizorul de servicii nu a eliminat din paginile web găzduite sau aflate sub controlul său informația respectivă la solicitarea organelor de drept sau dacă stabilirea datelor de contact ale acestui furnizor de servicii nu a fost posibilă. Sistarea accesului la paginile web ce conţin pornografie infantilă, promovează abuzul sexual sau exploatarea sexuală a copiilor, ce nu sunt găzduite de furnizorul respectiv, se dispune de organele de drept conform Listei elaborate de Organizația Internațională a Poliției Criminale (INTERPOL "Worst of"-list), pusă la dispoziția furnizorului de servicii.

Codul penal

Art. 140 CP Propaganda războiului
(1) Propaganda războiului, răspîndirea de informaţii tendenţioase ori inventate, instigatoare la război sau orice alte acţiuni orientate spre declanşarea unui război, săvîrşite verbal, în scris, prin intermediul radioului, televiziunii, cinematografului sau prin alte mijloace.

Art. 279/2 CP. Instigarea în scop terorist sau justificarea publică a terorismului
(1) Instigarea în scop terorist, adică distribuirea sau punerea în alt mod la dispoziţia publicului a unui mesaj cu intenţia de a instiga sau cunoscînd că un astfel de mesaj poate instiga la comiterea unei infracţiuni cu caracter terorist.
(2) Justificarea publică a terorismului, adică distribuirea sau punerea în alt mod la dispoziţia publicului a unui mesaj despre recunoaşterea unei ideologii sau practici de comitere a infracţiunilor cu caracter terorist ca fiind justă, care necesită a fi susţinută sau este demnă de urmat,

Art. 176 CP Încălcarea egalităţii în drepturi a cetăţenilor
(1) Orice deosebire, excludere, restricţie sau preferinţă în drepturi şi în libertăţi a persoanei sau a unui grup de persoane, orice susţinere a comportamentului discriminatoriu în sfera politică, economică, socială, culturală şi în alte sfere ale vieţii, bazată pe criteriu de rasă, naţionalitate, origine etnică, limbă, religie sau convingeri, sex, vîrstă, dizabilitate, opinie, apartenenţă politică sau pe orice alt criteriu.

În conformitate cu prevederile generale ale CPP, orice hotărîre a instanței de judecată poate fi atacată în instanța ierarhic superioară.

Pactul internaţional cu privire la drepturile civile şi politice din 16 decembrie 1966, ratificat la 26.01.1993
Articolul 20
1. Orice propagandă în favoarea războiului este interzisă prin lege.
2. Orice îndemn la ură naţională, rasială sau religioasă care constituie o incitare la discriminare, la ostilitate sau la violenţă este interzisă prin lege.

Art. VII. Legea nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice

7. Articolul 10. Solicitările autorităţilor competente străine

(1) În cadrul cooperării internaţionale, autoritatea competentă străină poate solicita autorităţii competente din Republica Moldova conservarea ~~imediată~~ rapidă a datelor informatice sau a datelor privind traficul informatic, existente într-un sistem informatic de pe teritoriul Republicii Moldova, referitor la care autoritatea competentă străină urmează să formuleze o cerere, argumentată, de asistenţă juridică internaţională în materie penală.

(2) Cererea de conservare ~~imediată~~ rapidă prevăzută la alin.(l) cuprinde:

[...]

se completează cu alineatul (5) cu următorul cuprins:

(5) În cazul în care, în timpul executării unei solicitări de conservare a datelor referitoare la trafic, autoritatea competentă din Republica Moldova descoperă că un furnizor de servicii a participat într-un alt stat la transmiterea acestei comunicări, aceasta va dezvălui rapid autorităţii competente străine solicitante o cantitate suficientă de date referitoare la trafic, pentru identificarea acestui furnizor de servicii şi a canalului prin care comunicarea a fost transmisă.

Convenția Budapesta
Art. 30

Art. VIII. Legea nr. 59/2012 privind activitatea specială de investigaţii

Articolul 18. Măsurile speciale de investigaţii

(1) Pentru realizarea sarcinilor prevăzute de prezenta lege pot fi efectuate următoarele măsuri speciale de investigaţii:

1) cu autorizarea judecătorul de instrucţie, la demersul procurorului:

[...]

c[1]) interceptarea și înregistrarea datelor informatice;

d) reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale și/sau comunicărilor electronice;

Vă mulțumim pentru atenție!

Centrul pentru Combaterea Crimelor Informatice
MD-2004, Chişinău, str. Bucuriei, 14
Tel: (022) 57-72-65
e-mail: ccci@mai.gov.md