

LEGE
pentru modificarea unor acte normative
(prevenirea și combaterea atacurilor împotriva sistemelor informatice)

Parlamentul adoptă prezenta lege organică

Prezenta lege transpune:

art. 2 lit. (a) și (b); art. 3 – 5; art. 7; art. 9 alin. (2), (3) și (4) litera (a) și (c) din Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului, nr. CELEX: 32013L0040, publicată în Jurnalul Oficial al Uniunii Europene L218/8 din 14 august 2013.

Art. I. – Codul penal al Republicii Moldova nr. 985/2002 (republicat în Monitorul Oficial al Republicii Moldova, 2009, nr. 72–74, art. 195), cu modificările ulterioare, se modifică după cum urmează:

1. Articolul 134²⁵ va avea următorul cuprins:

„**Articolul 134²⁵. Sistem informatic**

Prin sistem informatic se înțelege orice dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în legătură care asigură ori dintre care unul sau mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor informatice, inclusiv a datelor informatice stocate, prelucrate, recuperate sau transmise de acest dispozitiv sau ansamblu de dispozitive în vederea exploatării, a utilizării, a protecției și a întreținerii lor.”.

2. Se completează cu articolul 134²⁷ cu următorul cuprins:

„**Articolul 134²⁸. Date informatice**

Prin date informatice se înțelege datele definite astfel în Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice.”

3. La articolul 259:

la alineatului (1):

după textul „Accesarea ilegală” se completează cu textul „, în întregime sau în parte, prin violarea măsurilor de securitate,”;

textul „până la 1 an” se substituie cu textul „până la 2 ani”;

la alineatul (2), litera a) se abrogă.

4. La articolul 260:

dispoziția va avea următorul cuprins:

„Producerea, vânzarea, procurarea, importul, distribuirea sau punerea în alt mod la dispoziție, în mod ilegal, a unui mijloc tehnic sau program de calculator, conceput sau adaptat în principal în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 237, 259, 260¹–260³, 260⁵–260⁷,”;

cuvântul „întreprinderii” se substituie cu cuvântul „persoanei juridice”.

5. La articolul 260¹:

cuvântul „întreprinderii” se substituie cu cuvântul „persoanei juridice”.

6. La articolul 260²:

alineatul (1) va avea următorul cuprins:

„(1) Ștergerea, periclitarea, deteriorarea, modificarea, eliminarea datelor informatice dintr-un sistem informatic sau împiedicarea accesului la aceste date, cu intenție și fără drept, precum și transferul neautorizat de date informatice dintr-un sistem informatic, dintr-un mijloc de stocare, dobândirea, comercializarea sau punerea la dispoziție, sub orice formă, a datelor informatice cu acces limitat

se pedepsesc cu amendă în mărime de la 850 la 1350 unități convenționale sau cu închisoare de la 2 la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 2000 la 4000 unități convenționale cu privarea de dreptul de a exercita o anumită activitate.”;

la alineatul (2):

se completează cu litera c) cu următorul cuprins:

„c) săvârșite prin utilizarea unui program de calculator, a unei parole de calculator, a unui cod de acces sau a altor date de acces la un sistem informatic sau la o parte a acestuia, dacă aceste date au fost concepute sau adaptate în scopul afectării a două sau mai multor sisteme informatice;

după textul „cu închisoare de la 3 la 7 ani”, se completează cu textul „, , cu amendă, aplicată persoanei juridice, în mărime de la 4000 la 7000 unități convenționale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea persoanei juridice”.

la alineatul (3):

se completează cu litera c) cu următorul cuprins:

„c) săvârșite împotriva unui sistem informatic din infrastructura critică,”;

după textul „cu închisoare de la 5 la 10 ani”, se completează cu textul „, , iar persoana juridică se pedepsește cu amendă de la 10000 la 30000 de unități convenționale cu lichidarea persoanei juridice”.

7. La articolul 260³:

dispoziția alineatului (1) va avea următorul cuprins:

„(1) Perturbarea sau întreruperea funcționării unui sistem informatic prin introducerea, transmiterea, periclitarea, ștergerea, deteriorarea, modificarea, eliminarea datelor informatice sau împiedicarea accesului la aceste, cu intenție și fără drept ,”;

alineatul (2):

litera c) va avea următorul cuprins:

„c) săvârșite prin utilizarea unui program de calculator, a unei parole de calculator, a unui cod de acces sau a altor date de acces la un sistem informatic sau la o parte a unui sistem informatic, dacă aceste date au fost concepute sau adaptate în scopul afectării a două sau mai multor sisteme informatice;”.

dispoziția alineatului (3) va avea următorul cuprins:

(3) Acțiunile prevăzute la alin. (1) sau (2):

a) săvârșite de un grup criminal organizat sau de o organizație criminală;

b) care au cauzat daune în proporții deosebit de mari;

c) săvârșite împotriva unui sistem informatic din infrastructura critică”.

8. La articolul 260⁴, dispoziția din alineatul (1) va avea următorul cuprins:

„Producerea, vânzarea, procurarea, importul, distribuirea sau punerea în alt mod la dispoziție, în mod ilegal, a unei parole de calculator, a unui cod de acces sau a unor date similare, prin care un întreg sistem informatic sau orice parte a acestuia poate fi accesat, în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 237, 259, 260¹–260³, 260⁵ sau 260⁶,”.

Art. II. – Codul contravențional al Republicii Moldova nr. 218/2008 (republicat în Monitorul Oficial al Republicii Moldova, 2017, nr. 78–84, art. 100), cu modificările ulterioare, se completează cu articolul 250³ cu următorul cuprins:

„Articolul 250³. Accesul ilegal la un sistem informatic

Accesarea ilegală, în întregime sau în parte, a unui sistem informatic de către o persoană care nu este autorizată în temeiul legii sau al unui contract, care depășește limitele autorizării ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfășoare cercetări științifice sau să efectueze orice altă operațiune într-un sistem informatic, dacă fapta nu constituie infracțiune,

se sancționează cu amendă de la 50 la 80 de unități convenționale aplicată persoanei fizice, cu amendă de la 120 la 240 de unități convenționale aplicată persoanei juridice.”

Art. IV. – Prezenta lege intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

PREȘEDINTELE PARLAMENTULUI

NOTA DE FUNDAMENTARE

la proiectul legii pentru modificarea și completarea unor acte normative (prevenirea și combaterea atacurilor împotriva sistemelor informatice)

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ

Proiectul legii pentru modificarea și completarea unor acte normative (prevenirea și combaterea atacurilor împotriva sistemelor informatice) a fost elaborat de Ministerul Justiției.

2. Condițiile ce au impus elaborarea proiectului actului normativ

2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ

Proiectul a fost elaborat în temeiul angajamentelor asumate de Republica Moldova în calitate de stat candidat pentru aderare la Uniunea Europeană (*în continuare – UE*) privind transpunerea legislației europene relevante. În acest sens, Foaia de parcurs privind „Statul de drept” (criteriu de referință în procesul de aderare a Republicii Moldova la Uniunea Europeană) (*în continuare – Foaie de parcurs*) este un document strategic elaborat în contextul cadrului de negocieri pentru aderarea Republicii Moldova la Uniunea Europeană. Acest document stabilește rezultatele strategice pe care Republica Moldova își propune să le obțină în următorii ani în vederea consolidării statului de drept ca piatră de temelie a dezvoltării democratice a țării.

La concret, în Foaia de parcurs, în Capitolul I „Combaterea criminalității organizate”, pct. 5.4 prevede ca măsură „adoptarea cadrului normativ de aliniere la Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului”.

2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative

Locul infracțiunilor informatice în peisajul juridic penal al Republicii Moldova a devenit în scurt timp la fel de important ca acela al infracțiunilor „clasice”, gravitatea acestora fiind accentuată de ușurința comiterii și camuflării lor, de caracterul preponderent transfrontalier datorat mediului Internet și de potențialul devastator al efectelor acestor fapte. Atacurile informatice pot eroda stabilitatea și reziliența societății, exercitând presiune strategică fără a recurge la violență fizică. În acest context, este vitală asigurarea unei protecții eficiente a securității cibernetice prin prisma măsurilor de drept penal, cu aplicarea unor sancțiuni eficace, proporționale și disuasive. Din această perspectivă, prezența în partea specială a Codului penal al Republicii Moldova a Capitolul XI „Infracțiuni informatice și infracțiuni în domeniul comunicațiilor electronice” este pe deplin justificată.

În cadrul acestui capitol, art. 259 – 260⁴ prezintă anumite similitudini cu art. 3 – 7 din Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12

august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (în continuare – Directivă). Totuși, există și anumite neconcordanțe care au ca efect reducerea eficienței procesului de prevenire și combatere în Republica Moldova a infracțiunilor informatice. Dat fiind caracterul transnațional, care nu ține seama de frontiere, al sistemelor informatice moderne, atacurile împotriva acestor sisteme sunt de natură transfrontalieră, subliniind nevoia urgentă de a se face în continuare demersuri pentru armonizarea legislațiilor penale în acest domeniu.

3. Obiectivele urmărite și soluțiile propuse

Obiectivul general al proiectului este de a consolida spațiul de libertate, securitate și justiție, în conformitate cu cele mai înalte standarde ale UE referitoare la Capitolul 24 din Programul Național de Aderare (2025 – 2029) al Republicii Moldova la UE.

Urmare a promovării prezentului proiect vor fi atinse următoarele obiective specifice:

- alinierea cadrului normativ penal din Republica Moldova (art. 134²⁵, 259 – 260⁴ din Codul penal al Republicii Moldova) la prevederile Directivei;
- consolidarea compatibilității cadrului normativ penal cu prevederile unor acte normative extrapenale de referință: Legea Republicii Moldova nr. 20 din 03.02.2009 privind prevenirea și combaterea criminalității informatice; Hotărârea Guvernului Republicii Moldova nr. 701 din 11.07.2018 pentru aprobarea Regulamentului privind protecția antiteroristă a infrastructurii critice;
- ajustarea art. 134²⁵, 259–260⁴ din Codul penal al Republicii Moldova la noile provocări sociale într-o conjunctură de instabilitate globală crescândă.

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Completarea CP cu art. 134²⁸:

Sintagma „date informatice” este folosită în următoarele articole din Codul penal al Republicii Moldova (în continuare – CP):

- art. 260 („Producerea, importul, comercializarea sau punerea ilegală la dispoziție a mijloacelor tehnice sau produselor program”) care este similar cu art. 7 lit. (b) al Directivei;
- art. 260¹ („Interceptarea ilegală a unei transmisii de date informatice”) care este similar cu art. 6 al Directivei;
- art. 260² („Alterarea integrității datelor informatice ținute într-un sistem informatic”) care este similar cu art. 5 al Directivei;
- art. 260³ („Perturbarea funcționării sistemului informatic”) care este similar cu art. 4 al Directivei.

Cu toate acestea, în CP lipsește o definiție de genul celei din art. 2 lit. b) al Directivei. Ceea ce afectează negativ claritatea și previzibilitatea art. 260 – 260³ din CP. Astfel, se impune completarea CP cu art. 134²⁸ în care noțiunea de „date informatice” ar fi definită în acord cu paradigma din art. 2 lit. b) al Directivei.

Modificarea art. 259 din CP și completarea Codului contravențional cu art. 250³:

În art. 259 din *CP*– „Accesul ilegal la un sistem informatic” – încălcarea măsurilor de securitate apare nu în calitate de condiție obligatorie a infracțiunii, ci doar ca circumstanță agravantă („cu violarea sistemelor de protecție” prevăzută la alin. (2) lit. a)). Aceasta deși art. 3 din *Directivă* impune expres ca aceasta să fie o condiție obligatorie, cu excepția cazurilor considerate minore. Prin urmare, componenta de bază prevăzută la art. 259 alin. (1) se completează cu semnul obligator „prin violarea măsurilor de securitate”, astfel încât acesta să devină condiție obligatorie a infracțiunii. Iar circumstanța agravantă de la alin. (2) va fi exclusă.

Totodată, *Codul contravențional* (în continuare – *CC*) se completează cu un articolul 250³ în să se prevadă răspunderea pentru „cazul minor”, adică pentru accesul ilegal la un sistem informatic, dacă fapta nu constituie infracțiune (și anume – dacă fapta nu implică încălcarea măsurilor de securitate). În acest mod, normele date vor transpune fidel art. 3 din *Directivă*. Cazurile „minore” de accesare ilegală a datelor fiind prevăzute în *CC*, iar cazurile „grave” vor fi prevăzute de *CP*.

O altă cerință stabilește că infracțiunile prevăzute de *Directivă* (art. 9 alin. (2)) trebuie pedepsite cu o pedeapsă maximă cu închisoarea de cel puțin doi ani, de aceea sancțiunea cu închisoarea pentru infracțiunea de la art. 259 din *CP* se majorează până la doi ani. Modificarea se justifică și datorită faptului că în componenta de bază a fost introdus semnul obligator descris mai sus.

Modificarea art. 260 și 260⁴ din *CP*:

Textul actual al Codului Penal prezintă o suprapunere de obiect material/imaterial între art. 260 și art. 260⁴, fapt ce poate genera dificultăți în încadrarea juridică a faptelor și creează un paralelism legislativ. În prezent, obiectul material/imaterial referitor la „parole, coduri de acces sau date informatice similare” este reglementat redundant în ambele articole menționate.

Comparând prevederile din *Directivă*, remarcăm că art. 7 incriminează infracțiunea, în dependență de obiectul material/imaterial, prin litere separate:

- (a) program de calculator [...];
- (b) parolă de calculator, cod de acces sau date similare [...].

O distincție clară se va face și în legislația națională, astfel încât, la art. 260 va fi prevăzută infracțiunea ce ține de „programul de calculator” (și mijloacele tehnice din redacția actuală), iar la art. 260⁴ va fi prevăzută infracțiunea ce ține de „parole de calculator, coduri de acces sau date similare”.

O altă modificare la art. 260 și 260⁴ ține de lista de modalități normative ale faptei prejudiciabile. Pentru a asigura concordanța cu art. 7 din *Directivă*, articolele menționate se completează cu următoarele modalități: procurarea și distribuirea.

La art. 260 a fost adăugat un semn suplimentar al infracțiunii prin care condiționează că mijloacele tehnice sau programele de calculator folosite, trebuie să fie concepute sau adaptate „în principal” pentru comiterea infracțiunilor enumerate. Această condiție este esențială pentru a distinge între instrumentele cu dublă utilizare, evitând astfel incriminarea posesiei unor mijloace/programe legitime folosite de specialiștii în securitate cibernetică pentru audit, administrare, etc. Prin sintagma „în principal”, legiuitorul limitează sfera penală doar la instrumentele create sau modificate cu scopul vădit de a facilita alte infracțiuni.

Modificarea art. 260² din CP:

În art. 260² din CP, nu sunt specificate următoarele modalități normative menționate în art. 5 al Directivei: „periclitatea”, „eliminarea” datelor informatice dintr-un sistem informatic. Fapt pentru care, articolul menționat se completează cu modalitățile respective.

În afară de aceasta, nu sunt identice modalitățile normative „restricționarea accesului” (art. 260² din CP) și „a face inaccesibile” datele informatice dintr-un sistem informatic” (art. 5 al Directivei). Restricționarea accesului la datele informatice presupune limitarea accesului la unul sau mai multe niveluri (parțial, pentru anumiți utilizatori, pe timp limitat etc.). În contrast, a face inaccesibil datele informatice implică îngrădirea totală a accesului, adică datele informatice devin inaccesibile în orice formă (citire, scriere, modificare, export etc.) pentru orice utilizator și pe timp nelimitat. Pentru a garanta conformitatea cu *Directiva*, modalitatea privind „restricționarea accesului” se înlocuiește cu „împiedicarea accesului”.

La art. 260² se introduc de asemenea sancțiuni și pentru persoana juridică, condiția fiind prevăzută la art. 10 din *Directivă*.

Alin. (2) se completează cu o nouă circumstanță agravantă care justifică scara și potențialul de propagare a atacurilor informatice moderne. Utilizarea unor instrumente (programe sau date de acces) special concepute pentru a compromite multiple sisteme simultan indică o pericolozitate sporită a făptuitorului și o vătămare extinsă a relațiilor sociale legate de siguranța informatică.

Alin. (3) la fel se completează cu o nouă circumstanță agravantă ce vizează protejarea directă a pilonilor fundamentali ai societății (energie, sănătate, transporturi, sistem bancar). Infracțiunile informatice îndreptate împotriva infrastructurii critice nu afectează doar date virtuale, ci pot genera consecințe catastrofale asupra serviciilor esențiale pentru populație și stat.

Modificarea art. 260³ din CP:

În art. 260³ din CP, nu sunt specificate următoarele modalități normative pe care le găsim în art. 4 al Directivei: „periclitatea”, „eliminarea” datelor informatice. Fapt pentru care, articolul menționat se completează cu modalitățile respective.

De asemenea, nu sunt identice modalitățile normative „restricționarea accesului” (art. 260² din CP) și „a face inaccesibile” datele informatice dintr-un sistem informatic” (art. 5 al Directivei). Restricționarea accesului la datele informatice presupune limitarea accesului la unul sau mai multe niveluri (parțial, pentru anumiți utilizatori, pe timp limitat etc.). În contrast, a face inaccesibil datele informatice implică îngrădirea totală a accesului, adică datele informatice devin inaccesibile în orice formă (citire, scriere, modificare, export etc.) pentru orice utilizator și pe timp nelimitat. Pentru a garanta conformitatea cu *Directiva*, modalitatea privind „restricționarea accesului” se înlocuiește cu „împiedicarea accesului”.

Articolul se completează cu noi circumstanțe agravante, pentru care se mențin argumentele de mai sus.

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

În vederea atingerii obiectivului trasat, opțiuni alternative nu au fost identificate.
4. Analiza impactului de reglementare
4.1. Impactul asupra sectorului public
Adoptarea Legii pentru modificarea și completarea unor acte normative va spori claritatea și previzibilitatea art. 259 – 260 ⁴ din Codul penal al Republicii Moldova. Totodată, va fi diminuat riscul de interpretare extensivă defavorabilă a legii penale. Cunoaștem că o astfel de interpretare constituie o încălcare a articolului 7 din Convenția Europeană a Drepturilor Omului. Cerința interpretării stricte a normei penale, ca și interzicerea analogiei defavorabile în aplicarea legii penale, urmăresc protecția persoanei împotriva arbitrarului.
4.2. Impactul financiar și argumentarea costurilor estimative
Nu este aplicabil.
4.3. Impactul asupra sectorului privat
Nu este aplicabil.
4.4. Impactul social
Nu este aplicabil.
4.4.1. Impactul asupra datelor cu caracter personal
Nu este aplicabil.
4.4.2. Impactul asupra echității și egalității de gen
Nu este aplicabil.
4.5. Impactul asupra mediului
Nu este aplicabil.
4.6. Alte impacturi și informații relevante
Nu este aplicabil.
5. Compatibilitatea proiectului actului normativ cu legislația UE
5.1. Măsurile normative necesare pentru transpunerea actelor juridice ale UE în legislația națională
Prezentul proiect de lege realizează o transpunere a Directivei 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului.
Obiectivul acestui act juridic constă în armonizarea sistemelor de drept penal ale statelor membre în ceea ce privește atacurile împotriva sistemelor informatice, prin instituirea unor norme minime privind definirea infracțiunilor și a sancțiunilor relevante, precum și de a îmbunătăți cooperarea dintre autoritățile competente, inclusiv poliția și alte servicii specializate de aplicare a legii din statele membre, precum și agențiile și organismele specializate competente ale Uniunii, cum ar fi Eurojust, Europol și Centrul european de combatere a criminalității informatice și

<p>Agencia Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA).</p> <p>Gradul de transpunere al actului este prezentat în tabelul de concordanță, anexat la prezentul proiect de lege. Astfel prezentul proiect de lege transpune: art. 2 lit. (a) și (b); art. 3 – 5; art. 7; art. 9 alin. (2), (3) și (4) litera (a) și (c) din Directiva menționată.</p>
<p>5.2. Măsurile normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE</p>
<p>Conform art. 46 din Codul penal, „grupul criminal organizat este o reuniune stabilă de persoane care s-au organizat în prealabil pentru a comite una sau mai multe infracțiuni”. Această definiție corespunde doar în parte definiției noțiunii „organizație criminală” din art. 1 pct. 1 al Deciziei-cadru 2008/841/JAI a Consiliului din 24 octombrie 2008 privind lupta împotriva crimei organizate: „«organizație criminală» desemnează o asociație structurată, stabilită în timp, de mai mult de două persoane, care acționează concertat în vederea comiterii de infracțiuni pasibile de o pedeapsă privativă de libertate sau de aplicarea unei măsuri de siguranță privative de libertate cu o durată maximă de cel puțin patru ani, sau de o pedeapsă mai severă, pentru a obține, direct sau indirect, un beneficiu financiar sau de altă natură materială”.</p>
<p>6. Avizarea și consultarea publică a proiectului actului normativ</p>
<p>În scopul respectării prevederilor <i>Legii nr. 239/2008 privind transparența în procesul decizional</i>, pe pagina web oficială a Ministerului Justiției www.justice.gov.md, la compartimentul <i>Transparența decizională</i>, a fost plasat anunțul privind inițierea procesului de elaborare a prezentului proiect, care poate fi accesat la linkul: https://justice.gov.md/ro/content/anunt-privind-initierea-procesului-de-elaborare-proiectului-de-lege-pentru-modificarea-43.</p> <p>Un anunț similar a fost plasat pe portalul guvernamental particip.gov.md, unde poate fi accesat la următorul link: https://particip.gov.md/ro/document/stages/anunt-privind-initierea-procesului-de-elaborare-a-proiectului-de-lege-pentru-modificarea-unor-acte-n/16162.</p> <p>Propuneri sau recomandări nu au fost recepționate.</p>
<p>7. Concluziile expertizelor</p>
<p>Proiectul urmează a fi supus expertizei juridice și anticorupție, iar constatările acestora vor fi incluse după recepționarea expertizelor.</p>
<p>8. Modul de încorporare a actului în cadrul normativ existent</p>
<p>Proiectul nu presupune modificarea sau abrogarea altor acte normative.</p>
<p>9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ</p>
<p>Implementarea prevederilor proiectului nu implică realizarea unor măsuri speciale în acest sens.</p>

Secretar de stat

Lilian APOSTOL

Tabel de concordanță

1.	Titlul actului Uniunii Europene, inclusiv cele mai recente amendamente incluse Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului			
2.	Titlul proiectului de act normativ național Proiectul de lege pentru modificarea unor acte normative (prevenirea și combaterea atacurilor împotriva sistemelor informatice)			
3.	Gradul general de compatibilitate: Compatibil			
Actul Uniunii Europene		Proiectul de act normativ național	Gradul de compatibilitate	Observațiile
4		5	6	7
<i>Articolul 1</i> Obiect Prezenta directivă stabilește norme minime privind definiția infracțiunilor și a sancțiunilor penale în domeniul atacurilor împotriva sistemelor informatice. De asemenea, prezenta directivă urmărește să faciliteze prevenirea unor astfel de infracțiuni și să îmbunătățească cooperarea dintre autoritățile judiciare și alte autorități competente.				
<i>Articolul 2</i>		Art. I pct. 1 din Proiectul de lege:	Compatibil	

<p align="center">Definiții</p> <p>În sensul prezentei directive, se aplică următoarele definiții:</p> <p>(a) „sistem informatic” înseamnă un dispozitiv sau grup de dispozitive interconectate sau omoloage, dintre care unul sau mai multe asigură, prin intermediul unui program, prelucrarea automată a datelor informatice, precum și datele informatice stocate, prelucrate, recuperate sau transmise de acest dispozitiv sau grup de dispozitive în vederea exploatării, a utilizării, a protecției și a întreținerii lor;</p>	<p>1. Articolul 134²⁵ va avea următorul cuprins:</p> <p>„Articolul 134²⁵. Sistem informatic</p> <p>Prin sistem informatic se înțelege orice dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în legătură care asigură ori dintre care unul sau mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor informatice, inclusiv a datelor informatice stocate, prelucrate, recuperate sau transmise de acest dispozitiv sau ansamblu de dispozitive în vederea exploatării, a utilizării, a protecției și a întreținerii lor.”.</p>		
<p>(b) „date informatice” înseamnă o reprezentare de fapte, informații sau concepte într-o formă adecvată pentru prelucrare într-un sistem informatic, inclusiv un program care permite unui sistem informatic să execute o funcție;</p>	<p>Art. I pct. 2 din Proiectul de lege:</p> <p>2. Se completează cu articolul 134²⁷ cu următorul cuprins:</p> <p>„Articolul 134²⁷. Date informatice</p> <p>Prin date informatice se înțelege datele definite astfel în Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice.”</p>	<p>Compatibil</p>	<p>În corespundere cu art. 2 al Legii nr. 20 din 03.02.2009 privind prevenirea și combaterea criminalității informatice, prin „date informatice” se are în vedere „orice reprezentare de fapte, informații sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcții de către un sistem informatic”. Această definiție o reproduce, aproape cuvânt cu cuvânt, pe cea din art. 2 lit. b) din Directiva 2013/40/UE.</p>
<p>(c) „persoană juridică” înseamnă o entitate care are statutul de persoană juridică în conformitate cu legislația aplicabilă, dar nu include statele sau alte organisme publice aflate în exercițiul autorității de stat și organizațiile internaționale de drept public;</p>		<p>Compatibil</p>	<p>În Codul civil găsim următoarele dispoziții relevante: „Persoana juridică este subiectul de drept constituit în condițiile legii, având o organizare de sine stătătoare și un patrimoniu propriu și distinct, afectat realizării unui anumit scop conform cu legea, ordinea publică și bunele moravuri” (art. 171 alin. (1)); „Persoanele juridice străine sunt asimilate, în condițiile legii, cu persoanele juridice ale Republicii Moldova” (art. 172); „Statul și unitățile administrativ-teritoriale participă la raporturile juridice civile pe</p>

			<p>poziții de egalitate cu celelalte subiecte de drept. Atribuțiile statului și ale unităților administrativ-teritoriale se exercită în asemenea raporturi de organele acestora, în conformitate cu competența lor” (art. 174 alin. (1)).</p> <p>Conform art. 21 alin. (4) din Codul penal, „persoanele juridice, cu excepția autorităților publice, răspund penal pentru infracțiunile pentru săvârșirea cărora este prevăzută sancțiune pentru persoanele juridice în partea specială din prezentul cod”.</p>
<p>(d) „fără a avea dreptul” înseamnă un comportament menționat de prezenta directivă, inclusiv accesarea, afectarea integrității sau interceptarea fără autorizare din partea proprietarului sau a unui alt titular de drepturi, a sistemului sau a unei părți a acestuia, sau care nu este permis în temeiul legislației naționale.</p>		Compatibil	<p>Potrivit art. 9 alin. (1) din Codul civil, „drepturile [...] civile apar în temeiul legii, precum și în baza actelor persoanelor fizice și juridice care, deși nu sunt prevăzute de lege, dau naștere la drepturi și obligații civile, pornind de la principiile legislației civile”. Extrapolând, se poate susține că orice drepturi apar fie în temeiul legii, fie în temeiul unor principii stabilite în legislația națională. Drept urmare, se poate afirma că a acționa fără drept înseamnă a acționa ilegal.</p> <p>În anumite articole din Codul penal, care sunt similare cu unele prevederi ale Directivei 2013/40/UE, găsim expresii care reprezintă extensii ale termenului „illegal”:</p> <ul style="list-style-type: none"> • „de către o persoană care nu este autorizată în temeiul legii sau al unui contract, care depășește limitele autorizării ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfășoare cercetări științifice sau să efectueze orice altă operațiune într-un sistem informatic” (art. 259); • „fără drept” (art. 2602 și 2603). <p>În alte articole din Codul penal, care sunt similare cu unele prevederi ale Directivei 2013/40/UE, putem identifica fie termenul „illegală”</p>

			(art. 2601), fie expresia „în mod ilegal” (art. 260 și 2604). În concluzie, termenii și expresiile susmenționate din art. 259, 260, 260 ¹ – 260 ⁴ din Codul penal) (coroborate cu art. 9 alin. (1) din Codul civil) sunt compatibile cu prevederea din art. 2 lit. (d) din Directiva 2013/40/UE.
<p><i>Articolul 3</i></p> <p>Accesarea ilegală a sistemelor informatice</p> <p>Statele membre adoptă măsurile necesare pentru a garanta că accesarea cu intenție și fără drept a unui sistem informatic sau a unei părți a acestuia este incriminată atunci când este săvârșită prin încălcarea unei măsuri de securitate, cel puțin atunci când nu reprezintă un caz minor.</p>	<p>Art. I pct. 3 din Proiectul de lege:</p> <p>3. La articolul 259: la alineatului (1): după textul „Accesarea ilegală” se substituie completează cu textul „Accesarea ilegală, în întregime sau în parte, prin violarea măsurilor de securitate,”; textul „până la 1 an” se substituie cu textul „până la 2 ani”; la alineatul (2), litera a) se abrogă.</p>	<p>Compatibil</p>	<p>Codul penal al Republicii Moldova nr. 985/2002 (redacția în vigoare)</p> <p>Articolul 259. Accesul ilegal la un sistem informatic</p> <p>(1) Accesarea ilegală a unui sistem informatic de către o persoană care nu este autorizată în temeiul legii sau al unui contract, care depășește limitele autorizării ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfășoare cercetări științifice sau să efectueze orice altă operațiune într-un sistem informatic [...].</p> <p>1. Art. 259 din Codul penal corespunde dispoziției de la art. 3 din Directiva 2013/40/UE în partea care se referă la „accesarea cu intenție și fără drept a unui sistem informatic, însă nu corespunde aceleiași dispoziții în partea care se referă la „accesarea cu intenție și fără drept [...] a unei părți a [unui sistem informatic]”. – din aceste considerente, prin prezentul proiect de lege, art. 259 se modifică astfel încât să incrimineze în art. 259 din Codul penal accesarea ilegală chiar și în parte a unui sistem informatic.</p> <p>2. Directiva prevede drept condiție obligatorie la comiterea infracțiunii „încălcarea unei măsuri de</p>

			securitate”, însă în art. 259 CP încălcarea măsurilor de securitate apare nu în calitate de condiție obligatorie a infracțiunii, ci doar ca circumstanță agravantă („cu violarea sistemelor de protecție” (alin. (2) lit. a)) – iar din aceste considerente, prin prezentul proiect de lege, art. 259 se completează cu această condiție obligatorie.
<p>Articolul 4</p> <p>Afectarea ilegală a integrității sistemului</p> <p>Statele membre adoptă măsurile necesare pentru a asigura că perturbarea gravă sau întreruperea funcționării unui sistem informatic prin introducerea, transmiterea, periclitarea, ștergerea, deteriorarea, modificarea, eliminarea datelor informatice sau prin a le face inaccesibile, cu intenție și fără drept, este incriminată, cel puțin atunci când nu reprezintă un caz minor.</p>	<p>Art. I pct. 7 din Proiectul de lege:</p> <p>7. La articolul 260³:</p> <p>dispoziția alineatului (1) va avea următorul cuprins:</p> <p>„(1) Perturbarea sau întreruperea funcționării unui sistem informatic prin introducerea, transmiterea, periclitarea, ștergerea, deteriorarea, modificarea, eliminarea datelor informatice sau împiedicarea accesului la aceste, cu intenție și fără drept ”;</p> <p>alineatul (2):</p> <p>litera c) va avea următorul cuprins:</p> <p>„c) săvârșite prin utilizarea unui program de calculator, a unei parole de calculator, a unui cod de acces sau a altor date de acces la un sistem informatic sau la o parte a unui sistem informatic, dacă aceste date au fost concepute sau adaptate în scopul afectării a două sau mai multor sisteme informatice;”.</p> <p>dispoziția alineatului (3) va avea următorul cuprins:</p>	<p>Compatibil</p>	<p>Codul penal al Republicii Moldova nr. 985/2002 (redacția în vigoare)</p> <p>Articolul 260³. Perturbarea funcționării sistemului informatic</p> <p>(1) Perturbarea funcționării unui sistem informatic prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea intenționată și fără drept a datelor informatice sau prin restricționarea accesului la aceste date [...].</p> <p>În art. 260³ din Codul penal, nu sunt specificate următoarele modalități normative pe care le găsim în art. 4 al Directivei 2013/40/UE:</p> <ul style="list-style-type: none"> a) periclitarea datelor informatice; b) eliminarea datelor informatice; c) a face inaccesibile datele informatice. <p>Aceste modalități normative au fost introduse prin prezentul proiect de lege.</p>

	<p>(3) Acțiunile prevăzute la alin. (1) sau (2):</p> <p>a) săvârșite de un grup criminal organizat sau de o organizație criminală;</p> <p>b) care au cauzat daune în proporții deosebit de mari;</p> <p>c) săvârșite împotriva unui sistem informatic din infrastructura critică”.</p>		
<p>Articolul 5</p> <p>Afectarea ilegală a integrității datelor</p> <p>Statele membre adoptă măsurile necesare pentru a asigura că fapta care constă în ștergerea, periclitarea, deteriorarea, modificarea, eliminarea datelor informatice dintr-un sistem informatic sau în a le face inaccesibile, cu intenție și fără drept, este incriminată, cel puțin atunci când nu reprezintă un caz minor.</p>	<p>Art. I pct. 6 din Proiectul de lege:</p> <p>6. La articolul 260²:</p> <p>alineatul (1) va avea următorul cuprins:</p> <p>„(1) Ștergerea, periclitarea, deteriorarea, modificarea, eliminarea datelor informatice dintr-un sistem informatic sau împiedicarea accesului la aceste date, cu intenție și fără drept, precum și transferul neautorizat de date informatice dintr-un sistem informatic, dintr-un mijloc de stocare, dobândirea, comercializarea sau punerea la dispoziție, sub orice formă, a datelor informatice cu acces limitat se pedepsesc cu amendă în mărime de la 850 la 1350 unități convenționale sau cu închisoare de la 2 la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 2000 la 4000 unități convenționale cu privarea de dreptul de a exercita o anumită activitate.”;</p>	Compatibil	<p>Codul penal al Republicii Moldova nr. 985/2002 (redacția în vigoare)</p> <p>Articolul 260². Alterarea integrității datelor informatice ținute într-un sistem informatic</p> <p>(1) Modificarea, ștergerea sau deteriorarea intenționată și fără drept a datelor informatice ținute într-un sistem informatic ori restricționarea ilegală a accesului la aceste date, transferul neautorizat de date informatice dintr-un sistem informatic, dintr-un mijloc de stocare, dobândirea, comercializarea sau punerea la dispoziție, sub orice formă, a datelor informatice cu acces limitat</p> <p>[...].</p> <p>În art. 260² din Codul penal, nu sunt specificate următoarele modalități normative menționate în art. 5 al Directivei 2013/40/UE:</p> <p>a) periclitarea datelor informatice dintr-un sistem informatic;</p> <p>b) eliminarea datelor informatice dintr-un sistem informatic;</p> <p>c) a face inaccesibile datele informatice.</p> <p>Aceste modalități normative au fost introduse prin prezentul proiect de lege.</p>
Articolul 6	Art. I pct. 5 din Proiectul de lege:	Compatibil	Codul penal al Republicii Moldova nr. 985/2002 (redacția în vigoare)

<p align="center">Interceptarea ilegală</p> <p>Statele membre adoptă măsurile necesare pentru a garanta că interceptarea, cu intenție și fără drept, prin mijloace tehnice, de transmisii private de date informatice către un sistem informatic, dinspre acesta sau în interiorul acestuia, inclusiv de emisii electromagnetice provenite de la un sistem informatic care transmite asemenea date informatice este incriminată, cel puțin atunci când nu reprezintă un caz minor.</p>	<p>5. La articolul 260¹: cuvântul „întreprinderii” se substituie cu cuvântul „persoanei juridice”.</p>		<p>Articolul 260¹. Interceptarea ilegală a unei transmisiide date informatice</p> <p>Interceptarea ilegală a unei transmisii de date informatice (inclusiv a unei emisii electronice ori electromagnetice) care nu sînt publice și care sînt destinate unui sistem informatic, provin dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic</p> <p>se pedepsește cu amendă în mărime de la 850 la 1350 unități convenționale sau cu închisoare de până la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 4000 la 7000 unități convenționale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea întreprinderii.</p>
<p align="center">Articolul 7</p> <p align="center">Instrumentele care servesc la săvârșirea infracțiunilor</p> <p>Statele membre adoptă măsurile necesare pentru a garanta că producerea, vânzarea, procurarea în vederea utilizării, importul, distribuirea sau punerea la dispoziție în alt mod, cu intenție, a următoarelor instrumente, fără a avea dreptul și cu intenția de a servi la săvârșirea oricăreia dintre infracțiunile menționate la articolele 3-6, sunt incriminate, cel puțin atunci când nu reprezintă un caz minor:</p> <p>(a) un program de calculator, conceput sau adaptat în principal în scopul săvârșirii oricăreia dintre infracțiunile menționate la articolele 3-6;</p>	<p align="center">Art. I pct. 4 din Proiectul de lege:</p> <p>4. La articolul 260: dispoziția va avea următorul cuprins: „Producerea, vânzarea, procurarea, importul, distribuirea sau punerea în alt mod la dispoziție, în mod ilegal, a unui mijloc tehnic sau program de calculator, conceput sau adaptat în principal în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 237, 259, 2601–2603, 2605–2607,”;</p> <p>cuvântul „întreprinderii” se substituie cu cuvântul „persoanei juridice”.</p>	<p align="center">Compatibil</p>	
<p>(b) o parolă de calculator, un cod de acces sau date similare, prin care un întreg sistem informatic sau orice parte a acestuia poate fi</p>	<p align="center">Art. I pct. 8 din Proiectul de lege:</p> <p>8. La articolul 260⁴, dispoziția din</p>	<p align="center">Compatibil</p>	

accesat(ă).	alineatul (1) va avea următorul cuprins: „Producerea, vânzarea, procurarea, importul, distribuirea sau punerea în alt mod la dispoziție, în mod ilegal, a unei parole de calculator, a unui cod de acces sau a unor date similare, prin care un întreg sistem informatic sau orice parte a acestuia poate fi accesat, în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 237, 259, 2601–2603, 2605 sau 2606.”.		
<p>Articolul 8</p> <p>Instigarea, complicitatea și tentativa</p> <p>(1) Statele membre asigură că instigarea și complicitatea la săvârșirea oricăreia dintre infracțiunile menționate la articolele 3-7 sunt incriminate.</p>		Compatibil	<p>În art. 42 din Codul penal se stabilește, inter alia: „[...] (4) Se consideră instigator persoana care, prin orice metode, determină o altă persoană să săvârșească o infracțiune. (5) Se consideră complice persoana care a contribuit la săvârșirea infracțiunii prin sfaturi, indicații, prestare de informații, acordare de mijloace sau instrumente ori înlăturare de obstacole, precum și persoana care a promis dinainte că îl va favoriza pe infractor, va tăinui mijloacele sau instrumentele de săvârșire a infracțiunii, urmele acesteia sau obiectele dobândite pe cale criminală ori persoana care a promis din timp că va procura sau va vinde atare obiecte”.</p> <p>La rândul său, art. 83 din Codul penal prevede că „[...] instigatorul și complicele la o infracțiune, prevăzută de legea penală, săvârșită cu intenție se sancționează cu pedeapsa prevăzută de lege pentru autor. La stabilirea pedepsei se ține cont de contribuția fiecăruia la săvârșirea infracțiunii, precum și de prevederile art. 75”.</p> <p>În concluzie, dispozițiile de la art. 42 alin. (4) și (5), art. 83 din Codul penal (coroborate cu art. 259, 260, 2601 – 2604 din Codul penal) sunt compatibile cu prevederea din art. 8 alin. (1) al Directivei</p>

			2013/40/UE.
(2) Statele membre se asigură că tentativa de săvârșire a oricăreia dintre infracțiunile prevăzute la articolele 4 și 5 este incriminată.		Compatibil	<p>Conform art. 25 alin. (3) din Codul penal, „răspunderea pentru [...] tentativă de infracțiune se stabilește, conform articolului corespunzător din partea specială a prezentului cod, ca și pentru infracțiunea consumată, cu trimitere la art. [...] 27, respectându-se prevederile art. 81”.</p> <p>În corespundere cu art. 27 din Codul penal, „se consideră tentativă de infracțiune acțiunea sau inacțiunea intenționată îndreptată nemijlocit spre săvârșirea unei infracțiuni dacă, din cauze independente de voința făptuitorului, aceasta nu și-a produs efectul”.</p> <p>La rândul său, art. 81 din Codul penal prevede, printre altele: „(1) La aplicarea pedepsei pentru infracțiunea neconsumată se ține cont de circumstanțele în virtutea cărora infracțiunea nu a fost dusă până la capăt. [...] (3) Mărimea pedepsei pentru tentativă de infracțiune ce nu constituie o recidivă nu poate depăși trei pătrimi din maximumul celei mai aspre pedepse prevăzute la articolul corespunzător din partea specială a prezentului cod pentru infracțiunea consumată. [...]”.</p> <p>În concluziile, dispozițiile de la art. 25 alin. (3), art. 27 și 81 din Codul penal (coroborate cu art. 2602 și 2603 din Codul penal) sunt compatibile cu prevederea din art. 8 alin. (2) al Directivei 2013/40/UE.</p>
<p>Articolul 9</p> <p>Sancțiuni</p> <p>(1) Statele membre iau măsurile necesare pentru a garanta că infracțiunile menționate la articolele 3-8 sunt sancționate de sancțiuni penale eficace, proporționale și disuasive.</p>		Compatibil	<p>Se poate afirma că în sancțiunile din art. 259, 260, 260¹ – 260⁴ din Codul penal (inclusiv atunci când aceste articole sunt coroborate cu art. 25 alin. (3), art. 27, art. 42 alin. (4) și (5), art. 81 sau 83 din Codul penal) sunt stabilite pedepse eficace, proporționale și disuasive.</p>

<p>(2) Statele membre iau măsurile necesare pentru a garanta că infracțiunile menționate la articolele 3-7 sunt sancționate cu o pedeapsă maximă cu închisoarea de cel puțin doi ani, cel puțin atunci când nu reprezintă un caz minor.</p>	<p>Art. I pct. 3 din Proiectul de lege:</p> <p>3. La articolul 259: la alineatului (1): după textul „Accesarea ilegală” se substituie completează cu textul „Accesare ilegală, în întregime sau în parte, prin violarea măsurilor de securitate,”;</p> <p>textul „până la 1 an” se substituie cu textul „până la 2 ani”;</p> <p>la alineatul (2), litera a) se abrogă.</p>	<p>Compatibil</p>	<p>În majoritatea cazurilor, în sancțiunile din art. 259, 260, 260¹ – 260⁴ din Codul penal, este respectată cerința din art. 9 alin. (2) al Directivei 2013/40/UE.</p> <p>Singura excepție constituie sancțiunea din art. 259 alin. (1) din Codul penal, în care este stabilită, inter alia, pedeapsa cu închisoare de până la 1 an.</p> <p>Drept urmare, s-a dispus modificarea sancțiunii articolului 259 alin. (1) pentru a corespunde cu art. 9 alin. (2) a Directivei 2013/40/UE.</p>
<p>(3) Statele membre iau măsurile necesare pentru a garanta că infracțiunile menționate la articolele 4 și 5 sunt sancționate cu o pedeapsă maximă cu închisoarea de cel puțin trei ani în cazul în care sunt săvârșite cu intenție și un număr semnificativ de sisteme informatice a fost afectat prin utilizarea unui instrument menționat la articolul 7, conceput sau adaptat în principal în acest scop.</p>	<p>Art. I pct. 7 din Proiectul de lege:</p> <p>La articolul 260³: [...] alineatul (2): litera c) va avea următorul cuprins: „c) săvârșite prin utilizarea unui program de calculator, a unei parole de calculator, a unui cod de acces sau a altor date de acces la un sistem informatic sau la o parte a unui sistem informatic, dacă aceste date au fost concepute sau adaptate în scopul afectării a două sau mai multor sisteme informatice;”.</p> <p>[...].</p> <p>Art. I pct. 6 din Proiectul de lege:</p> <p>La articolul 260²: [...] la alineatul (2): se completează cu litera c) cu următorul</p>	<p>Compatibil</p>	<p>Articolele 260² și 260³ se completează cu o nouă circumstanță agravantă care va acoperi această prevedere a Directivei.</p>

	<p>cuprins:</p> <p>„c) săvârșite prin utilizarea unui program de calculator, a unei parole de calculator, a unui cod de acces sau a altor date de acces la un sistem informatic sau la o parte a acestuia, dacă aceste date au fost concepute sau adaptate în scopul afectării a două sau mai multor sisteme informatice;</p> <p>după textul „cu închisoare de la 3 la 7 ani”, se completează cu textul „ , cu amendă, aplicată persoanei juridice, în mărime de la 4000 la 7000 unități convenționale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea persoanei juridice”.</p> <p>[...].</p>		
<p>(4) Statele membre iau măsurile necesare pentru a garanta că infracțiunile menționate la articolele 4 și 5 sunt sancționate cu o pedeapsă maximă cu închisoarea de cel puțin cinci ani în cazul în care:</p> <p>(a) sunt săvârșite în cadrul unei organizații criminale, astfel cum este definită în Decizia-cadru 2008/841/JAI, independent de sancțiunea prevăzută de aceasta;</p>	<p>Art. I pct. 7 din Proiectul de lege:</p> <p>La articolul 260³:</p> <p>[...]</p> <p>dispoziția alineatului (3) va avea următorul cuprins:</p> <p>(3) Acțiunile prevăzute la alin. (1) sau (2):</p> <p>a) săvârșite de un grup criminal organizat sau de o organizație criminală;</p> <p>b) care au cauzat daune în proporții deosebit de mari;</p> <p>c) săvârșite împotriva unui sistem informatic din infrastructura critică”.</p>	Compatibil	<p>Codul penal al Republicii Moldova nr. 985/2002 (redacția în vigoare)</p> <p>Articolul 260². Alterarea integrității datelor informatice ținute într-un sistem informatic</p> <p>[...]</p> <p>(3) ... a) săvârșite de un grup criminal organizat sau de o organizație criminală; ...</p> <p>se pedepsesc cu închisoare de la 5 la 10 ani.</p> <p>Art. 260³ se modifică prin prezentul proiect de lege pentru a acoperi alinierea cu această normă a Directivei. Pedeapsa cu închisoarea pentru alin. (3) este de la 5 la 10 ani.</p>
(b) provoacă prejudicii grave;	Art. I pct. 7 din Proiectul de lege:	Compatibil	Codul penal al Republicii Moldova nr. 985/2002

	<p>La articolul 260³: [...]</p> <p>dispoziția alineatului (3) va avea următorul cuprins: (3) Acțiunile prevăzute la alin. (1) sau (2): a) săvârșite de un grup criminal organizat sau de o organizație criminală; b) care au cauzat daune în proporții deosebit de mari; c) săvârșite împotriva unui sistem informatic din infrastructura critică”.</p>		<p>(redacția în vigoare) Articolul 260². Alterarea integrității datelor informatice ținute într-un sistem informatic [...] (3) ... b) care au cauzat daune în proporții mari... se pedepsesc cu închisoare de la 5 la 10 ani. Pedepsa cu închisoarea pentru art. 260³ alin. (3) este de la 5 la 10 ani.</p>
sau (c) sunt săvârșite împotriva unui sistem informatic din infrastructura critică.	<p>Art. I pct. 6 din Proiectul de lege: La articolul 260²: [...] la alineatul (3): se completează cu litera c) cu următorul cuprins: „c) săvârșite împotriva unui sistem informatic din infrastructura critică,”;</p> <p>Art. I pct. 7 din Proiectul de lege: La articolul 260³: [...]</p> <p>dispoziția alineatului (3) va avea următorul cuprins: (3) Acțiunile prevăzute la alin. (1) sau (2): a) săvârșite de un grup criminal organizat sau de o organizație criminală; b) care au cauzat daune în proporții deosebit de mari; c) săvârșite împotriva unui sistem</p>	Compatibil	

	informatic din infrastructura critică”.		
<p>(5) Statele membre iau măsurile necesare pentru a garanta că infracțiunile menționate la articolele 4 și 5, în cazurile în care sunt săvârșite prin abuzul de date cu caracter personal ale unei alte persoane, în scopul de a obține încrederea unei terțe părți, cauzând prejudicii prin aceasta deținătorului de drept al identității, acestea, în conformitate cu legislația națională, pot fi considerate circumstanțe agravante, cu excepția cazurilor în care respectivele circumstanțe sunt încadrate la altă infracțiune sancționată de legislația națională.</p>		Compatibil	<p>Art. 177¹ din Codul penal prevede răspundere pentru falsul de identitate, precum și art. 260⁷ din Codul penal care prevede răspunderea pentru furtul de identitate.</p> <p>Interpretarea sistemică a acestor două articole denotă că ele corespund exigenței „cu excepția cazurilor în care respectivele circumstanțe sunt încadrate la altă infracțiune sancționată de legislația națională” din art. 9 alin. (5) din Directiva 2013/40/UE. În consecință, nu este necesară completarea art. 260² și 260³ din Codul penal.</p>
<p>Articolul 10</p> <p>Răspunderea persoanelor juridice</p> <p>(1) Statele membre iau măsurile necesare pentru a garanta angajarea răspunderii persoanelor juridice pentru oricare dintre infracțiunile prevăzute la articolele 3-8, săvârșite în beneficiul lor de către orice persoană, acționând fie în nume propriu, fie ca parte a unui organism al persoanei juridice și având o funcție de conducere în cadrul persoanei juridice, în temeiul:</p> <p>(a) unei împuterniciri din partea persoanei juridice;</p> <p>(b) unei prerogative de a lua decizii în numele persoanei juridice;</p> <p>(c) unei prerogative de a exercita controlul în cadrul persoanei juridice.</p>	<p>Art. I pct. 6 din Proiectul de lege:</p> <p>6. La articolul 260²:</p> <p>alineatul (1) va avea următorul cuprins:</p> <p>„(1) Ștergerea, periclitarea, deteriorarea, modificarea, eliminarea datelor informatice dintr-un sistem informatic sau împiedicarea accesului la aceste date, cu intenție și fără drept, precum și transferul neautorizat de date informatice dintr-un sistem informatic, dintr-un mijloc de stocare, dobândirea, comercializarea sau punerea la dispoziție, sub orice formă, a datelor informatice cu acces limitat</p> <p>se pedepsesc cu amendă în mărime de la 850 la 1350 unități convenționale sau cu închisoare de la 2 la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 2000 la 4000 unități convenționale cu privarea de dreptul de a exercita o anumită activitate.</p>	Compatibil	<p>Dispozițiile de la art. 21 alin. (3) lit. a) și b), alin. (3¹) și (4) din Codul penal sunt compatibile cu prevederea din art. 10 alin. (1) al Directivei 2013/40/UE.</p> <p>În art. 259, 260, 260¹, 260³ și 260⁴ din Codul penal sunt prevăzute pedepse pentru persoanele juridice.</p> <p>În contrast, în art. 260² din Codul penal nu prevedea pedepse pentru persoanele juridice. Prin urmare, art. 260² se completează cu acest aspect.</p> <p>Codul penal al Republicii Moldova nr. 985/2002 (redacția în vigoare)</p> <p>Articolul 21. Subiectul infracțiunii</p> <p>(3) O persoană juridică, cu excepția autorităților publice, este pasibilă de răspundere penală pentru o faptă prevăzută de legea penală dacă aceasta nu a îndeplinit sau a îndeplinit necorespunzător dispozițiile directe ale legii ce stabilesc îndatoriri sau interdicții privind efectuarea unei anumite activități și se constată cel puțin una din următoarele circumstanțe:</p> <p>a) fapta a fost săvârșită în interesul persoanei juridice</p>

			<p>respective de către o persoană fizică împuternicită cu funcții de conducere, care a acționat independent sau ca parte a unui organ al persoanei juridice;</p> <p>b) fapta a fost admisă sau autorizată, sau aprobată, sau utilizată de către persoana împuternicită cu funcții de conducere;</p> <p>c) fapta a fost săvârșită datorită lipsei de supraveghere și control din partea persoanei împuternicite cu funcții de conducere.</p> <p>(3¹) O persoană fizică se consideră împuternicită cu funcții de conducere dacă are cel puțin una din următoarele funcții:</p> <p>a) de reprezentare a persoanei juridice;</p> <p>b) de luare a deciziilor în numele persoanei juridice;</p> <p>c) de exercitare a controlului în cadrul persoanei juridice.</p>
<p>(2) Statele membre adoptă măsurile necesare pentru a garanta angajarea răspunderii persoanelor juridice în cazul în care nesupravegherea sau neexercitarea controlului, imputabile unei persoane menționate la alineatul (1), a permis săvârșirea, de către o persoană aflată în subordine, a oricăreia dintre infracțiunile menționate la articolele 3-8, în beneficiul acelei persoane juridice.</p>		Compatibil	<p>Codul penal al Republicii Moldova nr. 985/2002 (redacția în vigoare)</p> <p>Articolul 21. Subiectul infracțiunii</p> <p>(3) O persoană juridică, cu excepția autorităților publice, este pasibilă de răspundere penală pentru o faptă prevăzută de legea penală dacă aceasta nu a îndeplinit sau a îndeplinit necorespunzător dispozițiile directe ale legii ce stabilesc îndatoriri sau interdicții privind efectuarea unei anumite activități și se constată cel puțin una din următoarele circumstanțe:</p> <p>a) fapta a fost săvârșită în interesul persoanei juridice respective de către o persoană fizică împuternicită cu funcții de conducere, care a acționat independent sau ca parte a unui organ al persoanei juridice;</p> <p>b) fapta a fost admisă sau autorizată, sau aprobată, sau utilizată de către persoana împuternicită cu funcții de conducere;</p> <p>c) fapta a fost săvârșită datorită lipsei de</p>

			supraveghere și control din partea persoanei împuternicite cu funcții de conducere.
(3) Răspunderea persoanelor juridice în temeiul alineatelor (1) și (2) nu exclude procedurile penale îndreptate împotriva persoanelor fizice care sunt autori, instigatori sau complici la oricare dintre infracțiunile prevăzute la articolele 3-8.		Compatibil	Codul penal al Republicii Moldova nr. 985/2002 (redacția în vigoare) Articolul 21. Subiecții infracțiunii (5) Răspunderea penală a persoanei juridice nu exclude răspunderea persoanei fizice pentru infracțiunea săvârșită.
<p>Articolul 11</p> <p>Sancțiuni aplicabile persoanelor juridice</p> <p>(1) Statele membre iau măsurile necesare pentru a garanta că oricărei persoane juridice a cărei răspundere este angajată în temeiul articolului 10 alineatul (1) i se aplică sancțiuni eficiente, proporționale și disuasive, care includ amenzi penale sau administrative și care pot să includă alte sancțiuni, ca de exemplu:</p> <p>(a) decăderea din dreptul de a primi beneficii publice sau ajutor public;</p> <p>(b) interdicția temporară sau permanentă de a desfășura activități comerciale;</p> <p>(c) punerea sub supraveghere judiciară;</p> <p>(d) lichidarea judiciară;</p> <p>(e) închiderea temporară sau permanentă a unităților care au servit la comiterea infracțiunii.</p>		Compatibil	<p>În art. 259, 260, 260¹, 260³ și 260⁴ din Codul penal, amenda este stabilită ca pedeapsă principală pentru persoanele juridice. În aceleași articole, privarea persoanei juridice de dreptul de a exercita o anumită activitate și lichidarea acesteia se aplică fie ca pedepse principale, fie ca pedepse complementare. Considerăm astfel de pedepse eficiente, proporționale și disuasive.</p> <p>O afirmație similară se poate face în legătură cu pedepsele stabilite în art. 260² din Codul penal (în varianta <i>de lege ferenda</i> propusă <i>supra</i> pentru sancțiunile din acest articol).</p> <p>Referitor la pedepsele menționate la art. 11 lit. (a), c) și (e) din Directivă, acestea fac obiectul de reglementare a altui proiect de lege, proiectului de Lege pentru modificarea unor acte normative (consolidarea răspunderii penale a persoanei juridice) care a fost transmis Comisiei Europene la data de 9 februarie 2026.</p>
(2) Statele membre iau măsurile necesare pentru a garanta că oricărei persoane juridice a cărei răspundere este angajată în temeiul articolului 10 alineatul (2) i se aplică sancțiuni sau măsuri eficiente, proporționale și disuasive.		Compatibil	În art. 259, 260, 260 ¹ , 260 ³ și 260 ⁴ din Codul penal, amenda este stabilită ca pedeapsă principală pentru persoanele juridice. În aceleași articole, privarea persoanei juridice de dreptul de a exercita o anumită activitate și lichidarea acesteia se aplică fie ca pedepse principale, fie ca pedepse complementare.

			<p>Considerăm astfel de pedepse eficace, proporționale și disuasive.</p> <p>O afirmație similară se poate face în legătură cu pedepsele stabilite în art. 260² din Codul penal (în varianta <i>de lege ferenda</i> propusă <i>supra</i> pentru sancțiunile din acest articol).</p>
<p>Articolul 12</p> <p>Competență</p> <p>(1) Statele membre își determină competența cu privire la infracțiunile menționate la articolele 3-8 în cazul în care infracțiunea a fost săvârșită:</p> <p>(a) integral sau parțial pe teritoriul lor; sau</p> <p>(b) de către unul dintre resortisanții lor, cel puțin în cazurile în care acțiunea constituie o infracțiune acolo unde a fost săvârșită.</p>		Compatibil	<p>Art. 11 din Codul penal consacră principiul teritorialității legii penale, stabilind expres și excepțiile de la acesta. În completare, art. 12 din Codul penal reglementează locul săvârșirii faptei, inclusiv în cazul infracțiunilor transnaționale</p>
<p>(2) Atunci când își determină competența în conformitate cu alineatul (1) litera (a), un stat membru se asigură că are competență atunci când:</p> <p>(a) autorul săvârșește infracțiunea atunci când este prezent fizic pe teritoriul său, indiferent dacă infracțiunea vizează un sistem informatic situat pe teritoriul său; sau</p> <p>(b) infracțiunea vizează un sistem informatic situat pe teritoriul său, indiferent dacă autorul era sau nu era prezent fizic pe teritoriul său.</p>		Compatibil	<p>Art. 11 din Codul penal consacră principiul teritorialității legii penale, stabilind expres și excepțiile de la acesta. În completare, art. 12 din Codul penal reglementează locul săvârșirii faptei, inclusiv în cazul infracțiunilor transnaționale</p>
<p>(3) Un stat membru informează Comisia atunci când decide să își determine competența în ceea ce privește o infracțiune dintre cele menționate la articolele 3-8, care a fost săvârșită în afara teritoriului său, inclusiv în cazul în care:</p> <p>(a) autorul infracțiunii își are reședința</p>		Compatibil	<p>Art. 11 din Codul penal consacră principiul teritorialității legii penale, stabilind expres și excepțiile de la acesta. În completare, art. 12 din Codul penal reglementează locul săvârșirii faptei, inclusiv în cazul infracțiunilor transnaționale</p>

obișnuită pe teritoriul său; sau (b) infracțiunea a fost săvârșită în beneficiul unei persoane juridice având sediul pe teritoriul său.			
<p>Articolul 13</p> <p>Schimbul de informații</p> <p>(1) În scopul efectuării schimbului de informații referitoare la infracțiunile menționate la articolele 3-8, statele membre se asigură că dispun de un punct de contact național operațional și că utilizează rețeaua existentă de puncte de contact operaționale disponibile 24 de ore din 24 și șapte zile pe săptămână. Statele membre se asigură, de asemenea, că dispun de procedurile necesare astfel încât, pentru cereri urgente de asistență, autoritatea competentă poate indica, în termen de cel mult opt ore de la primire, cel puțin dacă cererea va primi un răspuns, precum și forma și ora estimată ale acestui răspuns.</p>		Prevedere aplicabilă statelor membre UE	
(2) Statele membre informează Comisia cu privire la punctul lor de contact desemnat menționat la alineatul (1). Comisia comunică aceste informații celorlalte state membre, precum și agențiilor și organelor specializate competente ale Uniunii.		Prevedere aplicabilă statelor membre UE	
(3) Statele membre iau toate măsurile necesare pentru a se asigura că sunt puse la dispoziție canale adecvate pentru a facilita aducerea, fără întârziere, la cunoștința autorităților naționale competente a infracțiunilor menționate la articolele 3-6.		Prevedere aplicabilă statelor membre UE	
Articolul 14		Prevedere aplicabilă statelor	

<p>Monitorizare și statistici</p> <p>(1) Statele membre se asigură că dispun de un sistem adecvat pentru înregistrarea, producerea și furnizarea de date statistice cu privire la infracțiunile menționate la articolele 3-7.</p>		membre UE	
<p>(2) Datele statistice menționate la alineatul (1) acoperă, cel puțin, datele disponibile cu privire la numărul de infracțiuni menționate la articolele 3-7 înregistrate de statele membre și numărul de persoane urmărite penal și condamnate pentru infracțiunile prevăzute la articolele 3-7.</p>		Prevedere aplicabilă statelor membre UE	
<p>(3) Statele membre transmit Comisiei datele culese în conformitate cu prezentul articol. Comisia asigură publicarea unei revizuii consolidate a acestor rapoarte statistice și transmiterea acestora către agențiile și organele specializate competente ale Uniunii.</p>		Prevedere aplicabilă statelor membre UE	
<p>Articolul 15</p> <p>Înlocuirea Deciziei-cadru 2005/222/JAI</p> <p>Decizia-cadru 2005/222/JAI este înlocuită în ceea ce privește statele membre care participă la adoptarea prezentei directive, fără a aduce atingere obligațiilor statelor membre în ceea ce privește termenul pentru transpunerea deciziei-cadru în legislația națională.</p> <p>În ceea ce privește statele membre care participă la adoptarea prezentei directive, trimiterile la Decizia-cadru 2005/222/JAI se interpretează ca trimiteri la prezenta directivă.</p>		Prevedere aplicabilă statelor membre UE	
<p>Articolul 16</p> <p>Transpunere</p>		Prevedere aplicabilă statelor membre UE	

(1) Statele membre pun în aplicare actele cu putere de lege și actele administrative necesare pentru a se conforma prezentei directive până la 4 septembrie 2015.			
(2) Statele membre transmit Comisiei textul dispozițiilor care transpun în legislația națională obligațiile care le revin în temeiul prezentei directive.		Prevedere aplicabilă statelor membre UE	
(3) Atunci când statele membre adoptă respectivele măsuri, acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a acestei trimiteri.		Compatibil	Prezenta lege transpune: art. 2 lit. (a) și (b); art. 3 – 5; art. 7; art. 9 alin. (2), (3) și (4) litera (a) și (c) din Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului, nr. CELEX: 32013L0040, publicată în Jurnalul Oficial al Uniunii Europene L218/8 din 14 august 2013
<p>Articolul 17</p> <p>Raportare</p> <p>Până la 4 septembrie 2017, Comisia prezintă Parlamentului European și Consiliului un raport de evaluare a gradului în care statele membre au adoptat măsurile necesare pentru a se conforma prezentei directive, însoțit, dacă este necesar, de propuneri legislative. Comisia ține seama, de asemenea, de evoluțiile tehnice și juridice în domeniul criminalității informatice, în special cu privire la domeniul de aplicare al prezentei directive.</p>		Prevedere aplicabilă statelor membre UE	
<p>Articolul 18</p> <p>Intrarea în vigoare</p> <p>Prezenta directivă intră în vigoare în a douăzecea zi de la data publicării sale în</p>		Prevedere aplicabilă statelor membre UE	

Jurnalul Oficial al Uniunii Europene.			
<p>Articolul 19</p> <p>Destinatarii</p> <p>Prezenta directivă se adresează statelor membre, în conformitate cu tratatele.</p>		<p>Prevedere aplicabilă statelor membre UE</p>	

CERERE nr. 03/1826 din 18 februarie 2026
privind înregistrarea de către Cancelaria de Stat
a proiectului de Lege pentru modificarea unor acte normative
(prevenirea și combaterea atacurilor împotriva sistemelor informatice)

Nr. crt.	Criterii de înregistrare	Nota autorului
1.	Categoria și denumirea proiectului	- Lege - Proiectul de lege pentru modificarea unor acte normative (prevenirea și combaterea atacurilor împotriva sistemelor informatice)
2.	Autoritatea care a elaborat proiectul	Ministerul Justiției
3.	Justificarea depunerii cererii	Necesitatea alinierii legislației naționale la aquis-ul UE
4.	Referința la documentul de planificare care prevede elaborarea proiectului (<i>PNA, PND, PNR, alte documente de planificare sectoriale</i>)	Transpunerea Directivei 2013/40/UE ce derivă din acțiunea nr. 16, subdomeniul 1.5., Anexa A, Capitolul 24, Clusterul 1 din PNA, aprobat prin <i>Hotărârea Guvernului nr. 306/2025</i> .
5.	Lista autorităților și instituțiilor a căror avizare este necesară	1. Procuratura Generală 2. Ministerul Afacerilor Interne 3. Serviciul de Informație și Securitate 4. Uniunea Avocaților din Moldova
6.	Termenul-limită pentru depunerea avizelor/expertizelor	10 zile
7.	Persoana responsabilă de promovarea proiectului	Gheorghe GHEORGHIȚĂ, consultant superior, Secția drept public, Direcția elaborare acte normative, tel.: 0 (22) 20 14 27, email: gheorghe.gheorghita@justice.gov.md
8.	Anexe	- Proiectul de lege – 3 file; - Nota informativă – 6 file - Tabelele de concordanță – 20 file.
9.	Data și ora depunerii cererii	18 februarie 2026
10.	Semnătura	