NOTA DE FUNDAMENTARE
la proiectul legii pentru modificarea și completarea unor act 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 – 260^4 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. 134^{25}, 259 – 260^{4} 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. 134^{25}, 259–260^{4} 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. 134^{28}:

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. 260^{1} („Interceptarea ilegală a unei transmisii de date informatice”) care este similar cu art. 6 al Directivei;

• art. 260^{2} („Alterarea integrității datelor informatice ținute într-un sistem informatic”) care este similar cu art. 5 al Directivei;

• art. 260^{3} („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 – 260^{3} din *CP*. Astfel, se impune completarea *CP* cu art. 134^{28} 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. 250^{3}:

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, componența 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 250^3 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 componența de bază a fost introdus semnul obligator descris mai sus.

Modificarea art. 260 și 260^4 din *CP*:

Textul actual al Codului Penal prezintă o suprapunere de obiect material/imaterial între art. 260 și art. 260^4, 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 îl 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. 260^4 va fi prevăzută infracțiunea ce ține de „parole de calculator, coduri de acces sau date similare”.

O altă modificare la art. 260 și 260^4 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 „<u>în principal</u>” 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. 260^2 din *CP*:

În art. 260^2 din *CP*, nu sunt specificate următoarele modalități normative menționate în art. 5 al Directivei: „periclitarea”, „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. 260^2 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. 260^2 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 periculozitate 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. 260^3 din *CP*:

În art. 260^3 din *CP*, nu sunt specificate următoarele modalități normative pe care le găsim în art. 4 al Directivei: „periclitarea”, „eliminarea” datelor informatice. Fapt pentru care, articolul menționat se completează cu modalitățile respective.

De asemenea, nu sunt identice modalitățile normative „restricționarea accesului” (art. 260^2 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. Măsuri 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

Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA).

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.

5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

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".

6. Avizarea și consultarea publică a proiectului actului normativ

În scopul respectării prevederilor *Legii nr. 239/2008 privind transparența în procesul decizional,* pe pagina web oficială a Ministerului Justiției www.justice.gov.md, la compartimentul *Transparența decizională,* 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.

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.

Propuneri sau recomandări nu au fost recepționate.

7. Concluziile expertizelor

Proiectul urmează a fi supus expertizei juridice și anticorupție, iar constatările acestora vor fi incluse după recepționarea expertizelor.

8. Modul de încorporare a actului în cadrul normativ existent

Proiectul nu presupune modificarea sau abrogarea altor acte normative.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Implementarea prevederilor proiectului nu implică realizarea unor măsuri speciale în acest sens.

Secretar de stat **Lilian APOSTOL**