SINTEZA
obiecțiilor și propunerilor la proiectul de lege pentru modificarea unor acte normative
(prevenirea și combaterea atacurilor împotriva sistemelor informatice)

Numărul unic înregistrat **140/MJ/2026**

Conținutul articolelor/punctelor din proiectul prezentat spre avizare și coordonare	Participantul la avizare, consultare publică, expertizare	Nr. crt.	Conținutul obiecției, propunerii, recomandării, concluziei	Argumentarea autorului proiectului
I. AVIZARE ȘI CONSULTARE PUBLICĂ				
Art. I. – Codul penal al Republicii Moldova nr. 985/2002				
1. Articolul 134^{25} va avea următorul cuprins: „Articolul 134^{25}. 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	**Procuratura Generală**	**1.**	1.1. La pct. 1, cu referire la art. 134^{25}, menționăm că, noțiunea de „sistem informatic" este definită la art. 2 din Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice (în continuare - Legea nr. 20/2009), fiind formulată după cum urmează: „sistem informatic orice dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în legătură care asigură sau dintre care unul ori mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor”. Subsidiar, constatăm că, definiția respectivă diferă de cea propusă în proiectul supus avizării, ceea ce poate genera neuniformități terminologice în cadrul normativ. Astfel, pentru a nu crea ambiguități în aspectul de aplicare a legii, propunem	**Se acceptă parțial** Definiția propusă în proiectul de lege asigură transpunerea definiției de „sistem informatic” din Directivă. Referitor la localizarea acesteia, se acceptă propunerea ca în Codul penal să se facă trimitere la Legea 20/2009.

vederea exploatării, a utilizării, a protecției și a întreținerii lor.”.			expunerea art. 134[25] din Codul penal în următoarea redacție: „Articolul 134[25]. Sistem informatic Prin sistem informatic se înțelege sistemul respectiv definit astfel în Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice.”	
	Serviciul de Informații și Securitate	**2.**	Din considerentul continuării firului logic prevăzut în punctul 2 al proiectului de lege, la punctul 1 sugerăm expunerea definiției după următorul model: „Prin sistem informatic se înțelege noțiunea definită în art. 2 din Legea nr. 1069/2000 cu privire la informatică”.	**Precizare** În sensul dreptului penal, definiția de sistem informatic trebuie să corespundă cu prevăzută de Directivă, care este cuprinsă în Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice.
	Serviciul Tehnologia Informației și Securitate Cibernetică	**3.**	1. Propunem expunerea alin. 1) din proiect, în următoare redacție: „Articolul 134[25] va avea următorul cuprins: Prin sistem informatic se înțelege sistem definit astfel în Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice.”. Propunerea dată rezumă, inclusiv din modelul de interpretare a noțiunii „date informatice”, utilizat în alineatul 2). De menționat, propunerea enunțată, este oportună și în sensul art. 55 alin. (1) din Lege nr. 100/2017 cu privire la actele normative, potrivit cărui reglementările de același nivel și având același obiect de reglementare se cuprind, de regulă, într-un singur act normativ. În cazul în care proiectul actului normativ cuprinde prevederi ce se regăsesc în alte acte normative, se face trimitere expresă la actul normativ care le conține.	**Se acceptă**
	Ministerul Dezvoltării Economice și Digitalizării	**4.**	Cu referire la art. I pct. 1 și 2, menționăm că în proiect se definește noțiunea de date informatice prin trimitere la Legea nr. 20/2009 privind prevenirea și combaterea criminalității	**Se acceptă**

			informatice. Totodată, în ceea ce privește noțiunea de sistem informatic, proiectul prevede introducerea în Codul penal a unei definiții noi, diferite de definiția specificată de Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice. Prin urmare, se constată existența a două formulări diferite pentru aceeași noțiune, una în proiectul de modificare a Codului penal, iar cealaltă în Legea nr. 20/2009. Astfel, pentru a evita dublarea de noțiuni și în scopul definirii corectă a noțiunii de „sistem informatic", propunem oferirea unei redacții noi a noțiunii date în Legea 20/2009, iar în Codul penal urmează a se face referire la aceasta după modelul propus la art. 134^{28}.	
2. Se completează cu articolul 134^{27} cu următorul cuprins: „Articolul 134^{28}. Date informatice Prin date informatice se înțelege datele definite astfel în Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice."	**Procuratura Generală**	**5.**	1.2. La pct. 2, din proiect constatăm o eroare de numerotare a indicelui articolului 134 din Codul penal, or, art. cu nr. 134^{27} deja este în Codul penal.	**Se acceptă**
	Serviciul de Informații și Securitate	**6.**	Ţinând cont că în cadrul legislației penale deja există articolul 134^{27} referitor la femicid, se propune înlocuirea sintagmei „se completează cu articolul 134^{27}" cu sintagma „se completează cu articolul 134^{28}".	**Se acceptă**
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,";	**Procuratura Generală**	**7.**	1.3. Cu referire la pct. 3 din proiect prin care se propune majorarea sancțiunii pentru infracțiunea prevăzută de art. 259 din Codul penal, prin substituirea textului „până la 1 an" cu „până la 2 ani", menționăm că, nu este clar raționamentul autorului proiectului de lege privind stabilirea sancțiunii maxime pentru infracțiunea prevăzută la alin. (1) art. 259 cu	**Precizare** Motivul majorării sancțiunii a fost expus în nota informativă. Aceasta se datorează faptului că în componența de bază a alineatului (1) a fost introdus un semn al infracțiunii nou, care oferă faptei un grad prejudiciabil mai ridicat.

textul „până la 1 an” se substituie cu textul „până la 2 ani”; la alineatul (2), litera a) se abrogă.			închisoarea de până la 2 ani, având în vedere că, din perspectiva pericolului social, nu există diferențe esențiale între infracțiunile reglementate la alin. (1) ale articolelor 260-260^6 din Codul penal, sancțiunile cărora prevăd închisoare de până la 5 ani. În aceste condiții, sancțiunea propusă de 2 ani pare disproporționată față de limitele stabilite pentru infracțiuni similare și poate genera inechitate în aplicarea normelor, precum și dezechilibru în cadrul sistemului sancționator. Prin urmare, se recomandă revizuirea sancțiunii maxime, sub aspectul înăspririi acesteia, în vederea asigurării echilibrului, coerenței și proporționalității măsurilor sancționatorii. Această recomandare este valabilă și pentru sancțiunile prevăzute la alin. (2) și (3) ale art. 259 din Codul penal.	Pe lângă cele menționate, Directiva stabilește la art. 9 alin.(2) condiția ca această faptă să fie sancționată cu o pedeapsă maximă cu închisoare de cel puțin 2 ani.
	Ministerul Afacerilor Interne	**8.**	Se propune expunerea art. 259 în următoarea redacție: „Articolul 259. Accesul ilegal la un sistem informatic (1) Accesarea cu intenție și fără drept, în întregime sau în parte, prin violarea măsurilor de securitate 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”. Necesitatea acestei intervenții legislative a fost evidențiată inclusiv în cadrul reuniunii de screening bilateral pentru Capitolul 24 „Justiție,	**Nu se acceptă** S-a decis a nu opera această modificare pentru că termenul „ilegal” este deja consacrat în practica judiciară națională, și nu se dorește crearea eventuală a unui efect de lege mai favorabilă care ar putea afecta cauzele pendinte sau cele definitiv soluționate. Din perspectiva juridică, termenii „ilegal” și „fără drept” sunt sinonime, pentru că sensul acestei noțiuni este dat de situațiile enumerate la art. 259 alin. (1). Astfel, accesarea se consideră ilegală atunci când: - o persoană care nu este autorizată în temeiul legii sau al unui contract;

			Libertate și Securitate”, desfășurată la Bruxelles în luna septembrie 2025, în cadrul căreia experții Consiliului Europei au recomandat alinierea cadrului normativ național prin introducerea expresă a sintagmei „fără drept” pentru a delimita în mod clar caracterul ilicit al accesului la sistemele informatice.	- care depășește limitele autorizării ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic; - să desfășoare cercetări științifice; - să efectueze orice altă operațiune într-un sistem informatic. Fiecare dintre aceste situații reprezintă, în esență, manifestarea juridică a lipsei unui drept specific. Prin urmare, introducerea sintagmei „fără drept” ar constitui o tautologie legislativă. Pe de altă parte, transpunerea unei directive nu înseamnă o preluare exactă a terminologiei, ci o adaptare conceptuală. Transpunerea unui directive impune statelor membre atingerea obiectivului de rezultat, însă lasă la latitudinea autorităților naționale alegerea formei și a mijloacelor. Având în vedere că sistemul de drept al RM posedă un lexic juridic propriu, este imperativ ca termenii utilizați să fie compatibili cu restul Codului penal.
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	**Procuratura Generală**	**9.**	1.4. La pct. 4 și pct. 8, având în vedere că, prin proiectul supus avizării se propune modificarea dispoziției art. 260 și, respectiv, art. 260^4, considerăm oportună revizuirea și titlurilor articolelor menționate, în vederea asigurării concordanței dintre titlul și conținutul normei.	**Se acceptă**
	Serviciul de Informații și Securitate	**10.**	Deoarece programele pot fi rezultatul diverselor tipuri de dispozitive, nu doar al celor de tip „calculator”, la punctul 4 se recomandă modificarea sintagmei „program de calculator” în sintagma „produs de program”.	**Nu se acceptă** A se vedea pct. 19 din sinteză.

prevăzute la art. 237, 259, 260^1–260^3, 260^5–260^7,"; cuvântul „întreprinderii" se substituie cu cuvântul „persoanei juridice".	**Ministerul Dezvoltării Economice și Digitalizării**	**11.**	La pct. 4 al proiectului, propunem a se completa cu o prevedere nouă privind modificarea titlului art. 260, conform modificărilor efectuate în textul acestuia.	**Se acceptă**
	Ministerul Afacerilor Interne	**12.**	În contextul alinierii cadrului normativ național la prevederile Directivei 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice, se propune utilizarea sintagmei „fără drept" în locul sintagmei „în mod ilegal" în cuprinsul art. 260 și art. 260^4 alin. (1) din Codul penal.	**Nu se acceptă** A se vedea pct. 8 din sinteză.
6. La articolul 260^2: 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	**Procuratura Generală**	**13.**	1.5. La pct. 6, cu referire la completarea prevederilor 260^2 alin. (3) cu lit. c) cu următorul cuprins: „săvârșite împotriva unui sistem informatic din infrastructura critică", menționăm că această formulare poate genera interpretări divergente în procesul de aplicare a normei. Or, noțiunea de „infrastructură critică" nu este definită în Codul penal, fiind reglementată în Legea nr. 120/2017 cu privire la prevenirea și combaterea terorismului.	**Se acceptă**
	Serviciul de Informații și Securitate	**14.**	Pentru evitarea caracterului limitativ, la punctul 6 (art. 260^2, alin. 2, lit. c), propunem substituirea sintagmei „program de calculator, a unei parole de calculator, a unui cod de acces sau a altor date de acces" cu sintagma „produs de program sau date de acces". Recomandăm utilizarea sintagmei „date de acces" deoarece aceasta cuprinde atât parolele, cât și codurile de acces.	**Nu se acceptă** A se vedea pct. 19 din sinteză.

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 juridicei”. 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”.				

	Serviciul de Informații și Securitate	**15.**	Din motive similare, la punctul 8 din proiect, se sugerează substituirea sintagmei „parole de calculator, a unui cod de acces sau a unor date similare” cu sintagma „date de acces”.	**Nu se acceptă** A se vedea pct. 19 din sinteză.
	Ministerul Afacerilor Interne	**16.**	Referitor la dispozițiile art. 260^4 alin. (1) din Codul penal, se propune completarea referinței la infracțiunile pentru a căror săvârșire pot fi utilizate parolele sau codurile de acces obținute sau furnizate fără drept, prin includerea articolelor 186 și 190 din Codul penal. Această completare este justificată de practica organelor de drept, potrivit căreia producerea, importul, comercializarea sau punerea la dispoziție, sub orice formă, a parolelor sau codurilor de acces care permit accesul la sisteme informatice constituie frecvent o etapă preliminară în comiterea infracțiunilor de sustragere a bunurilor sau fraudă în mediul digital, iar includerea articolelor 186 și 190 din Codul penal va contribui la consolidarea capacităților de documentare a infracțiunilor informatice și la sporirea eficienței intervenției organelor de drept în combaterea criminalității informatice.	**Nu se acceptă** O astfel de completare ar putea fi inadecvată în contextul Capitolului XI (Infracțiuni informatice). Infracțiunile cuprinse în înșiruirea de la art. 260^4 se referă pregătirea săvârșirii altor infracțiuni informatice. Pe de altă parte, infracțiunile prevăzute la art. 186 și art. 190 fac parte din Capitolul VI (Infracțiuni contra patrimoniului), având un obiect juridic distinct de cel al infracțiunilor informatice. Art. 260^4 este destinat combaterii faptelor care atentează la siguranța sistemelor informatice, nu la protecția bunurilor materiale. Articolele 186 și 190 au propriile lor forme agravante și praguri de prejudiciu. Prin includerea lor sub umbrela art. 260^4, s-ar putea ajunge la situații în care obținerea unei parole pentru un furt minor să fie pedepsită mai aspru (ca infracțiune informatică) decât tentativa de furt în sine. Totodată, Directiva nu extinde acest mecanism la infracțiunile „clasice” (furt, escrocherie) chiar dacă acestea se comit în mediul digital. Pentru frauda comisă prin sisteme informatice, UE are o altă directivă separată (Directiva 2019/713 privind combaterea fraudelor și a falsificării mijloacelor de plată fără numerar).
	Procuratura Generală	**17.**	1.6. Creșterea implicării grupurilor și organizațiilor criminale în săvârșirea	**Nu se acceptă**

			infracțiunilor informatice, constituie un pericol social sporit, care afectează securitatea cibernetică, ordinea publică și integritatea economică a statului. În vederea prevenirii și combaterii acestor fapte, precum și pentru descurajarea implicării grupurilor criminale sau a organizațiilor criminale la comiterea infracțiunilor prevăzute de articolele 260, 260^1, 260^5 și 260^7 din Codul penal, propunem completarea normelor prenotate cu un alineat nou, care ar reglementa comiterea infracțiunilor în interesul unui grup criminal organizat sau al unei organizații criminale, cu stabilirea unei pedepse corespunzătoare. Această propunere de completare a proiectului răspunde necesității de consolidare a capacității statului de a proteja societatea și sistemele informatice împotriva infracționalității organizate. Subsidiar, introducerea explicită a agravantei la prevederile articolelor 260, 260^1, 260^5 și 260^7 va permite autorităților competente să intervină eficient în cazurile de criminalitate informatică organizată și să aplice sancțiuni proporționale gravității faptelor și pericolului social ridicat pe care acestea îl generează.	Directiva 2013/40 nu impune aceste agravante specifice, fapt ce denotă că la nivel european s-a considerat că formele de bază și agravantele legate de impactul sistemic (infrastructura critică) sunt suficiente pentru a acoperi gradul de pericol al acestor fapte. Deși propunerea invocă o creștere a implicării grupurilor criminale, aceasta nu este însoțită de o analiză de impact sau de prezentarea unor cazuri concrete/indicatori statistici care să demonstreze insuficiența actualului cadru legal. Introducerea unor noi circumstanțe agravante trebuie să se bazeze pe o documentare riguroasă a dificultăților întâmpinate de organele de drept în aplicarea normelor existente. În lipsa unor motive care să ateste că actualul regim sancționare a împiedicat pedepsirea proporțională a infracționalității informatice organizate, propunerea apare ca fiind insuficient fundamentată sub aspectul necesității stringente. Totodată, legea penală prevede o posibilitate de aplicare a unei sancțiuni mai aspre în cazul săvârșirii infracțiunii de către un grup criminal organizat sau organizație criminală, și anume prin intermediul art. 77 din CP. Conform art. 77 săvârșirea infracțiunii prin orice formă de participație constituie deja o circumstanță agravantă generală, care permite instanței să aplice o pedeapsă mai aspră în limitele sancțiunii prevăzute de articol.
	Serviciul Tehnologia	**18.**	2. La elaborarea acestui proiect este oportun a se ține cont de faptul, că atacurile împotriva	**Nu se acceptă**

	Informației și Securitate Cibernetică		obiectivelor infrastructurii critice, în sensul Legii 120/2017 cu privire la prevenirea și combaterea terorismului și Regulamentului privind protecția antiteroristă a infrastructurii critice, aprobat prin Hotărârea Guvernului nr. 701/2018, la fel pot afecta sau pot avea impact negativ (întreruperea funcționării) asupra sistemelor informatice din infrastructura critică. Prin urmare, se propune examinarea necesității completării proiectului în acest sens.	Directiva prevede drept circumstanță agravantă doar cazurile când infracțiunea este săvârșită împotriva unui sistem informatic din „infrastructura critică” în ansamblul său, fapt pentru care stabilește o sancțiune proporțională cu pericolul acestei fapte. Conform definițiilor legale, „infrastructura critică” reprezintă sistemul a cărui perturbare sau distrugere are un impact semnificativ la nivel național, în timp ce „obiectivul infrastructurii critice” reprezintă un element component sau un punct specific. Deși afectarea unui obiectiv este gravă, aceasta nu echivalează automat cu prăbușirea întregului sistem critic național.
	Ministerul Dezvoltării Economice și Digitalizării	**19.**	Pentru un spor de precizie normativă, în tot textul proiectului considerăm oportun substituirea cuvintelor „program de calculator” cu cuvintele „produs program”, întrucât aceasta din urmă are un caracter mai larg și reflectă mai adecvat realitățile tehnologice actuale. Formularea propusă va asigura prevenirea apariției lacunelor de incriminare generate de interpretarea restrictivă a noțiunii de „program de calculator”.	**Nu se acceptă** Proiectul de lege urmărește transpunerea Directivei 2013/40/UE, care utilizează în mod consacrat termenul de „program de calculator” (computer programme). Totodată, conform Legii nr. 1069/2000 cu privire la informatică noțiunea de „produs program” este mult mai largă decât noțiunea de „program (program de calculator)” pentru că aceasta include și documentele asociate ale unui sistem de prelucrare a informației. Dacă înlocuim „program de calculator” cu „produs program”, o persoană care ar sustrage ilegal un simplu Manual de utilizare (document asociat) ar putea fi acuzată teoretic de aceeași infracțiune gravă ca o persoană care a spart codul sursă al sistemului, deoarece ambele sunt părți componente ale „produsului program”.

				Opinia autorului prin care sesizează că ar putea exista o interpretare restrictivă, este puțin probabilă deoarece jurisprudența s-a adaptat deja la faptul că un program poate rula pe orice tip de arhitectură hardware.
Art. II. – Codul contravențional al Republicii Moldova nr. 218/2008				
„**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.”	**Ministerul Afacerilor Interne**	**20.**	Referitor la modificarea Codului contravențional, având în vedere faptul că elementele constitutive ale contravenției prevăzute la art. 250³ din proiect coincid, în mare măsură, cu cele ale infracțiunii prevăzute la art. 259 din Codul penal, considerăm oportun revizuirea conținutului normativ al acestei contravenții, în vederea delimitării mai clare dintre răspunderea contravențională și cea penală. În acest sens, se propune reformularea dispoziției art. 250³ din Codul contravențional (proiect), astfel încât aceasta să vizeze situațiile în care accesarea fără drept a unui sistem informatic nu a cauzat prejudicii materiale și/sau nu a produs consecințe juridice. Prin urmare, se propune expunerea art. 2593 în următoarea redacție: „Articolul 2503 . Accesul ilegal la un sistem informatic Accesarea fără drept, în întregime sau în parte, a unui sistem informatic de către o persoană care nu este autorizată în temeiul legii sau al unui contract, 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 a cauzat prejudicii materiale și/sau nu a produs consecințe juridice”. O asemenea abordare va permite stabilirea unui criteriu suplimentar de	**Precizare** Delimitarea dintre contravenția propusă și infracțiunea de la art. 259 din CP se asigură prin sintagma „dacă fapta nu constituie infracțiune” care este cuprinsă în redacția proiectului de lege. Totodată, delimitarea se asigură prin semnul componenței de infracțiune cuprins la art. 259 din CP și care nu este prezent în componența contravenției propuse. Astfel, fapta va fi calificată drept infracțiune doar dacă a fost săvârșită prin violarea măsurilor de securitate. Iar fapta va fi clasificată drept contravenție când nu va fi prezent acest semn. Sintagma „dacă fapta nu a cauzat prejudicii materiale și/sau nu a produs consecințe juridice” ar putea crea situații care să rămână neacoperite de lege. De exemplu, situația în care fapta nu este săvârșită cu violarea măsurilor de securitate, dar a produs careva prejudicii sau consecințe juridice, nu va putea fi calificată nici în baza art. 259 din CP și nici în baza normei propuse de autorul avizului.

			delimitare între contravenție și infracțiune, facilitând aplicarea uniformă a legislației de către organele competente.	
Declarația de Compatibilitate				
	Centrul de Armonizare al Legislației	**21.**	Potrivit Tabelului de concordanță, prevederile art. 13 și 14 din Directivă sunt calificate eronat ca ”Prevederi UE neaplicabile”, ori acestea sunt prevederi UE cu caracter obligatoriu care necesită transpunere în legislația națională în vederea asigurării transpunerii integrale a Directivei UE. Astfel, în ceea ce privește art. 13 din Directivă, care se referă la schimbul de informații între statele membre ale Uniunii Europene referitoare la infracțiunile constatăm că, acesta este implementat parțial prin art. 7 din Legea 48/2023 privind securitatea cibernetică și pct. 6 din Regulamentul cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică, aprobat prin HG nr. 1028/2023, care desemnează Agenția pentru Securitate Cibernetică ca punct național unic de contact pentru transmiterea, la cererea autorităților și instituțiilor publice sau a echipelor de răspuns la incidentele cibernetice, punctelor unice de contact din alte state notificări și solicitări privind incidentele cibernetice. În context, se impune concretizarea dacă Agenția acționează ca punct de contact și în cazul infracțiunilor informatice în condițiile și termenele stabilite de alin. (1). Mai mult ca atât, se impune completarea legislației relevante, cu obligația din art. 13 (2) din Directivă referitor la notificarea Comisiei privind punctul de contact desemnat, cu punere în aplicare din data aderării la UE.	**Precizare** În baza Legii nr. 6/2009 Republica Moldova, în conformitate cu articolul 35 alineatul 1 din Convenția privind criminalitatea informatică (2001), a desemnat punctul de contact responsabil de cooperarea internațională imediată și permanentă în domeniul combaterii criminalității informatice, care se află în cadrul Ministerului Afacerilor Interne.

	Centrul de Armonizare al Legislației	**22.**	Cu referire la art.14 din actul UE, care se referă la obligația statului de a institui un ”sistem adecvat pentru înregistrarea, producerea și furnizarea de date statistice cu privire la infracțiunile” respective constatăm că, acesta este implementat parțial de Legea nr. 216/2003 cu privire la Sistemul informațional integrat automatizat de evidență a infracțiunilor, a cauzelor penale şi a persoanelor care au săvârșit infracțiuni și de HG nr. 328/2012 cu privire la aprobarea Regulamentului privind organizarea şi funcționarea Sistemului informațional automatizat „Registrul informației criminalistice şi criminologice”, care instituie sistemul național de evidență statistică a infracțiunilor. Totodată, se impune completarea legislației relevante, cu obligația de la art. 14 (3) din Directivă referitor la transmiterea către Comisie a datelor culese, cu punere în aplicare din data aderării la UE.	**Se acceptă** Tabelul de concordanță a fost completate corespunzător
	Centrul de Armonizare al Legislației	**23.**	Obiecții privind tabelul de concordanță la Directiva 2013/40/UE Pentru art. 13 și 14 din Directivă, calificativul de compatibilitate „Prevederi aplicabile statelor membre UE” se va modifica în „Parțial compatibil”, cu inserarea explicațiilor și motivelor care stau la baza implementării parțiale expuse mai sus.	**Se acceptă**
II. EXPERTIZA ANTICORUPȚIE				
Art. I pct. 3 din proiect, prin care se modifică art. 259 alin. (1) din Codul Penal și Art. II din proiect, prin care se completează cu art. 250³ în Codul Contravențional.	**Centrul Național Anticorupție**	**24.**	Obiecții: Potrivit proiectului, se instituie răspunderea contravențională pentru „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	**Se acceptă.** În urma analizei obiecției formulate s-a decis revizuirea arhitecturii normative propuse inițial în proiectul de lege prin delimitarea faptei de accesare ilegală a unui sistem informatic în legislația penală (art.

Art. I. – Codul penal [...] , se modifică după cum urmează: 4. La articolul 259: la alineatului (1): după textul „Accesarea ilegală” se completează cu textul „ , în întregime sau în parte, prin violarea măsurilor de securitate,” Art. II. – Codul contravențional [...], 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.”			folosească, să administreze sau să controleze un sistem informatic [...], dacă fapta nu constituie infracțiune”. Concomitent, art. 259 alin. (1) din Codul Penal, în redacția propusă, va sancționa „accesarea ilegală, în întregime sau în parte, prin violarea măsurilor de securitate, a unui sistem informatic”. Astfel, din conținutul normelor rezultă că principalul criteriu de delimitare dintre răspunderea contravențională și cea penală îl constituie existența sau inexistența elementului „violarea măsurilor de securitate”. Deși, în mod formal acest criteriu reprezintă o diferențiere, analiza proiectului relevă că delimitarea practică dintre cele două forme de răspundere rămâne insuficient de explicită. În acest sens, art. 2 din Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice definește „măsurile de securitate” ca fiind „folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricționat sau interzis pentru anumite categorii de utilizatori” . Cu toate acestea, cadrul normativ nu conține criterii suficient de explicite pentru delimitarea situațiilor în care o anumită conduită urmează a fi calificată drept „violare a măsurilor de securitate”, aspect care poate genera dificultăți de interpretare și aplicare. În consecință, în practică pot apărea situații-limită în care încadrarea juridică a faptei să fie dificil de realizat, cum ar fi accesarea unui cont rămas activ după încetarea raporturilor contractuale sau de serviciu, exploatarea unei configurări defectuoase a sistemului ori accesarea unor resurse insuficient protejate. În asemenea circumstanțe, determinarea faptului dacă a existat sau nu o „violare a măsurilor de	259) și în legislația contravențională (art. 250[3]), în funcție de existența sau inexistența elementului „violarea măsurilor de securitate”. Principalul impediment în identificarea unor criterii suplimentare de delimitare a infracțiunii față de contravenție constă în natura juridică a valorii sociale protejate prin incriminarea acestei fapte. Infracțiunea de acces ilegal la un sistem informatic protejează **integritatea și securitatea sistemelor informatice,** iar stabilirea unor criterii suplimentarea de altă natură, cum ar fi existența sau lipsa unui prejudiciu, valoarea prejudiciului cauzat, consecințele produse asupra funcționării sistemului informatic etc, nu fac decât să preschimbe valoarea juridică protejată prin această infracțiune Accesarea ilegală a unui sistem informatic poate fi săvârșită fără a cauza vreun prejudiciu material cuantificabil, iar incriminarea nu poate fi condiționată de atingerea unui prag valoric, sau producerea unei anumite urmări.

			securitate” poate depinde de evaluări tehnice și juridice complexe, precum și de aprecierea subiectivă a organului constatator, a organului de urmărire penală sau a expertului desemnat. Mai mult, proiectul nu instituie criterii obiective suplimentare care să permită delimitarea clară dintre contravenție și infracțiune, cum ar fi existența sau lipsa unui prejudiciu, valoarea prejudiciului cauzat, consecințele produse asupra funcționării sistemului informatic, nivelul accesului obținut. În lipsa unor asemenea repere normative, aceeași conduită poate fi calificată diferit de către autoritățile competente, în funcție de modul în care este apreciată existența și încălcarea măsurilor de securitate. Această situație conferă organelor de constatare și organelor de urmărire penală o marjă largă de apreciere în procesul de calificare juridică a faptelor. Sub aspectul Metodologiei de efectuare a expertizei anticorupție a proiectelor de acte normative, norma analizată generează factorul de corupție aferent normelor insuficient determinate și normelor care permit interpretări extensive sau divergente. În lipsa unor criterii obiective de delimitare, autoritățile competente dispun de o marjă largă de apreciere în procesul de calificare juridică a faptelor, ceea ce poate conduce la aplicarea neuniformă a legislației și la tratamentul diferențiat al unor situații comparabile. Recomandări: Se recomandă revizuirea mecanismului de delimitare dintre contravenția prevăzută la art. 250³ din Codul Contravențional și infracțiunea prevăzută la art. 259 alin. (1) din Codul Penal, prin dezvoltarea normativă a elementului „violarea măsurilor de	

			securitate” și/sau prin instituirea unor criterii suplimentare, clare și verificabile, de calificare a faptelor, inclusiv prin raportare la gravitatea faptei, natura accesului obținut, existența prejudiciului, consecințele produse ori alte elemente relevante.	
III. Consultarea Comisiei Europene				
	Comisia Europeană (DG HOME)	**25.**	1. “without right” is to be interpreted A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Member States may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Directive, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Member State’s government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and	**Se acceptă** Art. 259, 260, 260^{1}, 260^{4} au fost ajustate corespunzător.

			common operating or commercial practices should not be criminalised. As such, this is distinct from ”illegal”: compatibility should be confirmed	
	Comisia Europeană (DG HOME)	**26.**	2. Cybersecurity research and pentesting are not criminalized Recital 17) of the Directive This Directive does not impose criminal liability where the objective criteria of the offences laid down in this Directive are met but the acts are committed without criminal intent, for instance where a person does not know that access was unauthorised or in the case of mandated testing or protection of information systems, such as where a person is assigned by a company or vendor to test the strength of its security system. In the context of this Directive, contractual obligations or agreements to restrict access to information systems by way of a user policy or terms of service, as well as labour disputes as regards the access to and use of information systems of an employer for private purposes, should not incur criminal liability where the access under such circumstances would be deemed unauthorised and thus would constitute the sole basis for criminal proceedings. Please confirm that the necessary exceptions are taken into account in national law	**Precizare** Art. 259 utilizează fraza „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” ceea ce presupune că atunci când făptuitorul are aceste permisiuni, fapta acestuia nu constituie infracțiune.
	Comisia Europeană (DG HOME)	**27.**	3. Liability of legal persons The applicability of Article 10 of the Directive to all offences should be confirmed	**Precizare** În tabelul de concordanță la art. 10 din Directivă este reflectat că toate infracțiunile cuprinse în Directivă, corespondente în

				Codul penal al RM, prevăd și stabilesc răspunderea persoanelor juridice pentru comiterea acestor infracțiuni.
	Comisia Europeană (DG HOME)	**28.**	4. Monitoring and statistics This provision is not applicable only to Member States and should be transposed”	**Precizare** Tabelul de concordanță a fost completat corespunzător.